Global Information Assurance Certification Paper

Protect your enterprise against clients centric attacks, using Windows 2000 GPO
Thierry Agassis
August 11, 2001

Introduction

Access to Internet from the enterprise is a must for more and more businesses.
Accessing information worldwide is easier than ever, projects and decisions are made faster and faster due to this new way of conducting business : get and send data from anywhere to anywhere.

But getting data from Internet within the enterprise introduces new security risks which make many companies to decide not to let their employees to surf the WEB.

Usually, attention is paid to securing critical servers, aspecially Internet servers.
We often protect our **servers** against potentials and real threats.
But it is time to prevent **client centric attacks**, too.

Every **user agent** in the enterprise (mail or WEB) is a potentiel hacker's agent.
Recent mail worms are typical and spectacular examples. But think about such piece of code which, instead of spreading itself and destroying files, steal data from your personnal computer or servers and send them back to a hacker or a competitor.
Did it happen to you ? How do you know ?

But it is not a security issue, only. WEB technologies can simply update or patch softwares on your computer. It may have no consequence at home, but on a network with thousands of desktops, it may become a nightmare due to applications and librairies versions incompatibilities. So limiting these risks should be part of your **assets management** policies, too.

Objectives

This paper explains how Windows 2000 technologies can **mitigate** the risks of clients centric attacks.

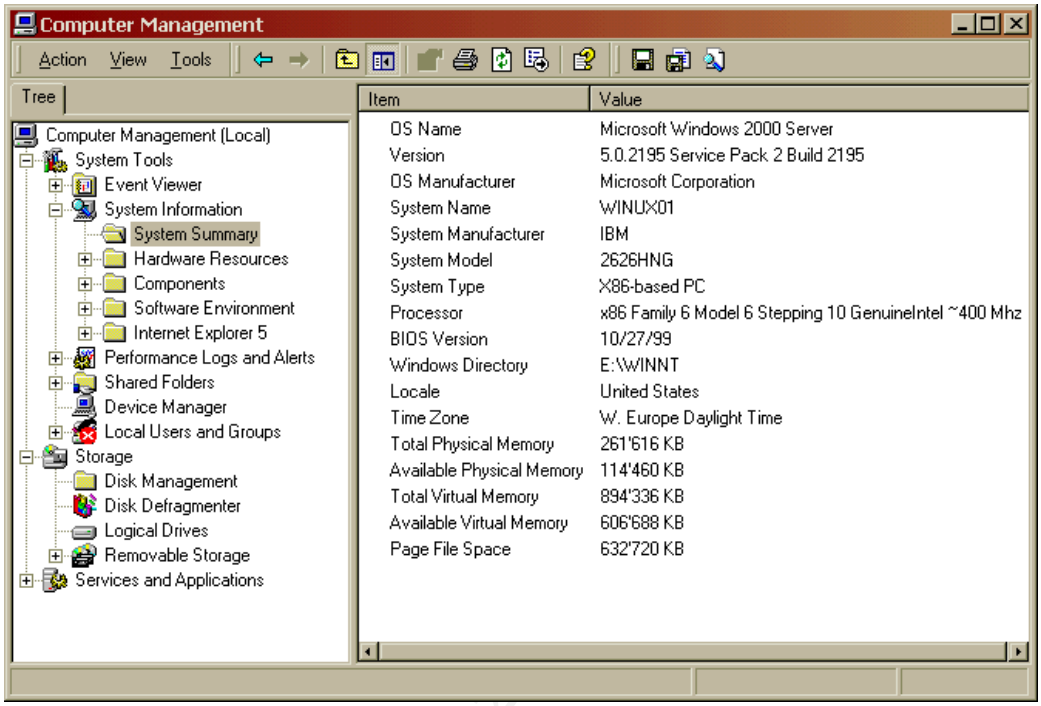
The steps required to implement security in the browsers of the enterprise are :

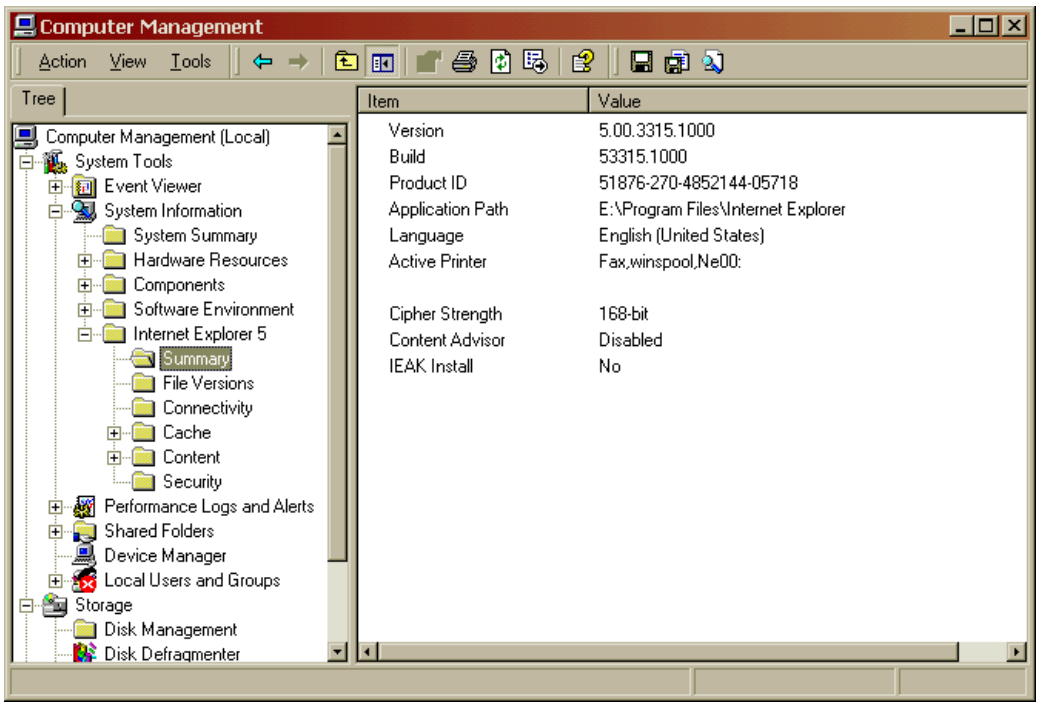
1. Understand risks related to WEB technologies used to/from Internet
2. Choose / understand your DNS and proxies topology
3. Define your users categories and respective Internet Explorer security settings
4. Organize your Windows 2000 groups and OU's for these categories of users
5. Create your GPO's with security settings,protect and link them to the respective OU's.
6. Test
7. Go to production

We first introduce WEB technologies to help the reader to make sound decisions on the way to configure the browsers within the enterprise.
Internet Explorer security settings are shown.
Then, the steps required on Windows 2000 to control browsers security settings with GPO's are explained.
Tips are provided, too, to find a balanced control and, hopefully, reduce the number of calls to the help desk.

Environment used

Any screen shot or procedure in this paper has been tested on the following environment (unless specified) :





Tip : if you live outside the USA, install service pack 2 on Windows 2000 to get the high encryption pack. This pack brings strong encryption for SSL (HTTPS)

WEB technologies

First, let's summarize what technologies make the WEB so convenient, while reminding the potential of these technologies to modify, read and write files or parameters on your computer.

HTTP

Hyper **T**ext **M**arkup **L**anguage
This is the base language **interpreted by the browser**. Each WEB pages has some HTML tags which define the presentation (layout) of the page.
The HTML tags are interpreted in the context of the browser itself.
The language has no local I/O functions available so HTML code cannot acess local ressources directly.

Here is an extract of HTML code :

```
<HTML>

<HEAD>
        <TITLE>Unicible</TITLE>
        <META NAME="Generator" CONTENT="Gaga 3.0.1 for Windows">
</HEAD>

<BODY BGCOLOR="#140A3F" LINK="#0000FF" VLINK="#800080" TEXT="#000000">

        <TABLE BORDER=0 CELLSPACING=0 CELLPADDING=0 WIDTH=630>
        <TR VALIGN="top" ALIGN="left">
        <TD WIDTH=96 HEIGHT =49><IMG SRC="./assets/auto_generated_images/img_3e594b69.gif »
…
</HTML>
```

XML

e**X**tended **M**arkup **L**anguage
Next generation of markup language.
As the accronym means, XML can be extended with new, custom tags.
This property extends the markup language capabilities, too, so that data structures can be defined. XML is not a presentation language, only, but make the data meaningfull, too, so that a script executed in the browser can interpret them.

Since the set of tags can be extended, a Data Type Dictionnary (DTD) may have to be provided, too, which describes the data types contained between tags. The DTD is needed for the application to handle new tags.

Since XML parsers are readily available, the language is used for other purposes, like configuration files.

XML can also be extended to define standard inter-applications messages (à la EDI), and will be a foundation of .Net services.

For the purpose of this paper, remember that XML pages are **interpreted in the context of the user agent** (browser) and that **no I/O functions exist** in the language. So local ressources cannot be accessed directly from XML code.

XML code example (from http://www.xml.org) :

```
<?xml version="1.0" encoding="iso-8859-1"?>
<!DOCTYPE titlepage SYSTEM "http://www.foo.bar/dtds/typo.dtd"
[<!ENTITY % active.links "INCLUDE">]>
<titlepage id="BG12273624">
   <white-space type="vertical" amount="36"/>
   <title font="Baskerville" size="24/30"
         alignment="centered">Hello, world!</title>
   <white-space type="vertical" amount="12"/>
   <!-- In some copies the following decoration is
         hand-colored, presumably by the author -->
   <image location="http://www.foo.bar/fleuron.eps"
         type="URL" alignment="centered"/>
   <white-space type="vertical" amount="24"/>
   <author font="Baskerville" size="18/22"
         style="italic">Vitam capias</author>
   <white-space type="vertical" class="filler"/>
</titlepage>
```

JavaScripts

Technology by Netscape.
JavaScripts are integrated into HTML pages and are interpreted by the user agent (browser). They have the same rights as the user of the browser, **but no native I/O functions are available in the language**, today.
A JavaScript can modify the HTML page it is in (adding tags). Using this fonctionality, a **JAVA applet could be « called » by the JavaScript**. This means that if the Java Virtual Machine (JVM) of the browser let an applet access a local disk or network, the JavaScript may indirectly access local resources.

JavaScript code extract :

```
<SCRIPT LANGUAGE=JavaScript>
        <!--
        var InternetExplorer = navigator.appName.indexOf("Microsoft") != -1;
        var portNumber;
        fonction blabla ()
        {
                ...
        }
</SCRIPT>
```

Typical consequences of running an hostile **JavaScript with a low security setting on the JVM** :

- Read local data and return them to the Internet WEB site
- Modify local files or registry settings
- Access to internal databases

VBScripts

Technology by Microsoft.
VBScripts are integrated into HTML pages and are interpreted by the user agent (browser). They have the same rights as the user of the browser**, but no native I/O functions are available**, today.
However, a **VBScript can interract with ActiveX controls and JAVA applets**. This means that, if scripting of ActiveX controls is allowed, local resources can be accessed with the user's privileges. See « Safe for scripting », too, in this document.

Extract of a page containing a Vbscript :

```
<SCRIPT LANGUAGE="VBScript">
<!--
                    Sub BtnHello_OnClick
                    MsgBox "Hello World!", 0, "My first active document"
                    End Sub
-->
</SCRIPT>
```

Potential consequences of running an hostile VBcript with scripting of ActiveX allowed :

- Read local data and return them to the Internet WEB site
- Modify local files or registry settings
- Access to internal databases

If the download of ActiveX controls is allowed, the hostile VBscript can bring in the necessary tools with it.

JAVA

Technology by SUN Microsystems.
JAVA is a technology of mobile code. Small applications (applets) are downloaded on request by the browser. JAVA is a compiled programming language, not a scripting language, and complex applications (or components of applications) can be designed, like word processing or spread sheet. Components of a given application can be downloaded on demand.
The code itself is semi-compiled (into a byte code) and is interpreted by the so called « Java Virtual Machine – JVM », usually part of the browser.
A JVM has its own security model which prevents an applet from accessing local files or local network ressources. By default, a JVM lets an applet to connect to the host it comes from (load host via HTTP), only, and nowhere else.
However, Internet Explorer has options to let an applet performing local I/O's. The security settings may depend on the fact that an applet is signed or not.

If an applet is allowed to perform local I/O's, it has as much priviledges as the user's account who downloaded it. So if a user is part of the Domain Administrators group, the applet she may download has full priviledge within the domain's ressources, as long as the JVM allows local I/O's.

Extract of an HTML page requesting a JAVA applet :

```
<APPLET CODEBASE="http://204.160.241.24/javanews/classes" CODE="News" WIDTH="200"
HEIGHT="140" ARCHIVE="news.jar,news.zip">

<PARAM NAME="bg-color" VALUE="255 255 204">
<PARAM NAME="country-string-color" VALUE="102 102 0">
<PARAM NAME="border-color"VALUE="102 102 0">

</APPLET>
```

Potential consequences of running an hostile JAVA code with a low security setting on the JVM :

- Read local data and return them to the Internet WEB site
- Modify local files or registry settings
- Access to internal database

ActiveX

Technology by Microsoft.
An ActiveX control can be considerred as « special » Dynamically Linked Libraries (DLL with normalized « entry points ») downloaded and executed by the browser.
No concept of virtual machine exist for ActiveX controls. **This means that a downloaded ActiveX has all the priviledges on local ressources that the user's account permits**.
When an ActiveX is downloaded, it is saved on disk and registerred in the local registry for future use (à la regsvr32.exe).
The next time the same ActiveX is requested by the browser, it is not downloaded as long as the classID and version referred in the page is the one registerred locally.
An ActiveX control can be pre-installed on a local machine and can be invoked by a VBScript or called directly by the browser.
More and more Windows applications are built with ActiveX controls and then, may be called from a VBscript downloaded from Internet…

Extract of an HTML page requesting an ActiveX :

```
<OBJECT
    id=HelloWorld
    CODEBASE="http://www.unicible.ch/HelloWorld.ocx"
    classid="clsid:7823A620-9DD9-11CF-A662-00AA00C066D2">
</OBJECT>
```

Potential consequences of running an hostile ActiveX control :

- Read local data and return them to the Internet WEB site
- Modify local files or registry settings
- Access to internal database

Mobile code signing

Authenticode is a way to electronically sign ActiveX controls or JAVA applets. Basically, a signature binds the developper's identity to the code he has published. It **doesn't add any security to the code itself** ; it simply « guarrantees » the identity of the author of the code. The word « guarrantees » is double-quoted, because the signature verification still depends on the Certification Authority (CA) who signed the publisher's certificate. This supposes that the certificate stores of the browsers contain **trusted CA's**, only…
For instance, the Root Agency CA should not be considerred as a trusted CA, since it is for test purposes, only.

While signing code, a developper may specify what JVM « priviledges » are needed. If the priviledges specified in the signature are not allowed by the JVM, a pop up window informs the user that the applet is forbiden by the browser security settings.
If an applet tries to perform « priviledged » operations not requested in the signature, the applet will fail and an uncomplete page may appear with no pop up window saying that there is a security problem.

« Safe for scripting »

As explained previously, ActiveX controls can be called by scripts. If an ActiveX is able to access local ressources, a JavaScript or VBscript downloaded from Internet could call the ActiveX and, say, return local data outside the company…
The writer of an ActiveX can mark his code as « safe for scripting » (IObjectSafety). By doing so, she says that the code can be safely called by a script.
Again, this is based on the level of trust you have in the publisher of the code and no security is enforced by the browser when an ActiveX is marked « Safe for scripting ».
An ActiveX could even be wrongly marked « Safe for scripting ». It is possible to mark a control « Safe for scripting » simply adding a registry key.

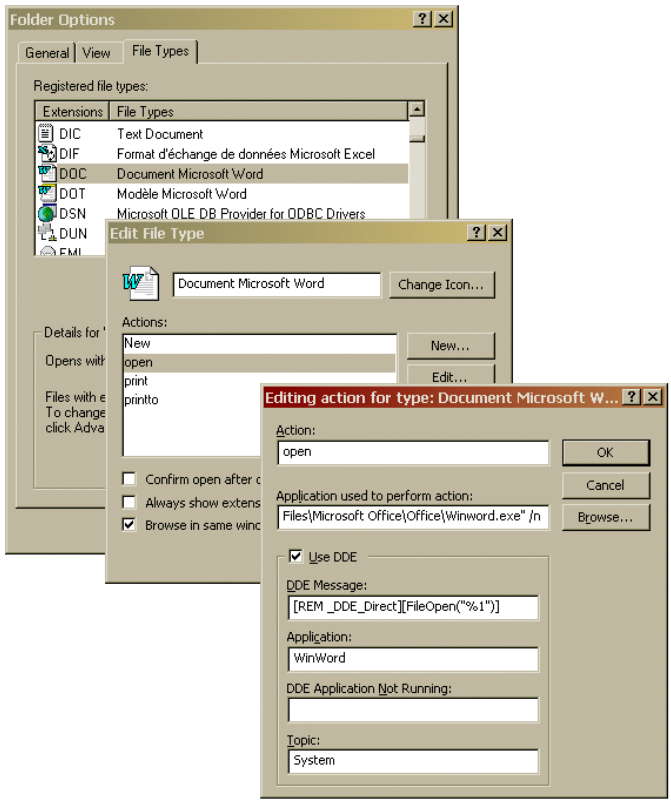
« Safe for scripting » should be combined with authenticode to eventually identify who pretends that the code is safe for scripting.

To view local ActiveX controls marked « Safe for scripting » in the registry, use **oleview.exe** (part of the ressource kit. All controls with the Implemented Categories key **7DD95801-9882-11CF-9FA9-00AA006C42C4** are marked « Safe for scripting ».

Here is a dialogue I had with a software developper who called me to open his browser to download some ActiveX from a WEB server used for developpement.
After helping him, I asked : why did you choose ActiveX instead of Java for your application ?
Answer : because we need to read the keys pressed by the users on the keyboard. (Note : the application is a 3270 terminal emulator)
Interresting ! And did you mark your code as « Safe for scripting » ?
Yes !
Why ?
To make it work regardless the browser settings.
Obvious. ☹

Helpers

Depending on the content type of a given page, the browser is either able to « handle » the content directly and displays it (e.g. GIF files), interprets it (e.g. scripts or Java applets) or calls an ActiveX control (downloaded or pre-installed).
If a given object cannot be handeled by the browser itself, the latter will look into the registry below HKEY_CLASSES_ROOT for an **external application** (helper) to be launched.
The application mappings can be displayed using Windows explorer (Tools menu, Folder Options) :



But the process used by Internet Explorer to define what external application is to be launched is complex. Here is the sequence of operations performed in the background :

1. Check the server supplied MIME type (content type)
2. If not available, several different tests are run to determine the real content of the file
3. Check the file extension.

(See http://msdn.microsoft.com/library/default.asp?url=/workshop/networking/moniker/overview/appendix_a.asp?frame=true for more information.)

If an application mapping is finally found, the respective application is launched.
If the « Confirm open after download » box is checked (see previous picture), the user is prompted, first.
If no application is found to handle the content, Internet Explorer prompts the user to

save it on disk or to specify an application to be launched.

Downloads

When a file is referred in a URL, it is downloaded and the steps just described to handle the file are taken.
It seems that sometimes Internet Explorer doesn't consider a file, which an ActiveX can handle, as « downloaded ».
For instance, when Adobe Acrobat Reader is installed, an ActiveX (pdf.ocx) is registerred locally. When a URL pointing to a PDF file (*.pdf) is selected, the file is displayed in the browser**, even if downloads are not allowed by the current security settings**.

User access to local files

Using **file://<local_filename>** URL types, a user might be able to access local files. It can be an undesirable consequence if your users are not supposed to access local files directly.

User access to LDAP directory

Using **ldap://<LDAP_server>/<Distinguished_Name>** URL's, a user might be able to access LDAP servers. It can be an undesirable consequence if your users are not supposed to access local LDAP directories directly.

Software distribution channels

Active Channels can be used to publish informations over HTTP(S) to users who have subscribed to given channel(s). The information can be refreshed automatically.
A channel is defined in a Channel Definition File (.CDF) accessible from a given URL.
The CDF file describes not the channel, only, but the way to represent it in the browser (icon, WEB page describing the channel content and purpose, etc.)
A user subscribes to channels

Channels can be used for software distribution, too. To define a software distribution channel, the CDF file contains Open Software Description (OSD) elements describing a software package to be installed. The package itself is a .CAB file containing the software itself.
Optionally, the .CAB file can include a .OSD file describing how to install the software.

OSD definitions can state if a package is to be copied on the users local disk or be installed directly automatically (then users are notified).

CDF and OSD files are made of XML code.

For a full description of CDF and OSD files, please read
http://msdn.microsoft.com/workshop/delivery/cdf/reference/channels.asp

And for a description on how to create software distribution channels, please, refer to
http://msdn.microsoft.com/workshop/delivery/osd/overview/osd.asp

But for the purpose of this paper, remember that if software channels are allowed in Internet Explorer, they can potentially install programs on the machines of your enterprise.

Cookies

A cookie can be sent to a browser from a WEB site for different purposes, typically :

- Maintain an applicative session
- « Mark » a user environment to remember that he visited the site before
- Store WEB application password…
- Etc.

When the user comes back on the WEB site, the server may query the cookie to the browser which returns it to the server for « interpretation ».
A cookie can be volatile or stored on disk. If it is supposed to maintain applicative, authenticated sessions, or contains a password, it is preferable that the cookie be volatile and sent over a secure session (e.g. over HTTPS - SSL).

Tip : Cookies containg a password or session ID's should not be stored on disk.

Ways to secure your browsing environment

Now that we've had an overview of what different technologies can do on our local machine(s), you can imagine what can potentially be done (and is sometimes done) by hostile code or scripts. If a script can call an ActiveX to read local files, the content of these files can potentially be returned to the WEB site serving the script. And if the local file were a copy of your local SAM in the repair directory ? Same question if the JVM let an applet access local ressources.

Notice that the same considerations are valid for mail user agents (MUA) tightly coupled to Windows and supporting Multimedia Internet Message Extensions (MIME). Such messages can carry the same content types. The only difference is the application transport protocol used (SMTP instead of HTTP(S)).

We will consider now some ways to **minimize the risks** of surfing on Internet from the enterprise.

System security

So far, most people in IT staff thought that the servers may have to be protected Desktop security was not a « priority », and is difficult to securize anyway, due to the many applications running on it.
But the desktop system security gets more important if your users can surf on Internet. By the way, isn't the desktop our entry point into all the information system ?

Minimum system priviledges.
Remember that mobile code has potentially as much priviledges as the user account has.
So, if not done, yet, give your users the access rights they **do** need, and not more. Typically, group membership and user rights determine the users priviledges.
To control the minimum priviledge rule, Windows 2000 security templates could be designed and imported into Group Policies. Start and test with Microsoft supplied templates, and adapt them to your desktops design.

Tip : The more priviledged a user is, the less she should go on Internet.

Create specific account for surfing, if needed.

Minimum system configuration
Install software componants that users need, and not more.
As an example, if your users don't need the ODBC driver on their desktop, don't install it. It can potentially be used by an ActiveX or an applet to access internal databases.

Latest system patches

Run an up to date anti-virus software

NTFS Access Control Lists
Make sure that the users accounts cannot modify system files or read sensitive informations they don't need to access directly (e.g. the SAM database).
To control the NTFS ACL's, Windows 2000 security templates could be designed and imported into Group Policies.
Start and test with Microsoft supplied templates, and adapt them to your desktops design.

Prevent/block surfing from enterprise servers
Most of time, they contain the data you want to save. See access control on proxies to prevent servers's browsers from reaching Internet.

Sites authentication and encryption

When conducting real business on Internet, make sure that the accessed sites have the right level of authentication and encryption. Most of time, both are achieved using SSL (https://…)
Site certificates are returned by secured WEB servers.
You have to define what Certification Authority (CA) are acceptable to your enterprise.
Certification Pratices Statements (CPS) should be read and evaluated, which is not legally easy. But as long as the « world » don't do so, site authentication should not be considerred as « legally » secured.
Make sure that the root CA in your browsers are the ones you trust.
Since Windows 2000 SP2, 128 bits encryption keys or 3DES are available for Internet Explorer. Use these encryption strengths.

Access control (and more) on proxies

Most of time, enterprises users don't surf on Internet directly from the browsers.
Proxies to Internet should be used. Some proxies just pass HTTP(S) trafic back and forth to Internet, while others can perform complex operations like :

- User authentication
- URL filterring
- Content scanning and filterring (doesn't work with HTTPS end to end)
- Bandwith control
- Control User Agent passing through the proxy.

These mechanisms are complementary to your desktop and browsers security settings.
For instance, file downloads in Internet Explorer is « allow, prompt or deny ». Assuming that users choose allow when prompted, it is « all or nothing » choice.
Adding a filterring proxy in between may mitigate the risk of dowloading files from

Internet. Same consideration for ActiveX dowloads.
URL filtering is more a « productivity » control than a security one.

Tip : log and publish users acesses statistics, instead of filtering URL's. It is an auto-regulator.
But check with your legal department and make sure users are aware that their Internet accesses logs are published enterprise wide, first.

Tip : Use proxies able to filter on the User Agent HTTP header and make sure that enterprise agents, only, are allowed to surf Internet.
The enterprise agents are those which settings comply with your security policies. Browsers on enterprise servers should not be allowed.
Windows 2000 GPO or IEAK let you add a substring to the User Agent string of the browsers.

Internet Explorer configuration

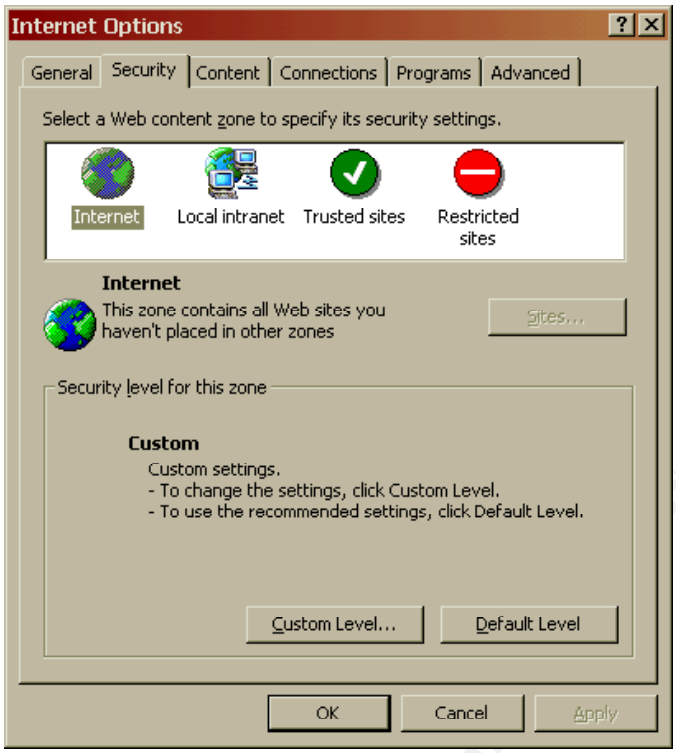
Internet Explorer has many security options to control what can be done within or from your browser. Let's have a look at them before jumping into the GPO configuration.

Security zones can be defined and have different security levels associated.
By default Internet Explorer is installed with 5 zones :

- **Restricted** (zone 4 in registry)
  - To map sites with high security risks
- **Internet** (zone 3 in registry)
  - All sites not listed in other zones
- **Trusted sites** (zone 2 in registry)
  - Internal or external sites that you may trust for content
- **Intranet** (zone 1 in registry)
  - Your local, internal servers (and all the ones you don't know inside ☺
- **Local host** (zone 0 in registry))

To display the security zones, start Internet Explorer, open the
Tools menu - Internet Options - Security tab**.**

As you can see, the local host is not displayed :



The only way to display the local host « zone » is using Internet Explorer Administration Kit (IEAK) editor, Windows 2000 GPO, or going straight into the registry.

By the way, you can find the zones definitions there :

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

The subkeys of « **Zones** » contain the security parameters of each zone, while the subkeys of « **ZoneMap** » define what sites or protocols are mapped to what zone.

Tip : Define a sixth security zone to differenciate official internal servers from intranet servers.

Your official internal servers are your production servers likely to be audited, with well identified and tested applications and antivirus protection up to date. If they are, you are sure that active contents are not infected, bugged or hostile code.
This may not be the case of all the intranet servers. For instance, development servers may contain uncomplete, bugged code, potentially dowlodable from anywhere in your enterprise.
Or « personnal » web servers may contain anything, depending on your enterprise policy on WEB servers deployment.

The Trusted Sites zone could be used to list your official internal sites, but in case you need special settings for Internet sites, a sixth zone could help. For instance, you may allow files (but no Activex) downloads from some Internet sites, while allowing ActiveX dowloads, too, from official local sites.

Here is a way to create an extra zone for your official internal servers :

1. Start regedit.exe
2. Go to **HKCU\Software\Microsoft\Windows\CurrentVersion\Internet**

Settings\Zones\2

3. Registry Menu – Export Registry File
4. Edit the resulting file with notepad.exe and save it.

   Change
   [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings**Zones\2**]
   into
   [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings**Zones\5**]

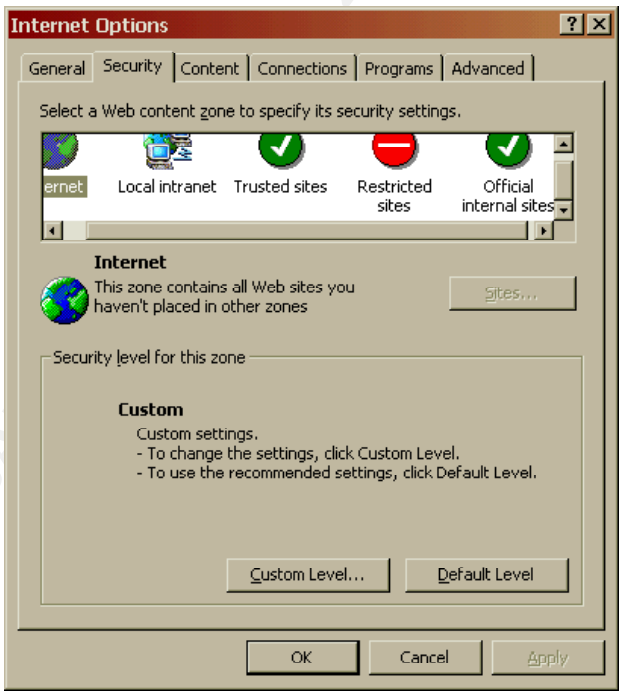
   Change "DisplayName"="**Trusted sites**"
   into someting like "DisplayName"="**Official internal sites**"

   Change
   "Description"="This zone contains **Web sites** that you trust not to damage your computer or data."
   Into something like
   "Description"="This zone contains **official internal web sites** that you trust not to damage your computer or data."

5. Start explorer.exe, double-click on the modified file and confirm when prompted to import the registry file.

6. Perform the same steps for **HKLM** instead of HKCU

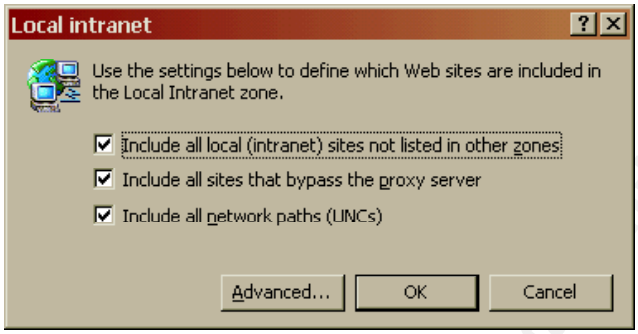
When done, Internet Explorer should display the new zone (see the new icon and descritpion on the right) :



Note : The usage of such an extra zone has been tested in production environments on NT4, but check with Microsoft if they still support you

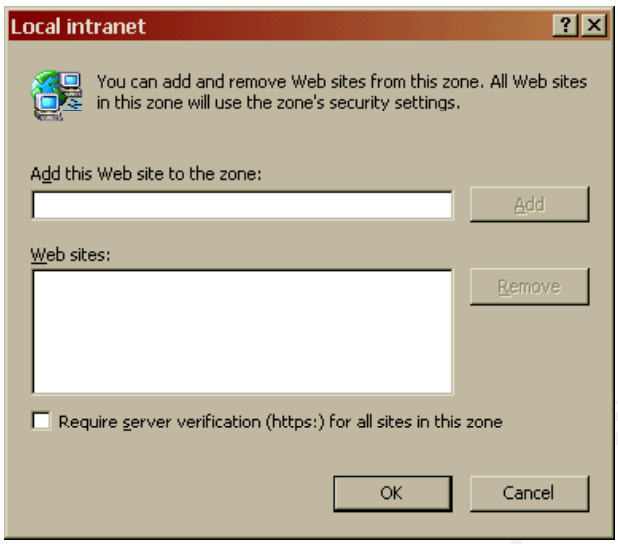
in case of troubles with Internet Explorer.

Now, for each zone, you have to choose what sites are part of it. The sites to zones mapping is under the ZoneMap registry key.
You can list specific sites for all zones, but the Internet one. The latter includes all the sites not listed in the other zones.
The intranet zone has special criterias to define what is part of the it. When you click on the site list, you get the following choices :



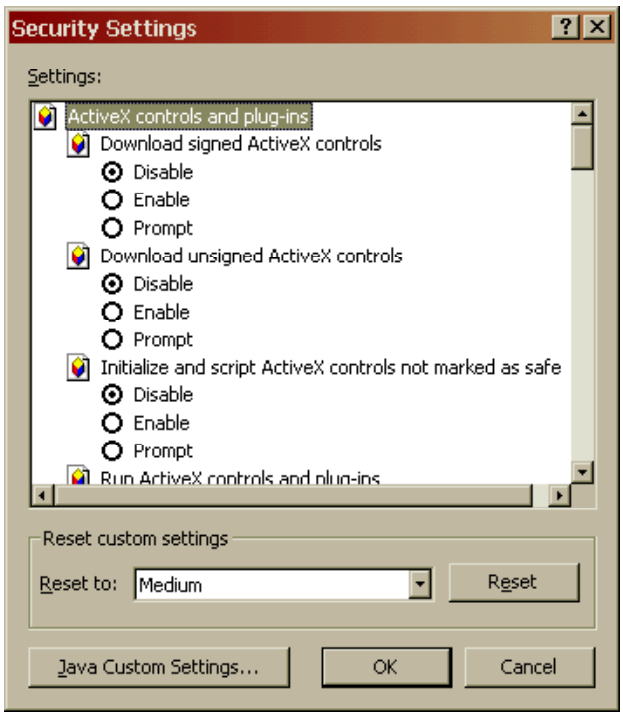
The boxes to be checked depend on your DNS namespace and proxy topology.
If the top one is checked, any URL with simple hostname (non DNS FQDN name) is considerred as part of the intranet zone.
If you decide to create a zone for official internal sites to differenciate them from intranet sites, may be should you uncheck the middedle box.

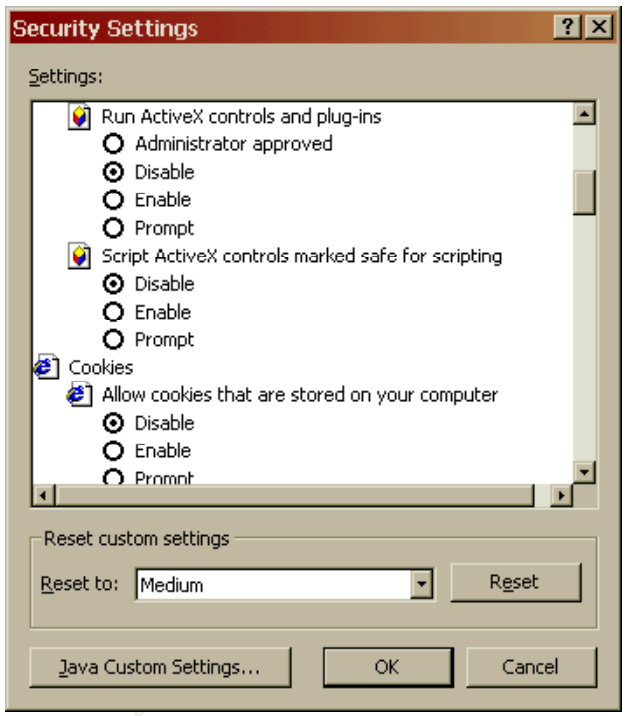
The Advanced button opens a dialog box to list explicitely sites or domains being part of the intranet zone :

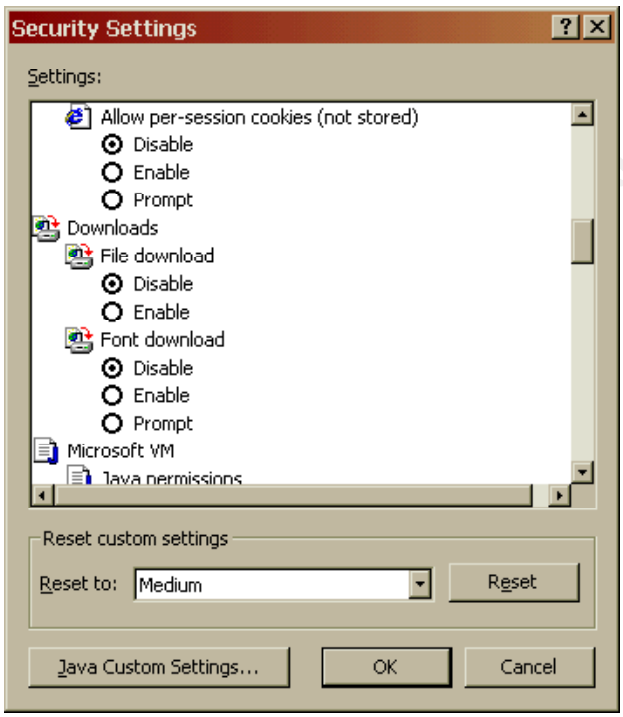


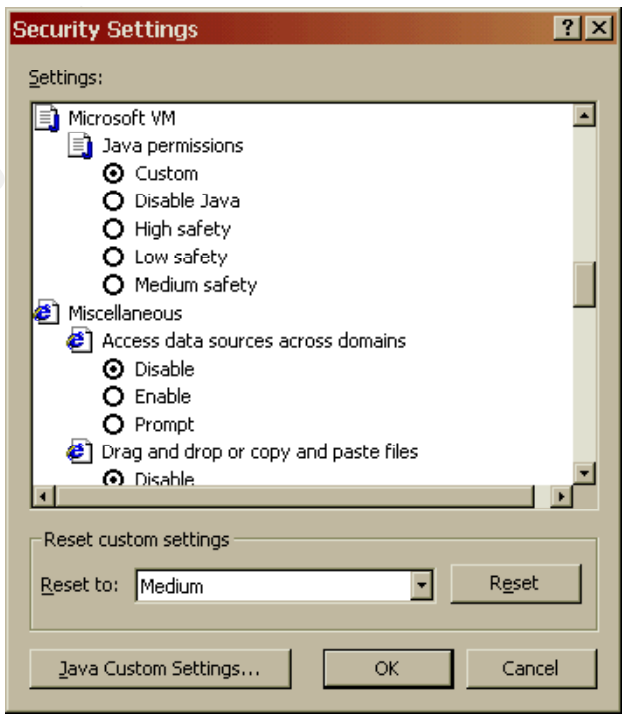
The same box appears when you click on the « Sites » button of the other security zones (but Internet zone).

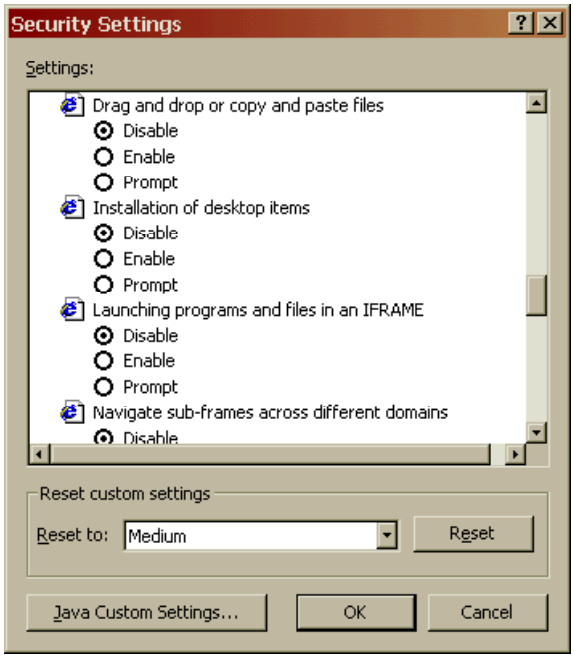
Here are the screen shots of the many security settings available **per zone** (look at the sections and remember what we've said previously on the different technologies) :

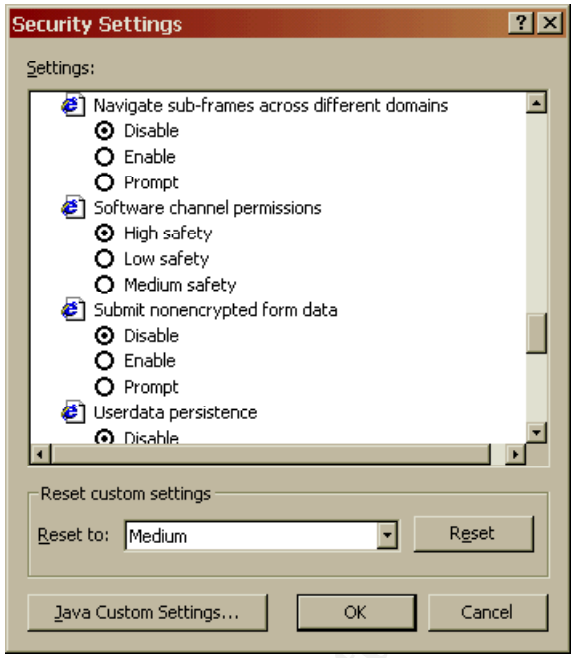


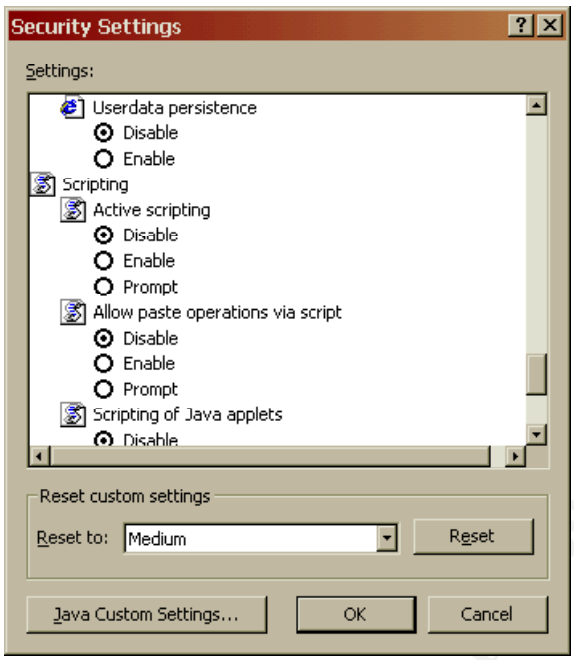


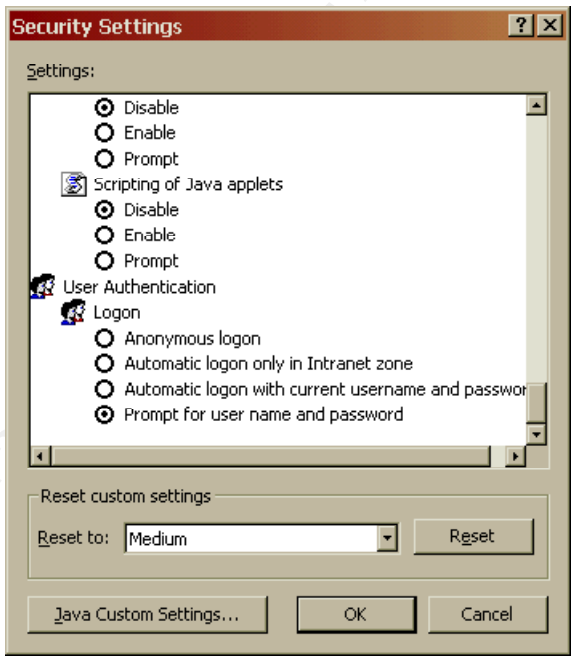




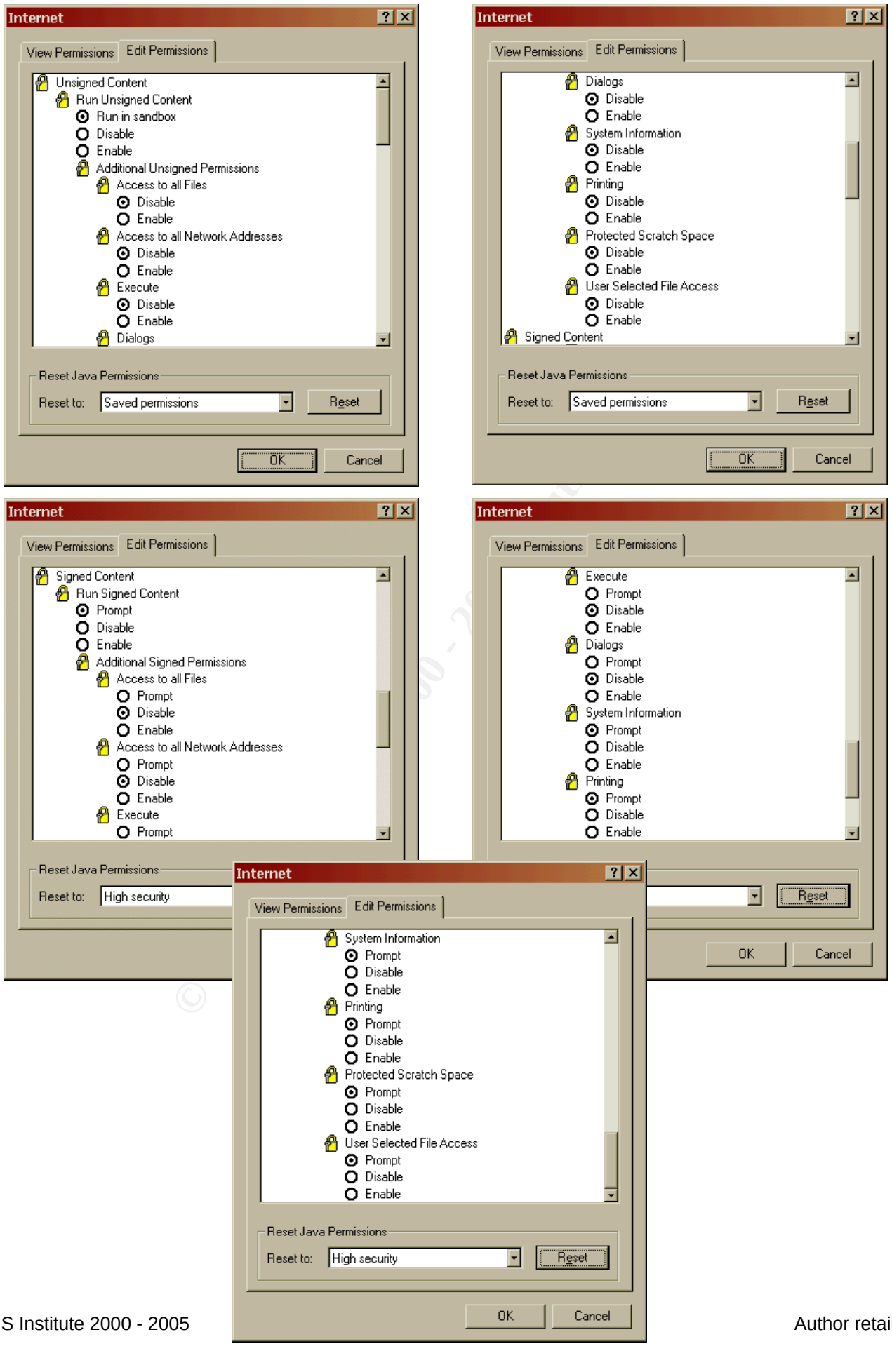








Here are the screen shots of the Java Custom Settings :



Notice that « High security » JAVA settings still let a user choose if a signed applet can access local files and/or network ressources.
Guess what an average user will choose between OK or Cancel.
I usually click OK until I get what I look for. Bad idea, right ? ☺

Tip : don't forget security education of the users if you let them surf on Internet from the enterprise.

Tip : regardless the zone, try to disable all I/O functions of the JVM.

The level of security of each zone depends on your **enterprise security policies**, if you have one. May be should they be reviewed to be « **e-business ready** » and support your decisions for the Internet Explorer security settings.

But remember what each technology (JAVA, ActiveX, etc.) can do before allowing such content to be downloaded ot activated, aspecially from Internet.

I would suggest not to allow any ActiveX downloads from Internet.
Even signed ActiveX should not be considerred more secure because they are signed, as long as the trusted root CA's and publishers are not «qualified » by your company.
Same for JAVA applets as long as your JVM prevent any local I/O's.

Here are some URL's which contain demonstration contents to test what can be done to your data (or even machine) from « hostile » code.
Try them **from a standalone machine** and play with your Internet Explorer parameters before deciding what you should enable or disable in the browsers of your enterprise. Then re-install the standalone machine clean, if needed ☺
Again : don't try them from your enterprise browsers as long as their security settings are not under control (who knows what these examples really content ?).

http://java.sun.com/sfaq#examples
http://www.finjan.com/mcrc/test.cfm
http://www.nat.bg/~joro/scrtlb.html
http://users.rcn.com/rms2000/acctroj/index.htm
(see references, too)

Your users will want to download Office and PDF files (at least) from Internet. Since files download is all or nothing choice in Internet Explorer, have filterring upstream proxies.

Tip : Such proxy should filter downloads (not HTTP requests) because you will want to call CGI ending with, say, the .exe extensions, but you don't want .exe files to be downloadable.

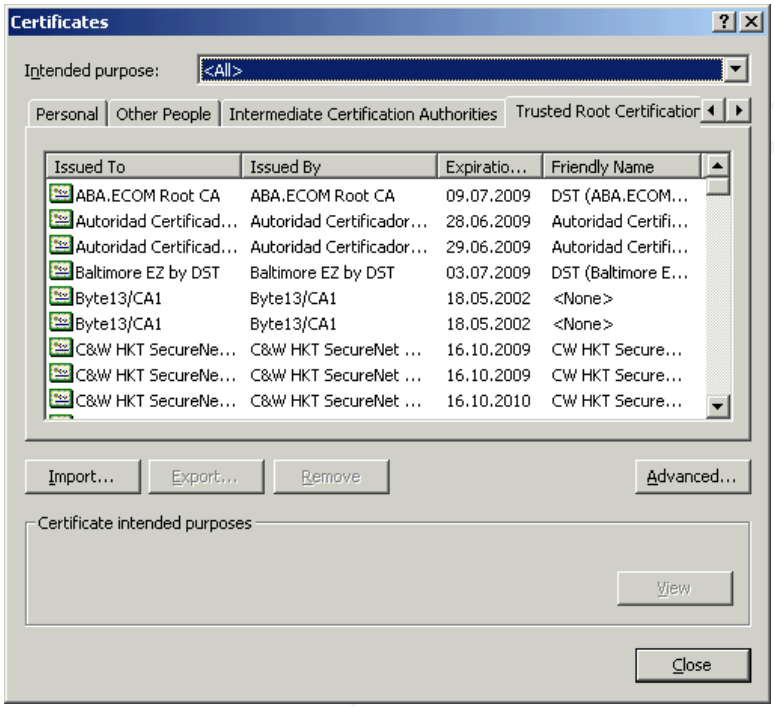
But the question is : what file types should I let come in ? Difficult to say, indeed.
I would suggest to list all extensions from HKEY_CLASSES_ROOT of a typical client PC that potentially have an application mapping. Block all of them on the proxy, **but** typical WEB contents (.htm, .html, .js, .asp, etc.) and the files types you want to dowload (.doc, .pdf, etc.)
Of course, the proxy will not filter downloads over HTTP**S**. Is your trusted root CA store up to date, according to your PKI policy ?

When you configure Internet Explorer, choose a base setting (Low, Low-Medium, Medium or High) and just change the options you want.

The next Internet Explorer windows are independant of the zones seen so far.
All the next parameters apply regardless of the zones.

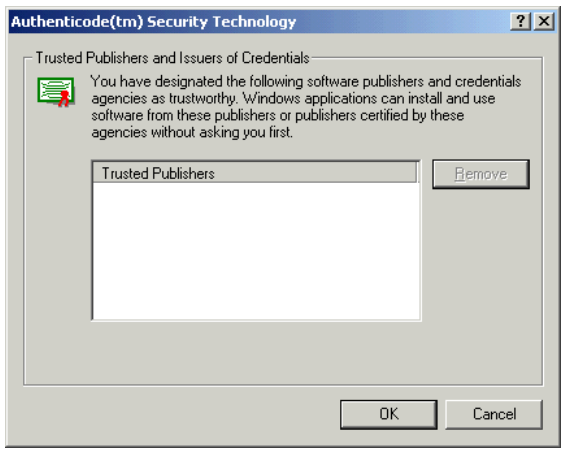
The Content tab is used to manage Internet Explorer certificate stores.
To get there : **Tools menu – Internet Options – Content Tab – Certificates** :

Internet Explorer has 4 different root stores : Personnal, Other People, Intermediate CA and Trusted Root CA.



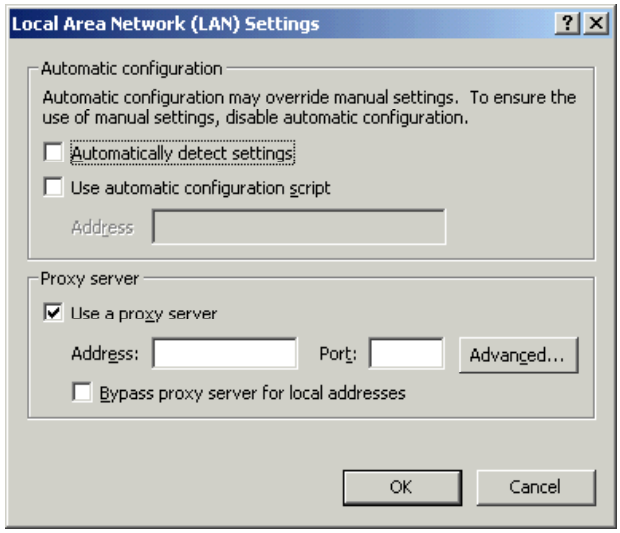
Tip : Intermediate and Trusted Root CA stores content should be controlled according to the enterprise PKI policies.
Enterprise users should not choose what CA is trusted by themselves.
So, remove (button) all but the ones you trust off browsers' stores and keep a copy (Export button) for later re-integration(Import button) , if any.
We will see later how to do so from a central point.

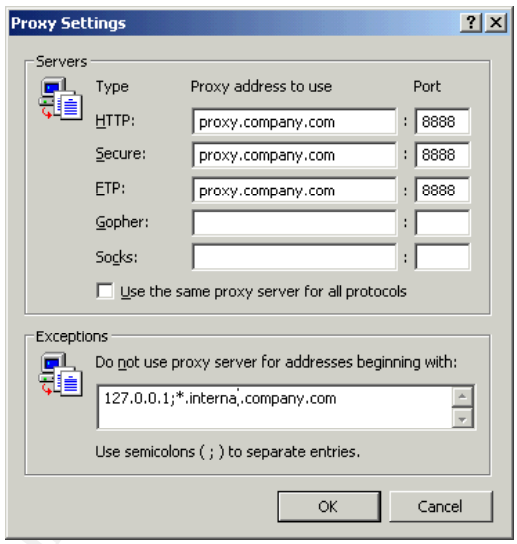
Tools menu – Internet Options – Content Tab – Certificates
shows the trusted software publishers, if any :



The text in the pop up Windows implicitely suggests that Enterprise users shouldn't be able to change the content of this store since any code signed by the publishers whose certificate is listed there could be installed under the covers.

Tools menu – Internet Options – Content Tab – Connections leads to the proxy settings. Make sure these settings point to your official enterprise proxy to Internet.

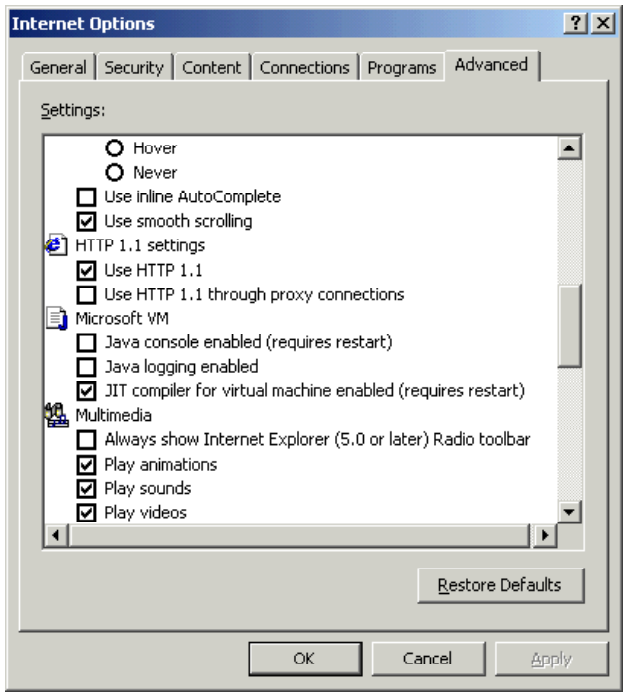


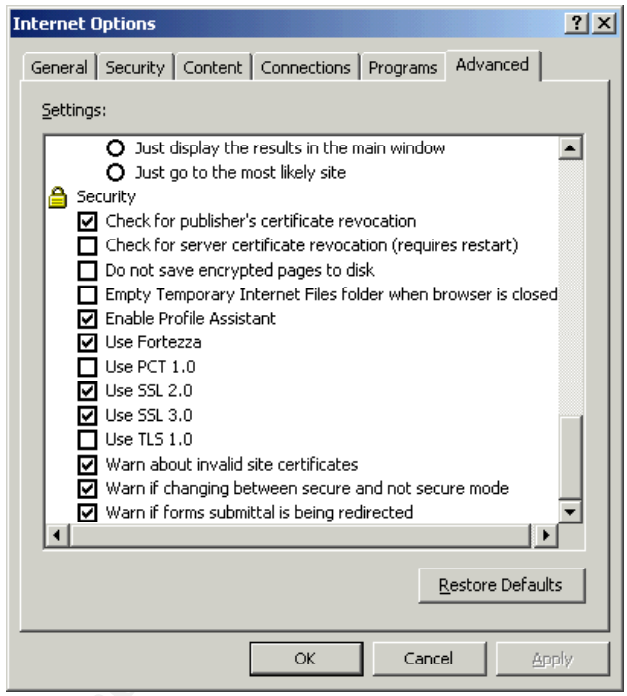


Notice the proxy exceptions on the right window. Remember that these exceptions can be automatically included in the intranet security zone. If you don't want so uncheck the respective box in the definition of sites of the intranet zone.

Tips : automatic settings shoud be disabled so that your central configuration will not be overwritten.

Finally let's get to the **Tools menu – Internet Options – Advanced** tab :





As you can see, several settings impact the security level of Internet Explorer.
On the left screenshot, HTTP 1.1 can be enabled or disabled (via proxy or not).
Some proxies or WEB servers still don't work fine with HTTP 1.1. Even venerable firewall vendors have some troubles with their transparent proxies over HTTP 1.1.
And from a security perspective, remember that HTTP 1.1 is able to maintain persistent TCP/IP connections between the browser and a given WEB site. Good to minimize TCP handshake overhead, but couldn't such persistent connexions be ideal to maintain a hacker session ?

On the right hand side, a whole set of security parameters can be set.
Checking for publisher's certificate revocation may lead to troubles if no URL is provided in the certificate to be checked or if the URL is unavailable.
Same consideration for the site certificates.
Not saving encrypted pages to disk is a good habit, as well as emptying the local cache when the browser is closed.
The last three boxes should be checked, too, but the warning messages are usefull to **educated users**, only.

When your security settings are defined, it is time to apply these settings to all the browsers within your enterprise.

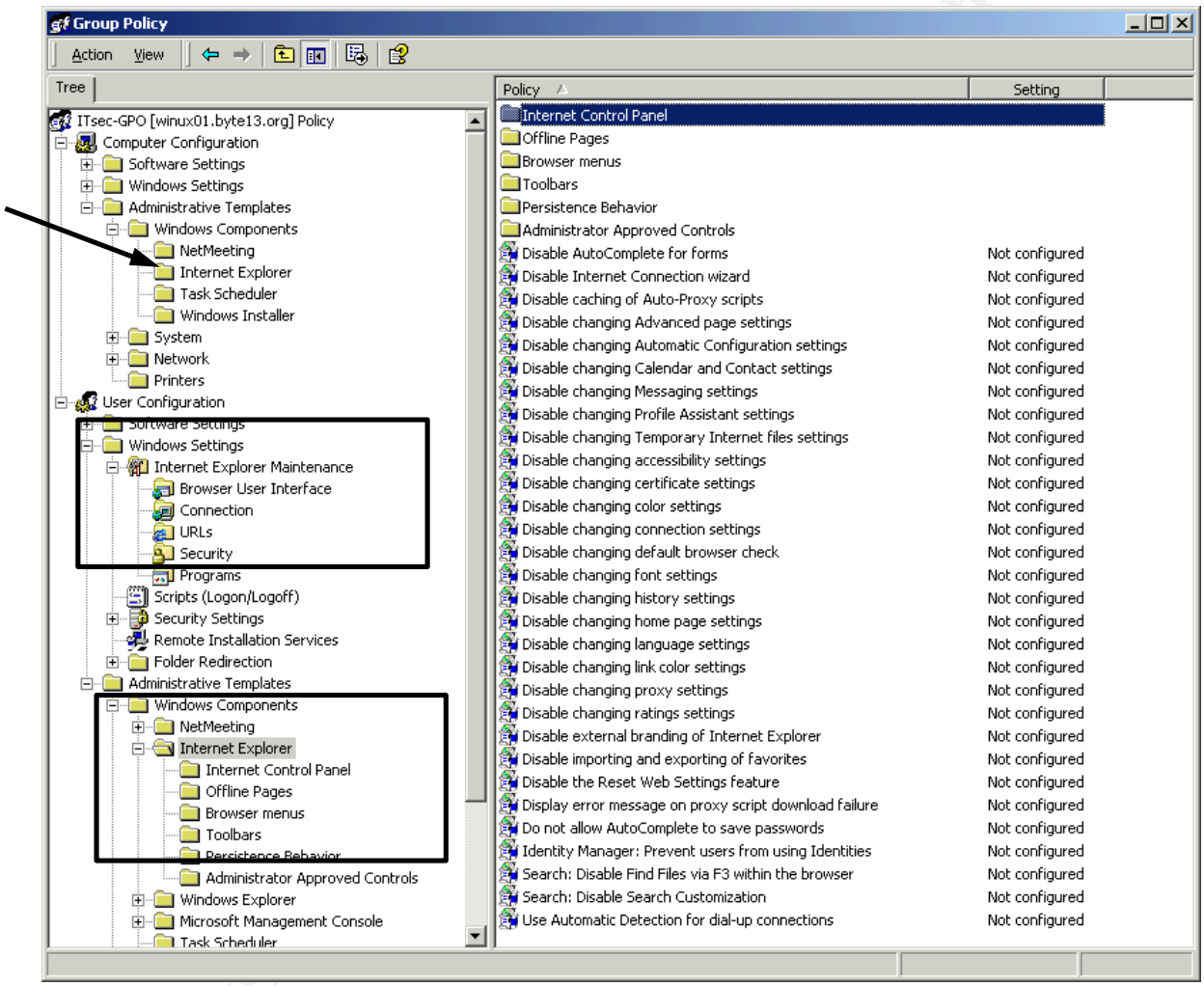
So let's see how Windows 2000 helps in managing the configuration of Internet Explorers within your enterprise from a central point.

Configuring the browsers centrally

Configuring the browsers with Group Policies

When your Internet Explorer security policies are defined, they can be applied in Windows 2000 Group Policies (GPO).

The next screen shot shows the GPO nodes containing Internet Explorer setting.



As the menu suggest, the GPO can set more Internet Explorer parameters than just security parameters, typically what menus and tool bars are available to the users.

Let's concentrate on security settings.
First, log into an account from which the GPO will be defined. Obvious ? Yes, but the first thing to start is…Internet Explorer, not the Microsoft Management Console (MMC), yet.
Choose an account and a machine which implement no Internet Explorer GPO.
You need full control of Internet Explorer to setup the GPO.

Now go into the secure zone windows of Internet Explorer, set your security policy and include sites, if any, into the respective zones.

Purge all root CA's and publishers you don't trust (Content tab – Certificates) to reflect what CA's the GPO will trust.
When you are done, start the Microsoft Management Console (MMC) and load the AD Users and Computers snap-in.

Suppose that your Internet Explorer policy applies to all the users in a given OU.

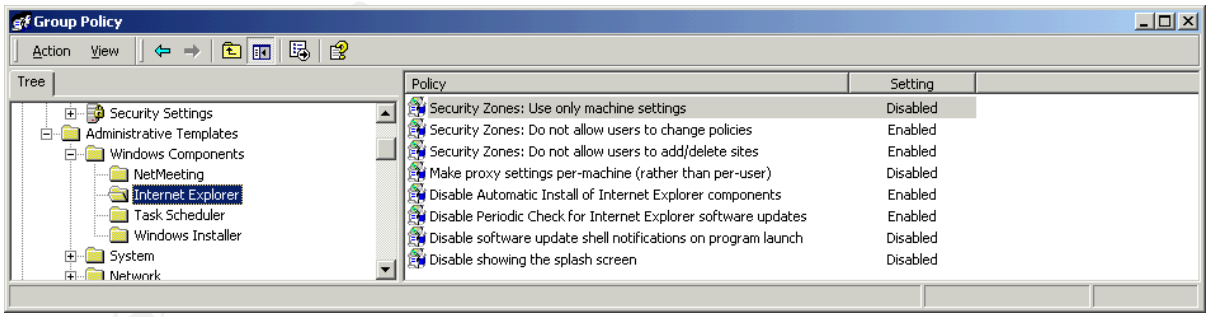
- Expand AD Users and Computers node on the left pane,
  right-click on the OU name and
  choose « Properties ».
  - Go onto the Group Policy tab.
    If you have a GPO for this OU, already, add (button) it, if not done yet.
    If no GPO exist or you want to make a specific one for security settings, click on New button and give your new GPO a name.

Tips : define a GPO which includes all security parameters (system and Internet Explorer). This GPO may be managed by the IT-Security department of your enterprise.

Now select the GPO from the list, Edit (button) it and go to
User Configuration – Windows Settings – Internet Explorer Maintenance – Security

- Double-click on Security Zones and Content Ratings in the right pane
  - Select Import current security zones setting
    - Click Modify button
      At this step, you will see the security zones you have just setup in Internet Explorer, as well as the local host zone (you didn't see the latter in Internet Explorer, remember ?)
      You can still adapt the current settings to your policy ; but remember that if you do so within the GPO, your local browser will not reflect the changes.

Other security options are available through GPO's. Let's review them :



If you need Internet Explorer profiles for different types of users, you probably don't want to use machine settings, only. Machine settings affect all users of a given computer. The configuration wouldn't be per user anymore.

You definitely want to prevent users from changing their policies.
You have to control the security level within the enterprise. You don't want either that users add or remove specific sites or domains from the security zones definitions.
Becarefull with the negative form of the setting statement ; you often need to Enable a setting to prevent users from doing things.

Most such settings are allowed by default ; so read the definition carefully.

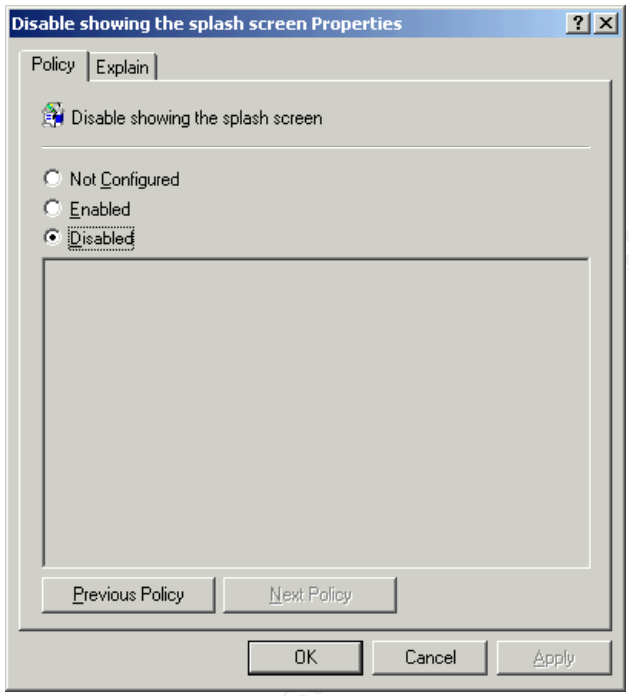
Proxy settings per user may be relevant if you have several proxies in your enterprise. It may be the case in companies with geographically dispersed branches or offices. If this is the case, make sure the proxies are under control and conform to your enterprise security policies.

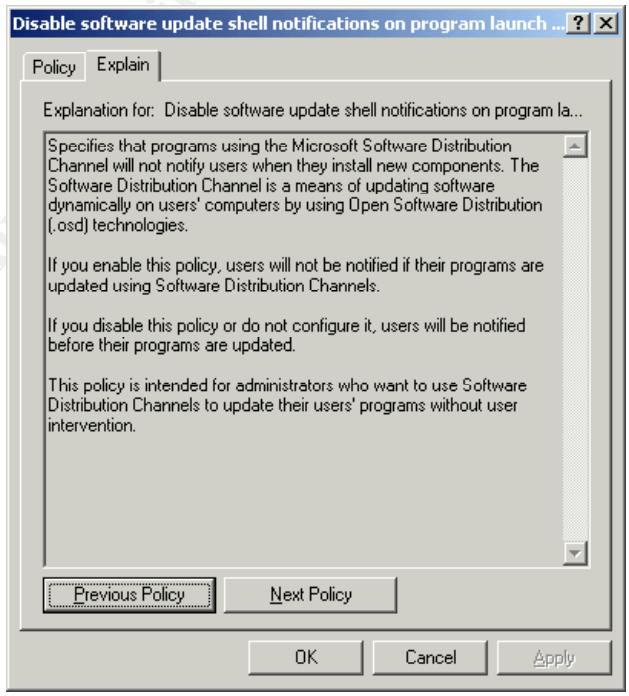
Keep automatic updates of Internet Explorer disabled. You want to control the version of the browsers in the enterprise. But keep up to date with patch releases.

Software update shell notification prompts the users in case a software channel downloads a package to be installed. If disabled, the package is installed silently…

The splash screen displays the program name, licensing and copyright information.

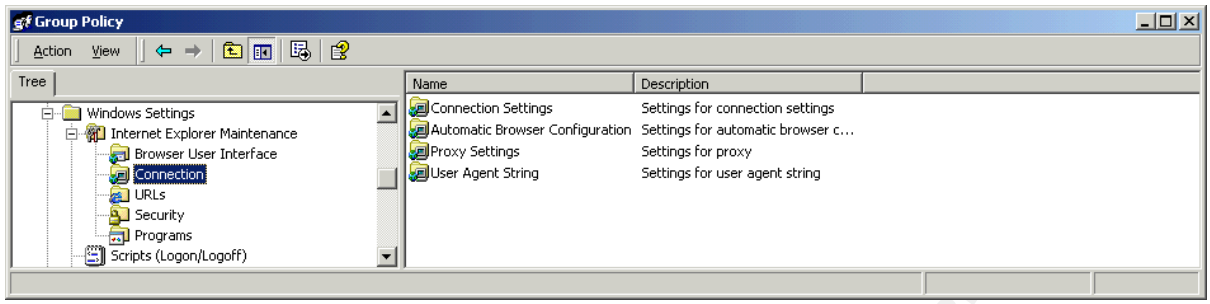
If you double-click on one of the settings, the following window pops up :



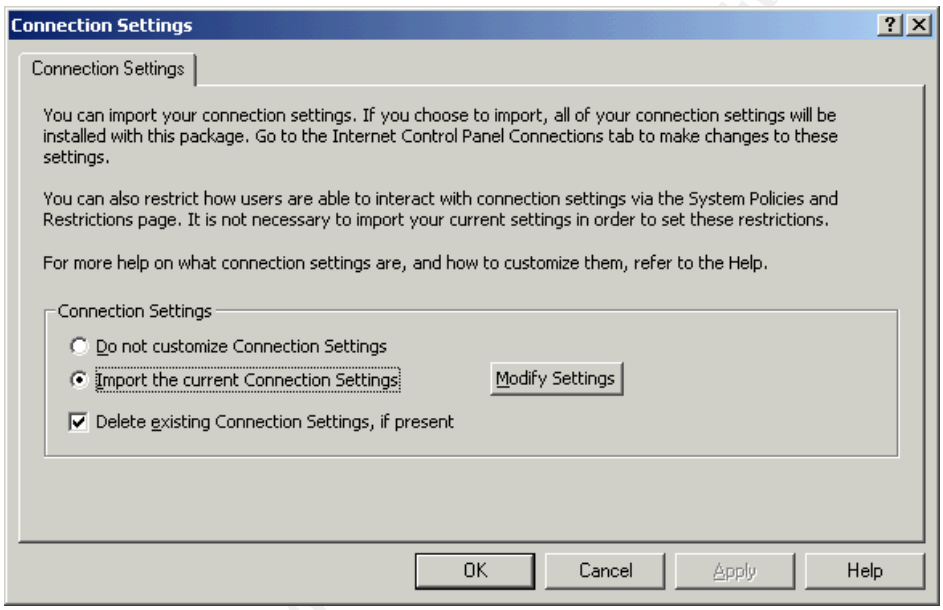


To know how each option changes the setting, select the « Explain » tab and read the explanation.

Here is another menu related to security settings :



Connection Settings can import the current Internet Explorer settings, like security zones setting does. Double-click on Connection Settings :

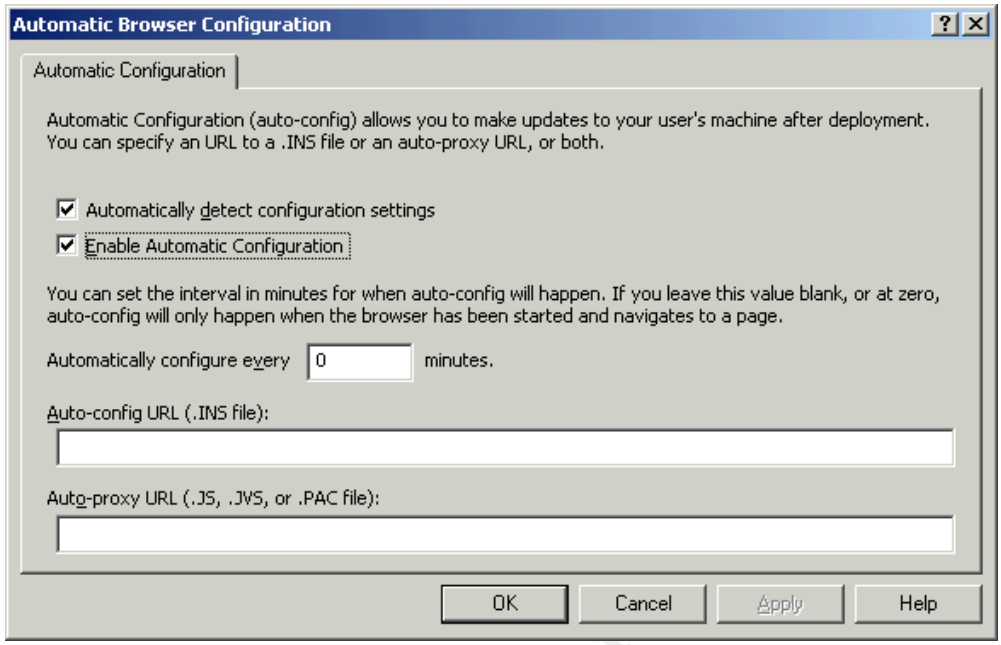


If you want to make sure that your enterprise settings overwrite previous proxy settings, check « Delete existing Connection Settings …»

If you don't want to import proxy settings from your current browser, you can use the next two options (Automatic browser config and Proxy settings). If enabled, they overwrite the imported settings.

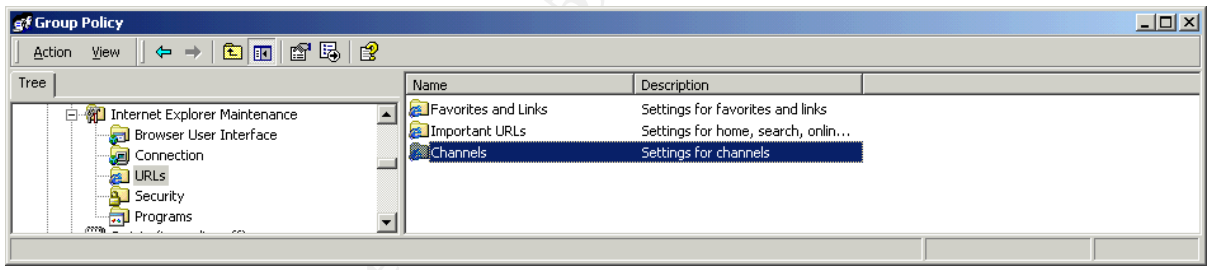
The User Agent setting is the one to add a strings to the user agent HTTP header. This is the string you want to test on your proxy(ies) to make sure that employees surfing Internet use browsers configured with your enterprise security settings.

Double-click on the Automatic Browser Configuration and you get to the following window :

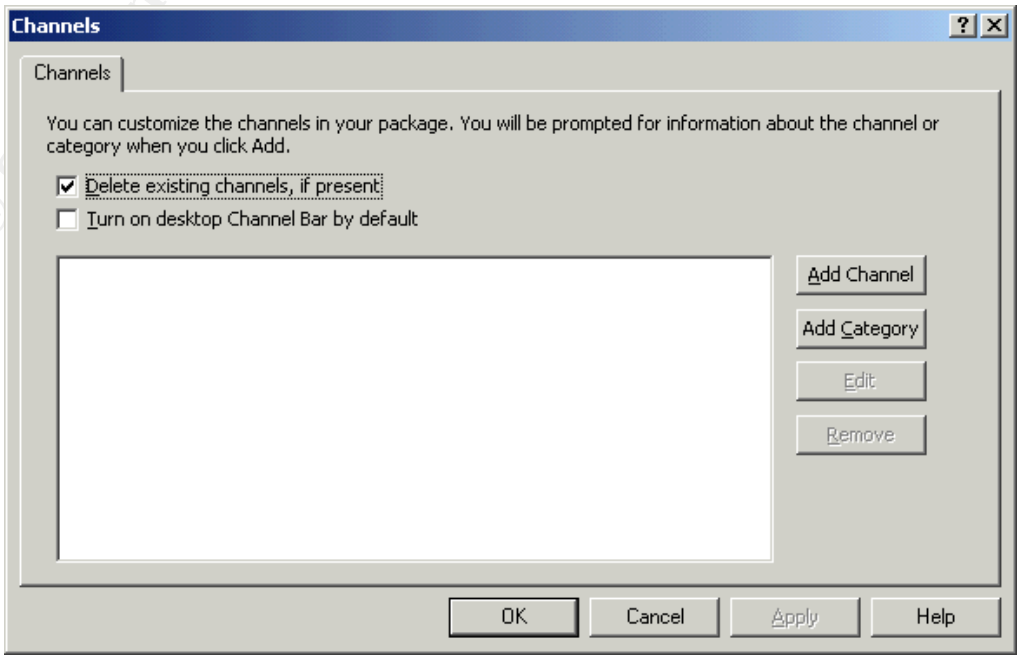


Enable Automatic Configuration is an alternate way of configuring your browsers, using the Internet Explorer Administration Kit (IEAK). See the section on IEAK.

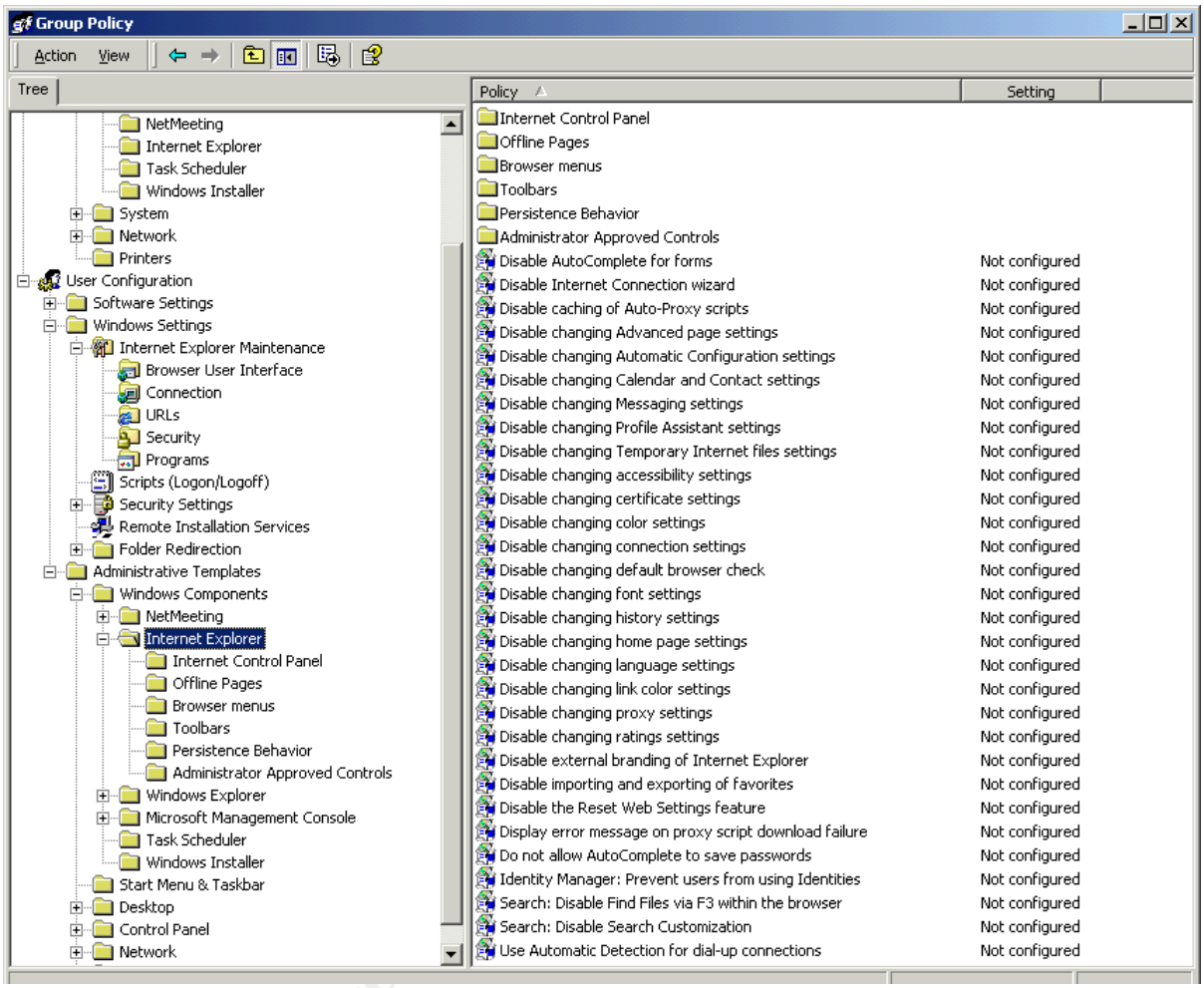
Software channels can be defined or deleted in the following menu :



To disable active channels (to avoid automatic download and/or installation of softwares) check the following box :

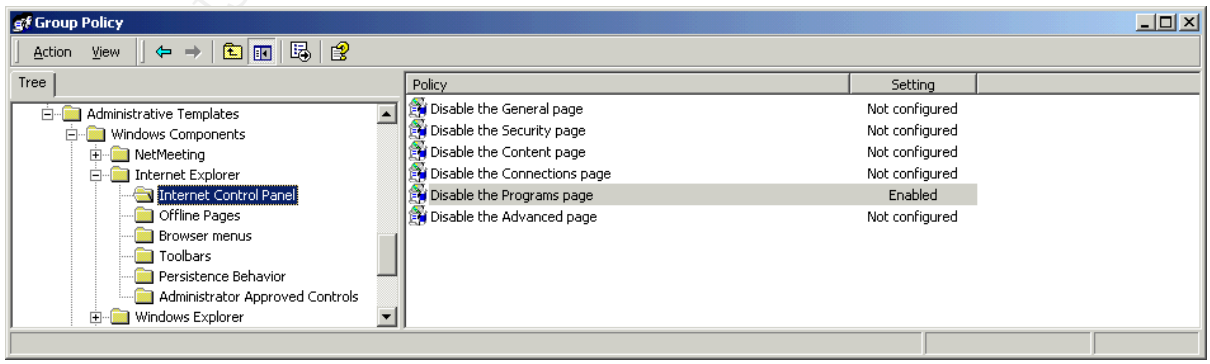


The Administrative templates in the user section of the GPO let you choose what menus and options are available to Internet Explorer users after they are configured by the GPO.
Many options can be set and it is up to you, according to your security policy, to choose what users can or cannot change :

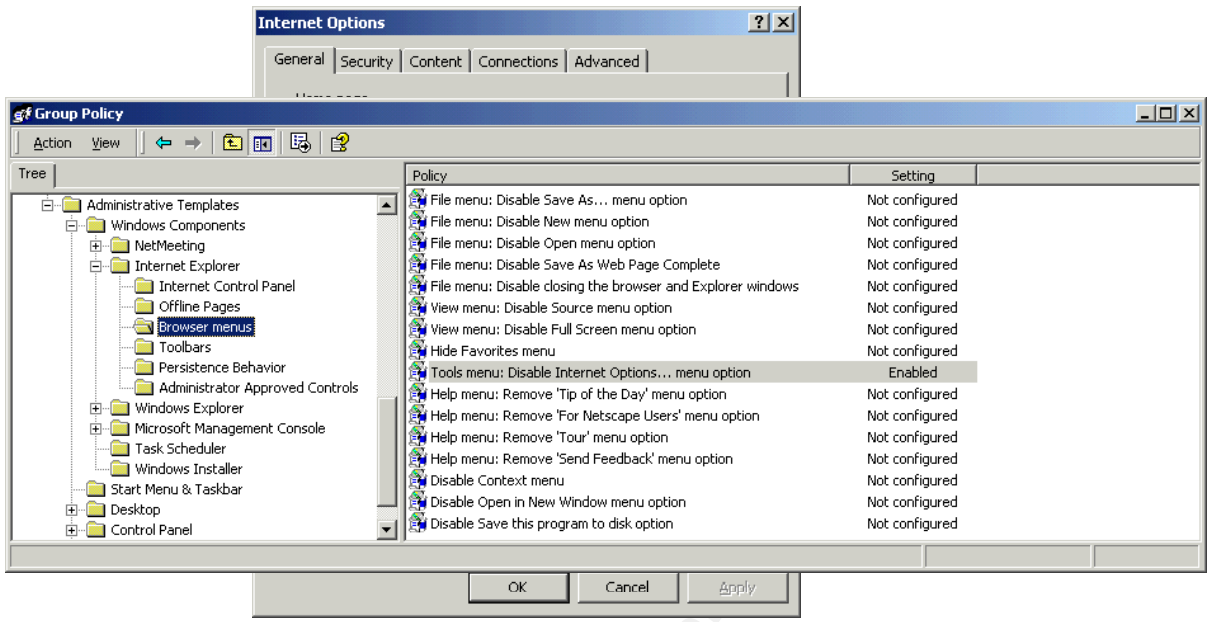


Typically, you don't want them to change their advanced settings, neither the proxy settings, nor their certificates settings, and the like.

The next menu can be used to completely hide the Internet Explorer setting tabs :

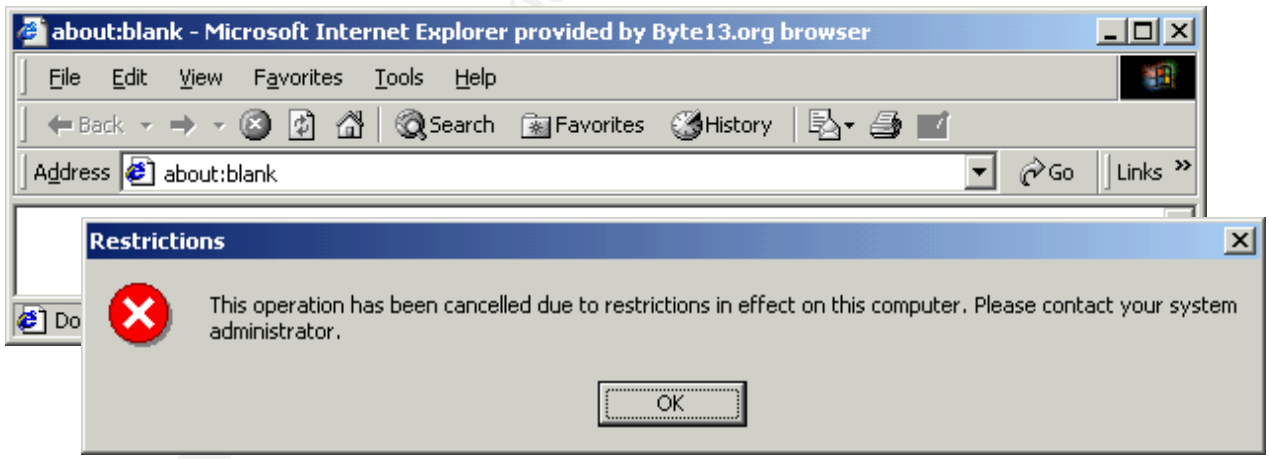


For instance, if you Enable « Disable the programs page », the Programs tab of the Internet options will disappear :

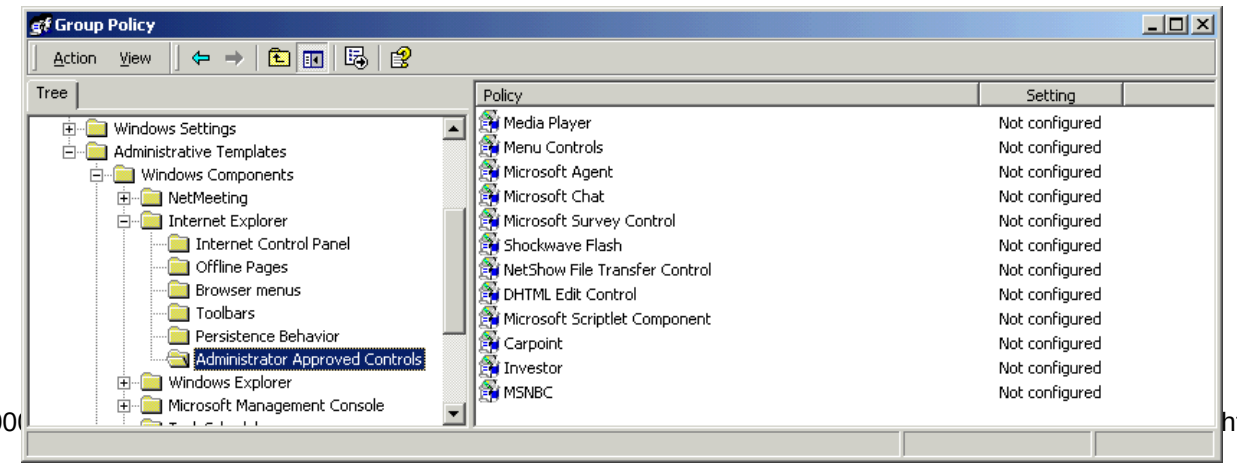


The Internet explorer GPO can be used to hide menus of the browser (windows or contextual menus) :

This example (Enable the « Disable Internet Options… ») will open the following pop up when the user tries to open **Tools – Internet Options** :



Maybe did you notice on the security zones screen shots that some ActiveX (Administrator approved), only, may be allowed for execution.
The following menu is where you define what are the « Administrator approved » controls :

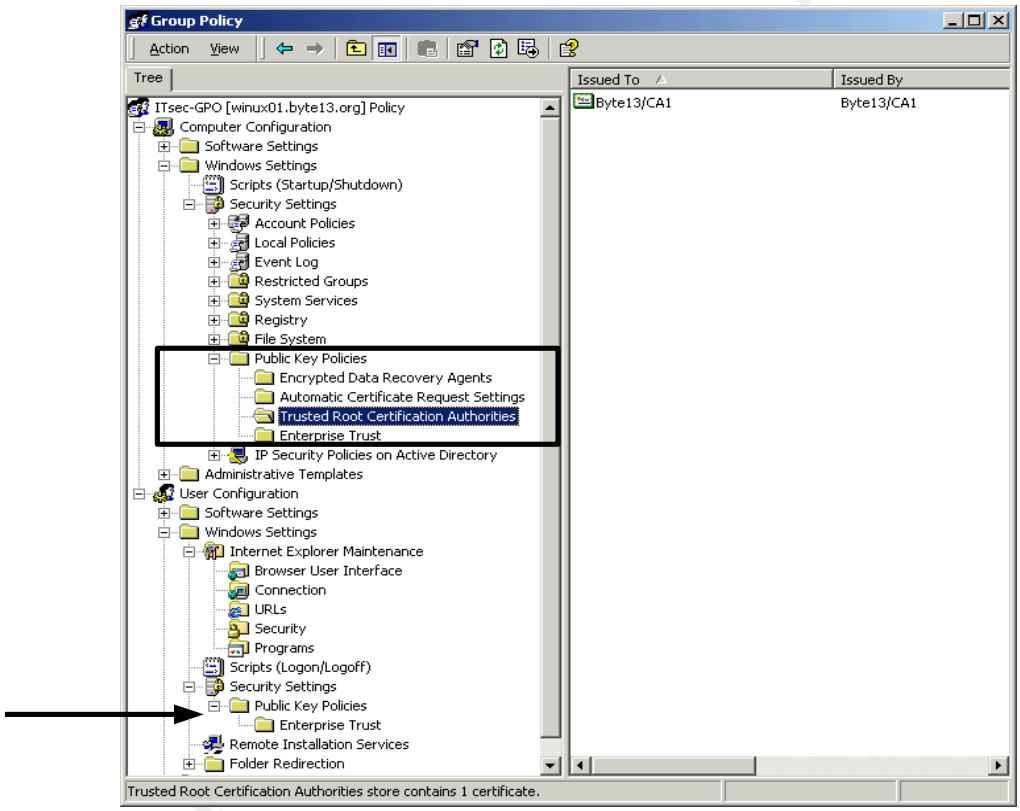


CA certificates

As we've seen, several security settings eventually depend on digital signature :

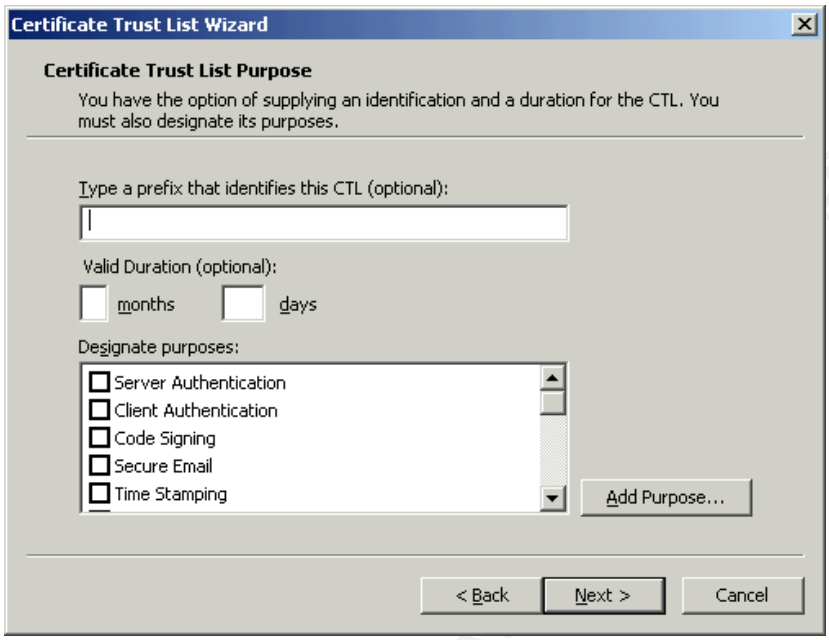
- Software channels
- Download of ActiveX controls
- Download of JAVA applets
- Identification of WEB sites
- Etc.

For a signature or site to be verified, trusted root CA's certificates should validate the publishers or sites's certificates.
So the root CA store is an important security setting. It lists what root CA('s) your enterprise trusts. Here is where certificates stores are managed via GPO :



You can manageTrusted Root CA stores and Enterprise Trusts.
Right-click on **Trusted Root CA** and choose **Import** (only choice under All Tasks).
You can import certificates in PKCS#7, PKCS#12 or .SST files format.
All purposes « certified » in the imported root CA (e.g. mail signature, code signing, etc.) are then accepted.

If you want a finer control on what a given CA is accepted for, use Enterprise Trust setting. When you right-click on it, you can create a Certificate Trust List (CTL) including all root CA certificates that you accept. But you can specify for what purposes the CTL is accepted as you can see if you start the **wizzard (right-click Enterprise Trust – New)** :



As we see CTL can have a lifetime, too.
The wizzard will lead you to sign the CTL with a CA key of your choice.
The GPO supports CTL per machine or per users.

Users categories

We have just reviewed the many GPO settings which control the security level of Internet Explorer.
But you may need different browser settings for different type of users.

The following paragraphs suggest some criterias which differenciate your users. You probably have your own perception of the needs of each category of users; the idea is just to make you think about it.

Business
Typically very end users who have nothing to do with IT services (but asking support to them !).
They use Internet for non technical business purpose, only.
You want them to surf from browsers with security settings compliant with the enterprise security policies.

Technical support (IT staff)
Supposed to have a better understanding of WEB technologies and risks.
They need to download patches and access technical services.
They shouldn't need control on their browsers' security settings when adequately setup.
You want them to surf from browsers with security settings compliant with the enterprise security policies.

Development
Most of time, they need « everything » otherwise they cannot work.
They test WEB technologies to make solutions.
You want them to surf from browsers with security settings compliant with the enterprise security policies.
But they need « free » environements to do their job.
If they need to surf Internet from the development environment, may be should it be part of a DMZ or be disconnected from the rest of the enterprise, with their own Internet connexion.
If they don't need to go to Internet from the development environment, make sure that the proxy prevent their access from browsers not configured centrally, according to your security policy.

Others
Contractors, consultants, etc.
Should not be allowed to surf Internet from within enterprise with their laptops.
They should use enetrprise desktops or laptops with security settings compliant with your security policies.

When the categories of users and respective needs are identified, you can create one GPO per security level.
You can apply the right GPO to the right persons, either by **OU membership**, or by applying **access control lists** (ACL) on the respective GPO objects.

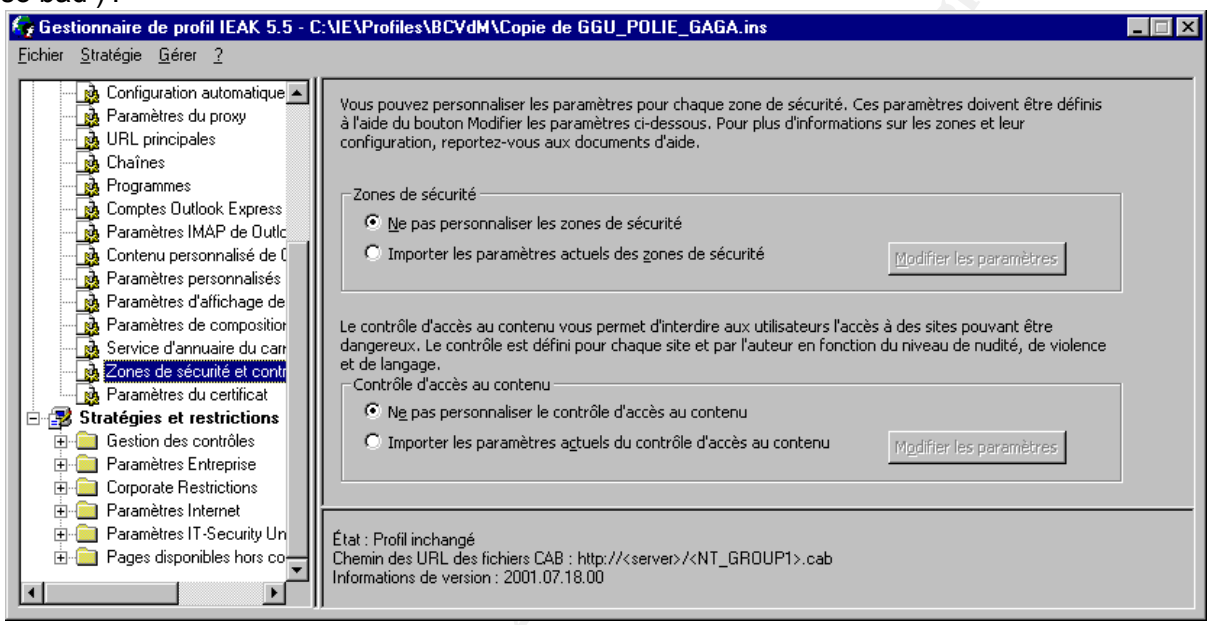
Remember that cumulated GPO's may have a negative impact on machine startup and logon times. If you control GPO enforcement by ACL, remember that to prevent a Windows group from applying a GPO, just clearing the **Apply** right is not enough ; the GPO would still be processed. To save this processing time, clear the **Read**

permission, too, on the GPO object.

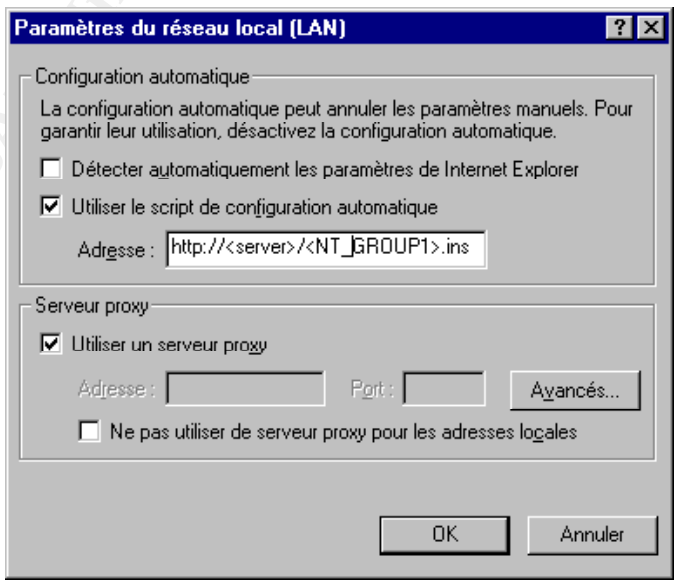
IEAK

Windows 2000 Internet Explorer GPO's work with Windows 2000 clients, only.
What can be done for other Windows (or even Unix !) clients
running Internet Explorer ? Internet Explorer Administration Kit can be used.

With IEAK, clients get their configuration over HTTP instead of, with GPO's,
LDAP and CIFS (SYSVOL).
IEAK is a GUI similar to system policy editor (it is one actually since it uses .adm files).
Here is the French version of it (I'll change it asap – so now you know why my English is so bad) :



Instead of generating a ntconfig.pol file, it produces a .INS file and one or more .CAB files referred by URL in the .INS file. The .CAB file(s) contains a set of .INF files with the registry settings.
When your configuration is ready, put all these files on an internal WEB server, and specify the URL to the .INS in Internet Explorer
(**Tools – Internet Options – Connexion – LAN Settings**) :



The above example suggests to specify an filename based on a Windows groupname.

Logon script could detect the « NT_GROUP » a user is part of and automatically set the registry key to configure the browser :
HKCU\Software\ Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL

If you do so, you can create profiles for your different categories of users, and just playing with Windows group membership can control the security level of a given user.

Tip : Predifine at least a low, a medium and a high security profile that you can switch to in case of need.
A business may have an urgent need to access a site with ActiveX, so switch to « Low » security if you dare.
Or an alert on Internet may indicate a serious security whole in, say, the Microsoft JVM, which makes you decide to switch your browsers to a high security profile (say with no JAVA) while waiting for your enterprise browsers to be patched.

With IEAK, the configuration is downloaded when Internet Explorer starts up.
If the configuration files have changed, they will ne downloaded again.
You can set an automatic refresh interval so that the browsers can be updated without having to restart them.

IEAK can control more settings than current GPO's (even other applications like Outlook), nottably the Internet Explorer « Advanced » tab settings.

Tip : If you plan to use IEAK for Internet Explorer settings, only, leave the following .adm files in %SYSTEMDRIVE%\Program Files\IEAK\policies\En (directory may change if you install IEAK somewhere else) :

- **axaa.adm**
- **inetcorp.adm**
- **inetres.adm**
- **inetset.adm**
- **subs.adm**

and remove the other .adm files.

Like with GPO, security zones settings can be imported from the current browser.
GPO has its own settings for certificates stores, but IEAK imports them from the current Internet Explorer.

But be very carefull when you change settings with IEAK. The GUI is very sensible. Clicking in a gray area could select a checkbox.

And we have seen some strange behaviour when you run concurrent instances of Internet Explorer configurred over IEAK. Zone membership of a site sometimes gets screwed up when two Internet Explorer processes are executed by the same user on the same machine.

Summary

We have seen WEB technologies and their security implications in clients centric attacks.
Some Internet sites have been mentionned for you to test if these technologies can really access local ressources within your enterprise.
Then Internet Explorer security settings have been reviewed, as well as security principles which reduce the risks.

Then GPO's used to control enterprise broswers settings have been reviewed.
Finally IEAK has bee introduced as an alternate tool to control enterprise brosers centrally.

Conclusion

Absolute security is not possible if an enterprise wants to be connected to Interrnet and conduct e-business.
However, system administrators and IT-Security staff have to understand the implication of opening such accesses to corporate employees.

Browsers security settings should be controllable centrally and quickly in case serious and massive Internet threats appear.

Windows 2000 GPO and IEAK are typical tools that you need for such control.

References

XML specifications :
http://www.xml.org
How Internet Explorer determines a file type :
http://msdn.microsoft.com/library/default.asp?url=/workshop/networking/moniker/overview/appendix_a.asp?frame=true
Active Channel definitions :
For a full description of CDF and OSD files :
http://msdn.microsoft.com/workshop/delivery/cdf/reference/channels.asp
How to create software distribution channels :
http://msdn.microsoft.com/workshop/delivery/osd/overview/osd.asp
URL containing « hostile » codes (to be used from test machines, only – see text) :
http://java.sun.com/sfaq#examples
http://www.finjan.com/mcrc/test.cfm
http://www.nat.bg/~joro/scrtlb.html
http://users.rcn.com/rms2000/acctroj/index.htm
Online audits for a fee : http://www.securitytour.com
IEAK homepage :
http://www.microsoft.com/windows/ieak/en/default.asp
Java versus ActiveX security :
http://www.cs.princeton.edu/sip/faq/java-vs-activex.html
http://www.cs.princeton.edu/sip/faq/java-faq.php3
Hacking Exposed, second edition chapter on « Hacking Internet Users »
ISBN 0072127481