

[How can I check if 128-bit encryption is being used?](#)

[What can I do if I find that 128-bit encryption is NOT being used in the Netscape Navigator browser?](#)

[How can I assure myself that I am connecting to BNP Paribas Connexis and not other parties?](#)

[Can I exit by closing the browser window?](#)

[What if I forget my password?](#)

[What is User ID?](#)

[Can I change my User ID and Password?](#)

[How secure is your Internet banking service?](#)

[If I suspect there are unauthorised transactions in my account, what should I do?](#)

SECURITY TIPS

INTERNET EXPLORER SECURITY SETTINGS

How can I check if 128-bit encryption is being used?

For Microsoft Internet Explorer,

- Move a mouse over the 'security lock icon' at the lower right hand corner. A tool-tip of '**SSL secured (128-bit)**' should pop up
OR
- Right-click any text on a page (not on a graphics object) and select 'Properties'. '**Connection**' with '**SSL 3.0, RC4 with 128 bit encryption (High); RSA with 1024 bit exchange**' is shown
OR
- Press 'File' in the toolbar and select 'Properties'. '**Connection**' with '**SSL 3.0, RC4 with 128 bit encryption (High); RSA with 1024 bit exchange**' is shown.

For Netscape Navigator,

'**Security**' with '**This is a secure document that uses a high-grade encryption key for U.S. domestic use only (RC4, 128 bit)**' is displayed if you.

- Press 'Security' in the toolbar. Then a 'Security Info' window will be displayed and click 'Open page info'
OR
- Right-click any text on a page (not on a graphic object) and select 'View info'.

[Top](#)

What can I do if I find that 128-bit encryption is NOT being used in the Netscape Navigator browser?

You should configure the settings in the browser to ensure 128-bit encryption as follows:

- Press 'Security' in the toolbar
- Click 'Navigator' in the left column
- Press 'Configure SSL v3' on the right of 'Enable SSL (Secure Sockets Layer) v3'
- Enable all ciphers except 'No encryption with an MD5 MAC'

[Top](#)

How can I assure myself that I am connecting to BNP Paribas Connexis and not other parties?

For Microsoft Internet Explorer,

You may check the validity of the certificate as follows:

- Click the 'security lock icon' at the bottom right corner (enable status bar if it cannot be seen)
- Check that the certificate information is displayed with:

Issued to = asia-connexis.bnpparibas.com
Issued by = www.verisign.com/CPS_Incorp.by Ref. LIABILITY LTD.(c)97VeriSign
Valid from = '...' is a valid date.

For Netscape Navigator,

You may check the validity of the certificate as follows:

- Press 'Security' in the toolbar
- In 'Security Info', press 'View Certificate'
- Check that the certificate information is displayed with:

This Certificate belongs to:
asia-connexis.bnpparibas.com
Terms of use at
www.verisign.com/rpa (c)00
Division Informatique
BNP Paribas
PARIS PARIS FR

This Certificate was issued by:
www.verisign.com/CPS_Incorp.by
Ref. LIABILITY LTD.(C)97 VeriSign
VeriSign International Server CA -
Class 3
VeriSign, Inc.
VeriSign Trust Network

Check if the certificate is within a valid date.

[Top](#)

Can I exit by closing the browser window?

We strongly suggest that you click "Logout" then click "Close window " to completely exit the service. The service is still available if you do not exit properly.

[Top](#)

What if I forget my password?

Contact your Connexis Administrator to re-set your password or contact Connexis customer support for assistance.

[Top](#)

What is User ID?

User ID is the name you use for identification when accessing Connexis. Your User ID is created by your company's Connexis administrator. Each User ID is unique within your company.

[Top](#)

Can I change my User ID and Password?

Once a User ID has been created, it can't be changed. You can alter your password at any time and you are advised to change your password every 30 days. Your new password should contain four to ten letters and/or numbers (with no spaces or symbols in between), and you are advised to keep it different from your User ID. Please note: the password is case sensitive.

[Top](#)

How secure is my Internet banking service?

Security is our top priority. Your financial information is protected by your User ID and password, a powerful Secure Socket Layer (SSL) 128-bit encryption, and automatic 'time-out'. Your User ID and password must be entered each time you logon to the Internet banking service. If there's no activity after a short period of time, your Internet banking session is terminated to prevent unauthorised access.

[Top](#)

If I suspect there are unauthorised transactions in my account, what should I do?

Change your password immediately, contact your company's Connexis administrator, then call the Connexis customer support hotline

[Top](#)

SECURITY TIPS

- Change your password immediately upon login with a new ID for the first time.

- Keep your Connexis Token in a secure place.
- Do not write the PIN on the back of the Connexis Token.
- NOT to disclose your login User ID and password to any one.
- User ID should be something you can easily remember, yet not easily guessed by anyone else. If you wish to use your name (or something equally familiar) we suggest using a mixture of alphabets and/or numbers.
- Do not use the same password for authorization as for your login
- The auto-complete function on your browser should be disabled, to avoid the automatic completion of your ID and password when you type in User ID.

In Internet Explorer browser, the AutoComplete feature saves previous entries you have made for Web addresses, forms, and passwords. Then, when you type information in one of these fields, AutoComplete suggests possible matches.

While you use Connexis, it may automatically prompt your User ID which you have used in the system. For your security concern, the auto-complete function of your browser should be disabled to avoid the automatic completion of your ID when you start to type the User ID.

To turn Autocomplete on or off in MS Internet Explorer browser, click the Tools menu, click Internet Options, click the Content tab, and click the Autocomplete button. Then disable the 'User names and passwords on forms'.

Your password is as important as User ID. Follow these tips when creating your own password:

- Select a password that cannot be easily guessed by anyone else. Do not associate your password with anything personal such as birthdays, names, phone numbers or other familiar words. Do not use part of your User ID as the password.
- Create a password with a combination of letters and numbers, use upper and lower case.
- Memorise your password. **Never** write it down or reveal it to anyone. If you cannot remember the password, you should disguise the password and keep it in a safe place separate from your computer and account details of your bank or credit cards.
- Remember **No One** at BNP Paribas will ever ask you for your password.
- Change your password on a regular basis - eg every 30 days.
- If you suspect any unusual account activity or last logon time, change your password immediately and contact your administrator, or call the Connexis customer support hotline
- Unknown E-Mail: The Bank never communicate with our clients through emails. Customers should not access the Bank's website through hyperlink embedded in emails. If you received this kind of email, you should contact our eBanking hotline immediately to confirm the status and do not provide your sensitive account information (such as PIN numbers and password) to anyone if in doubt. Avoid accessing e-mails sent from unknown sources or accessing unfamiliar websites. Do not open their attachments or install pirated software as they may contain "Sniffers" program to record your User ID and Password. (Sniffers are programs that monitor and record all information sent over the networks).
- Spoof websites: Always verify the domain name displayed on your browser's website address line or access websites through your browser's bookmark. Verify that the Internet address is the genuine BNP Paribas website by double clicking the 'lock' icon at the bottom bar of the screen to check the security certificate of BNP Paribas.

OTHER SECURITY TIPS

- You can clear the cache and history from you web browser. This feature is accessible from Internet Explorer's tools menu, and also from Netscape's preferences menu.
- Install virus detection software on your computer. This needs to be updated regularly to ensure that you have the latest protection.
- To prevent viruses or other unwanted problems, do not open attachments from unknown or untrustworthy sources. Do not install pirated software.
- Know everyone who uses your computer and limit unauthorised access.
- Do not conduct any banking transactions in a public place (eg. cyber cafe), as it is difficult to ensure such PCs are free of hacker programmes (someone might be able to access your personal/account information).
- Verify that the Internet address is the genuine BNP Paribas website by double clicking the 'lock' icon at the bottom bar of the screen to check the security certificate of BNP Paribas.
- Always remember to log off when you have completed your banking activities.
- Review your account regularly and always keep good records of your personal finances.
- You may want to print a hardcopy of this security FAQ page for reading offline.

Internet Explorer 5.x for Windows users:

Connexis Product

The settings listed in this document are mandatory for all Internet Explorer users. Please ensure these settings are correct. Incorrect settings may result in undesirable browser behavior and or lessened security. Please check through each item carefully.

Should you not already have a 128bit SSL capable browser with Java, you are advised to visit microsoft.com

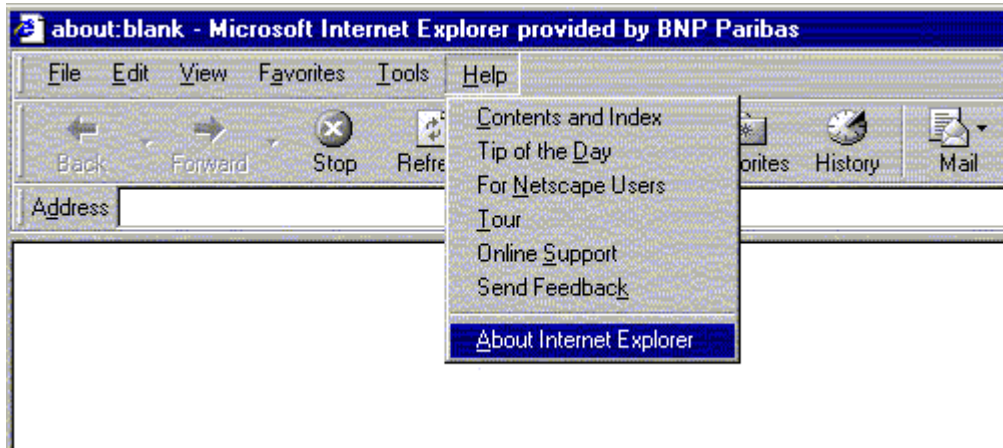
<http://www.microsoft.com/windows/ie/downloads/archive/default.asp>

to download Internet Explorer 5.x 128bit browser with Java plug-in.

Note that in some cases the browser maybe 128bit capable, but will need to additionally download the Java plug-in JIT component, which is also available from the above link. (Valid at the time of writing)

1) Browser version: IE 5.x 128bit SSL support

Open "Internet Explorer", go to "Help" menu item, click [About Internet Explorer](#).

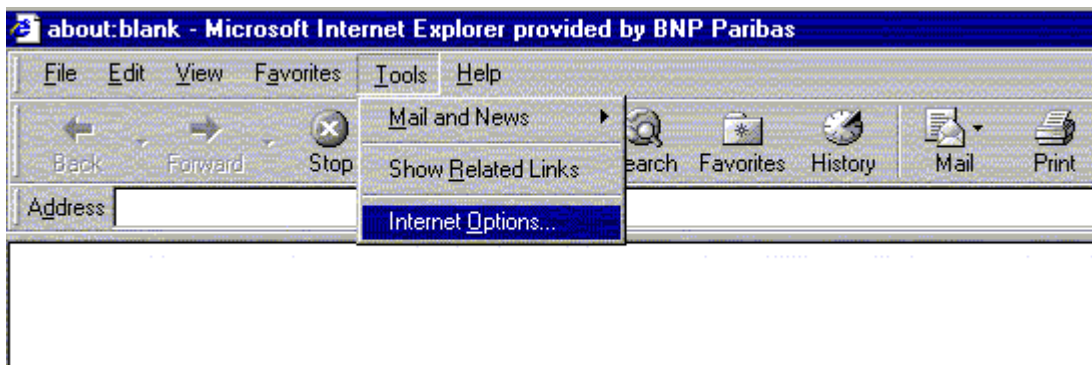


Check whether the Internet Explorer with "128bit Cipher Strength" for SSL pages

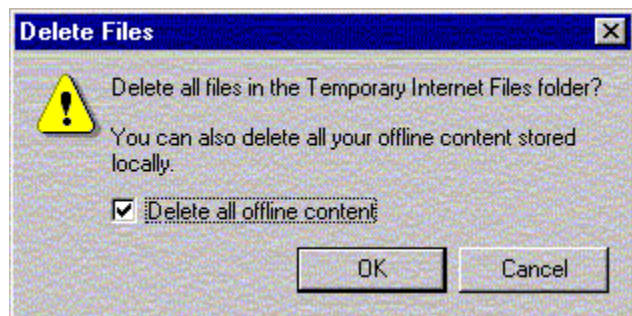
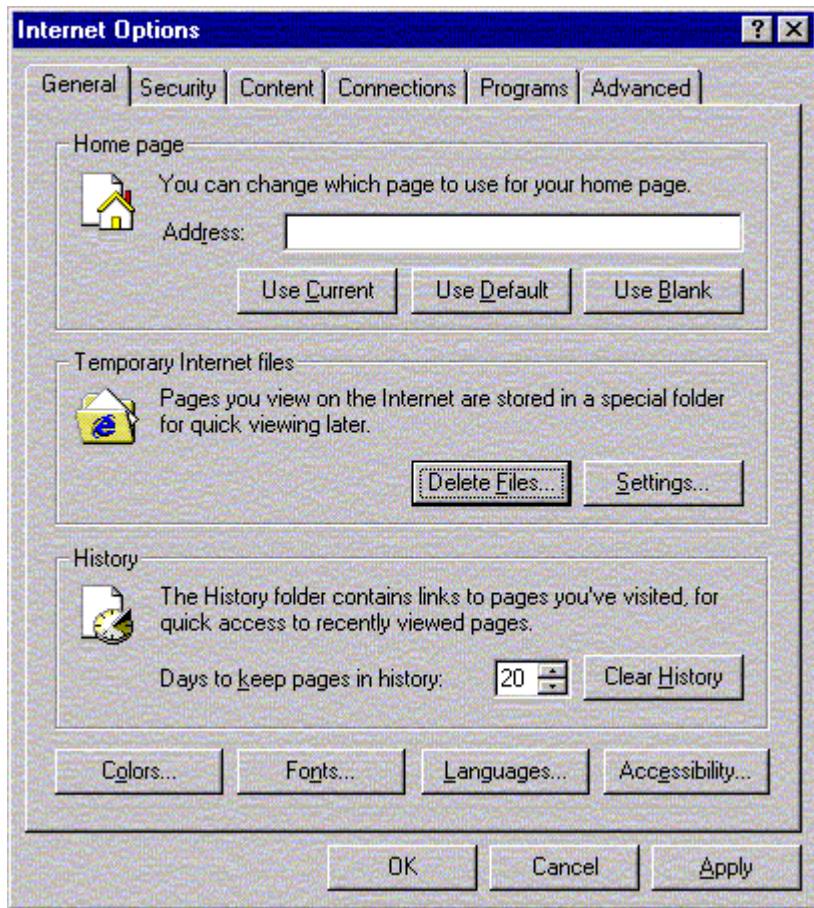


2) Temporary Internet Files "Delete all offline content"

Open "Internet Explorer", go to "Tools" menu item, click "Internet Options".



Under "Temporary Internet files", click [Delete Files...](#) button

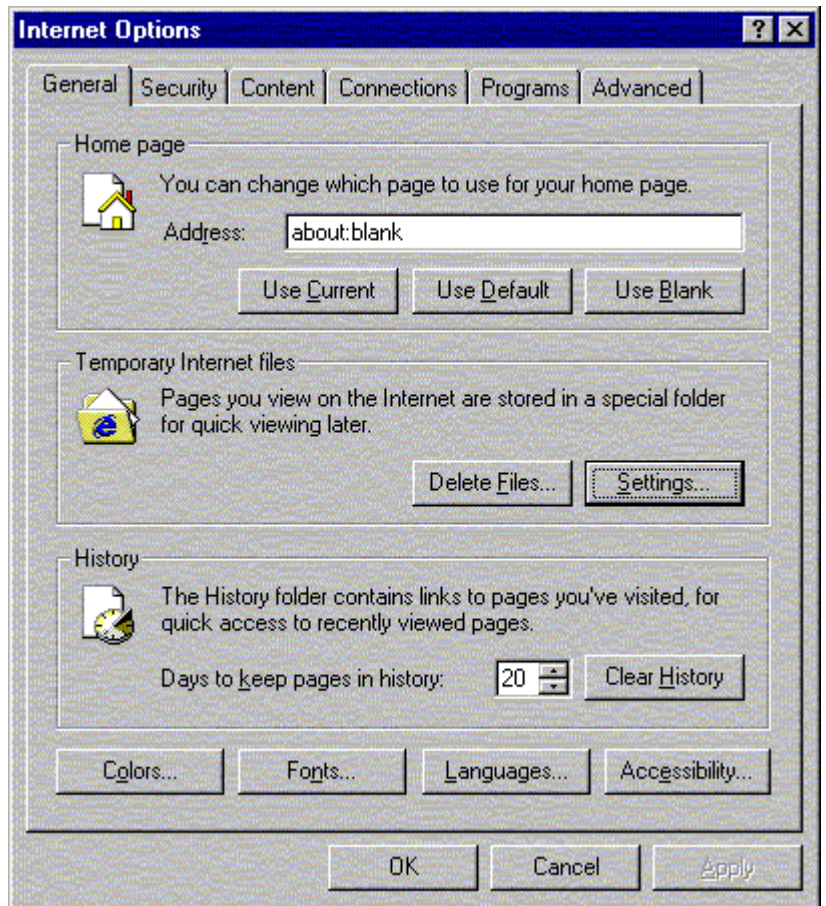


check "Delete all offline content" and then click the "OK" button.

3) Check for newer versions of stored pages

Open "Internet Explorer", goto "Tools" menu item, click "Internet Options".

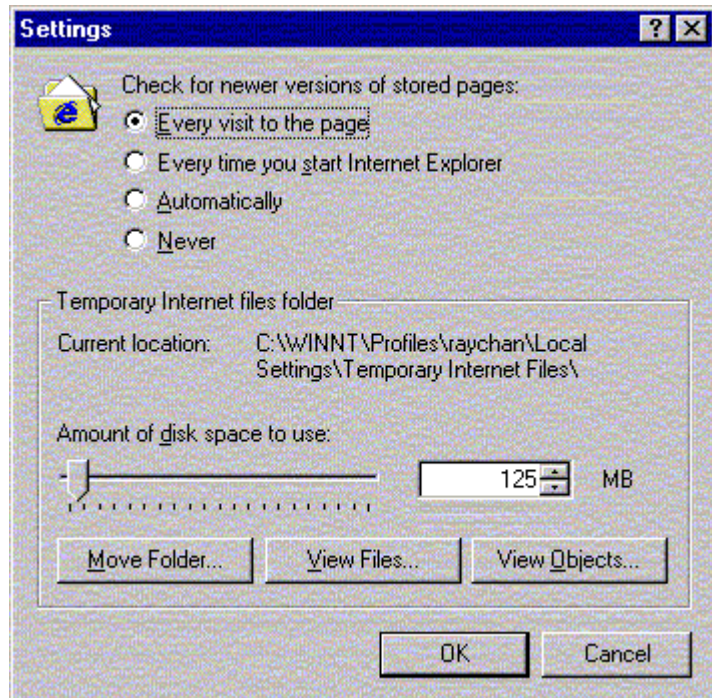




Under "Temporary Internet files", Click "Settings..." button

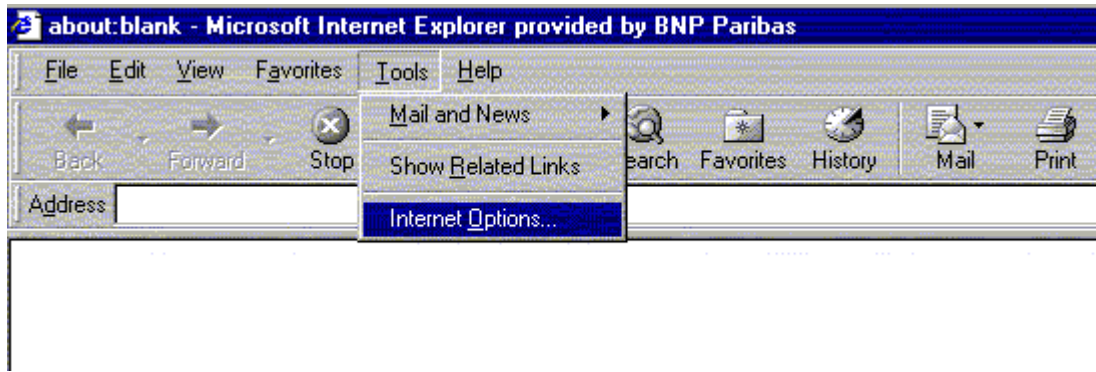
Check for newer versions of stored pages:

Select "Every visit to the page" and then click the "OK" button.



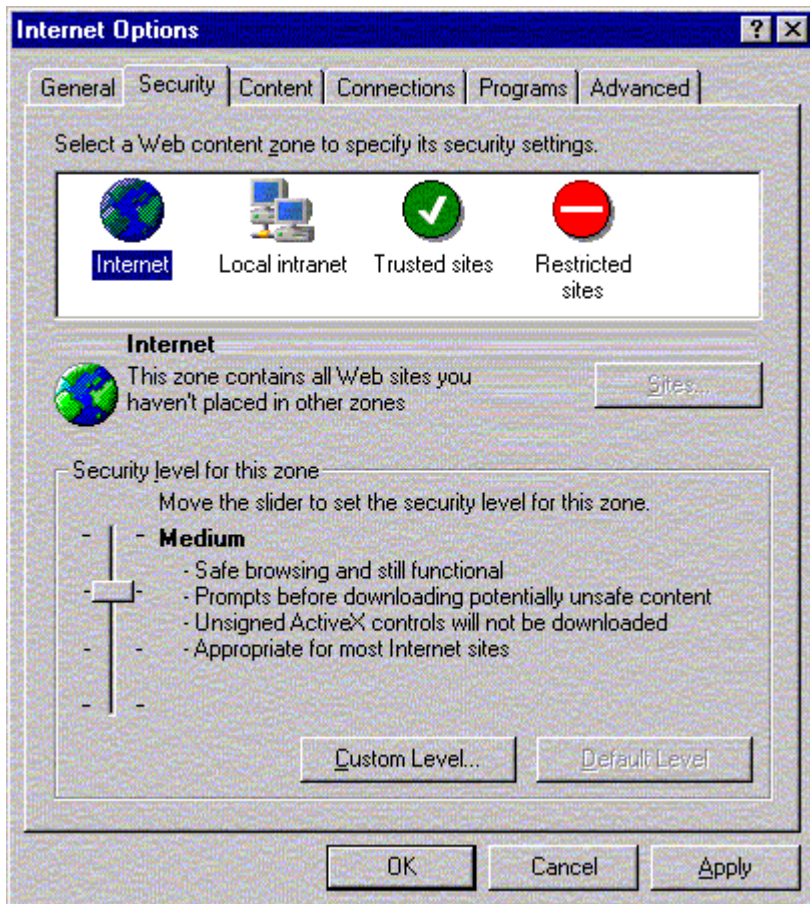
4) Internet Security Level

Open "Internet Explorer", goto "Tools" menu item, click "Internet Options".



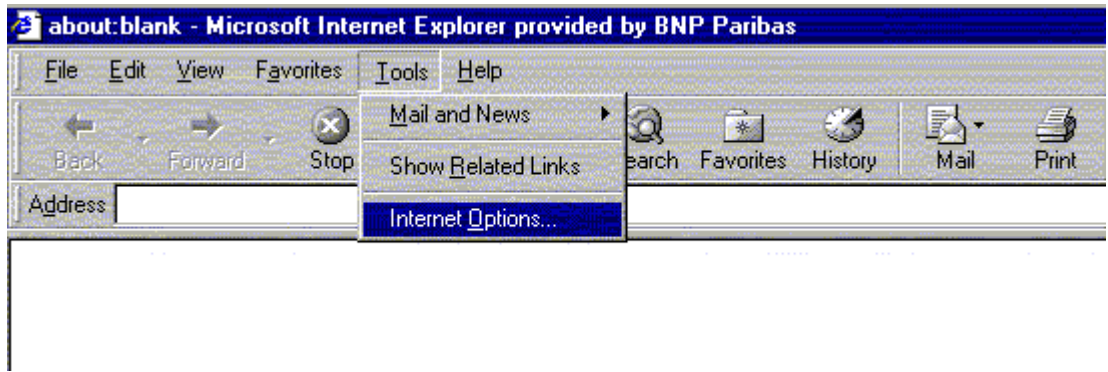
Select "Security" Tab and then select "Internet" under "Select a Web content zone to specify its security settings. After that, click Default Level button under "Security level for this zone". Click "Apply" button when finishing.

Restore "Security Level" to IE's "Default Level."



5) Disable AutoComplete

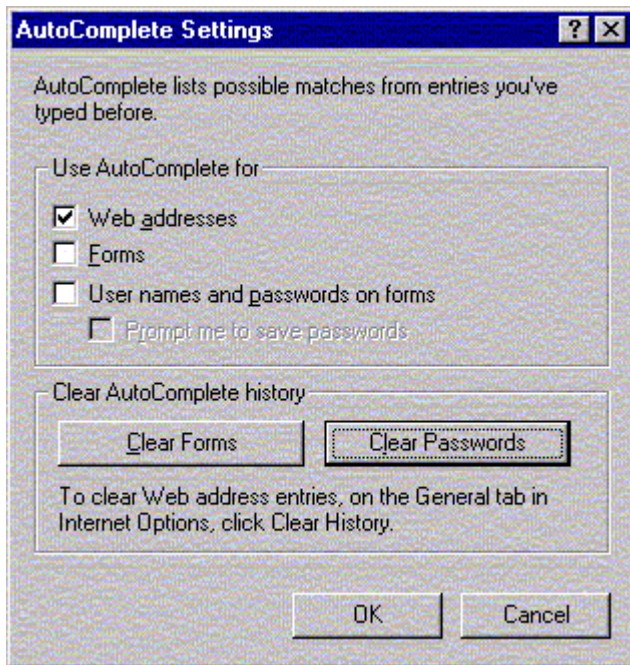
Open "Internet Explorer", goto "Tools" menu item, click "Internet Options".



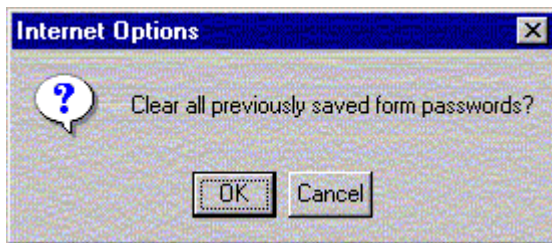
Choose "Content" Tab and then click AutoComplete button under "Personal Information"



Uncheck "User names and passwords on forms" under "Use AutoComplete for" and then Click Clear Passwords button under "Clear AutoComplete history"

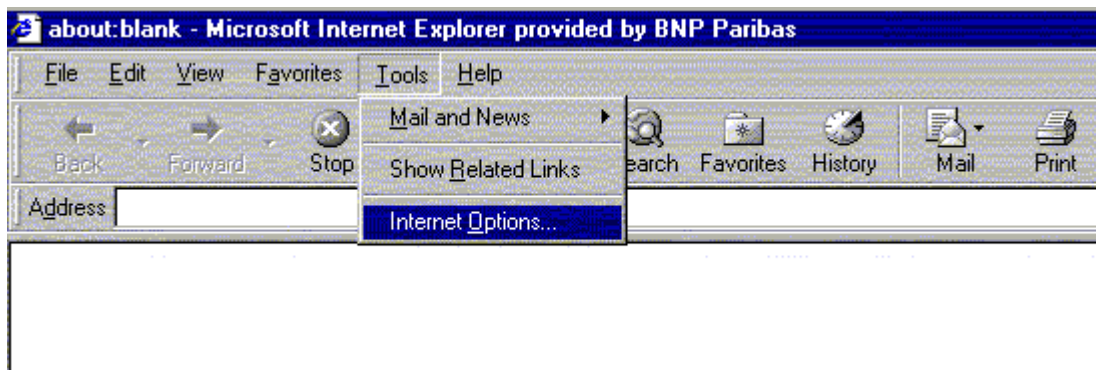


Dialog box popup for the question "Clear all previously saved form passwords?", Click "OK" button



6) Advanced Security

Open "Internet Explorer", goto "Tools" menu item, click "Internet Options".

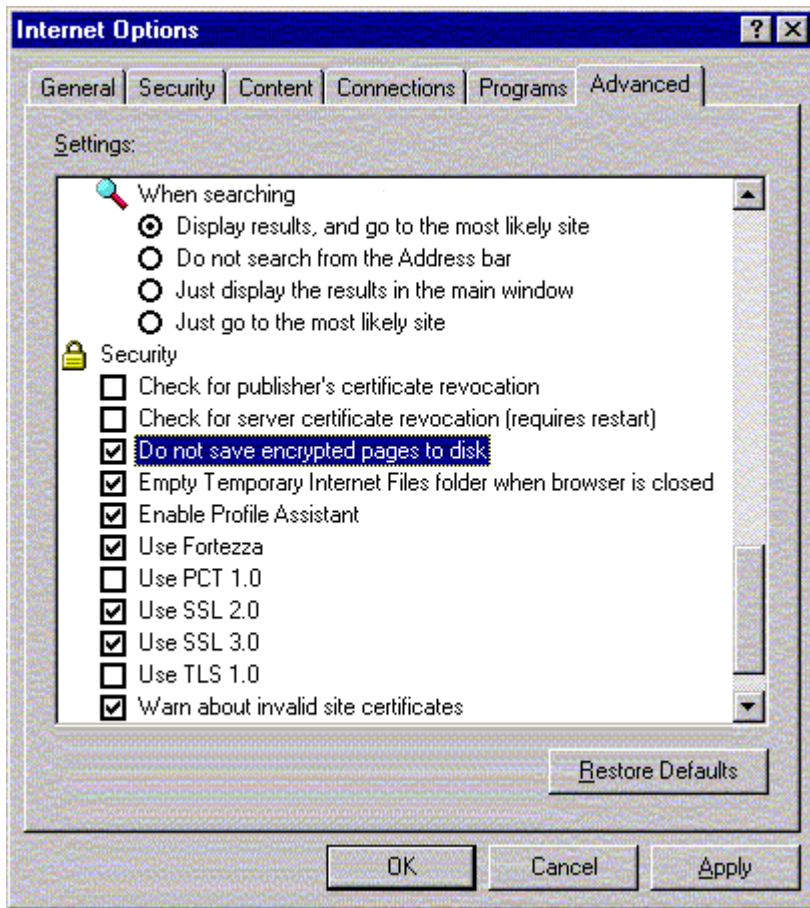


Select "Advanced" Tab, then goto Security section under "Settings".

Check-Do not save encrypted pages to disk.

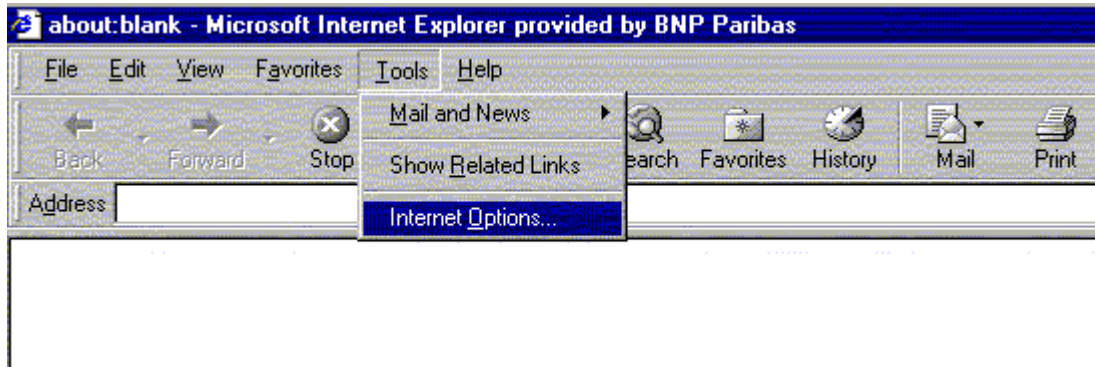
Check-Empty Temporary Internet Files folder when browser is closed.

Click "Apply" button after finishing.



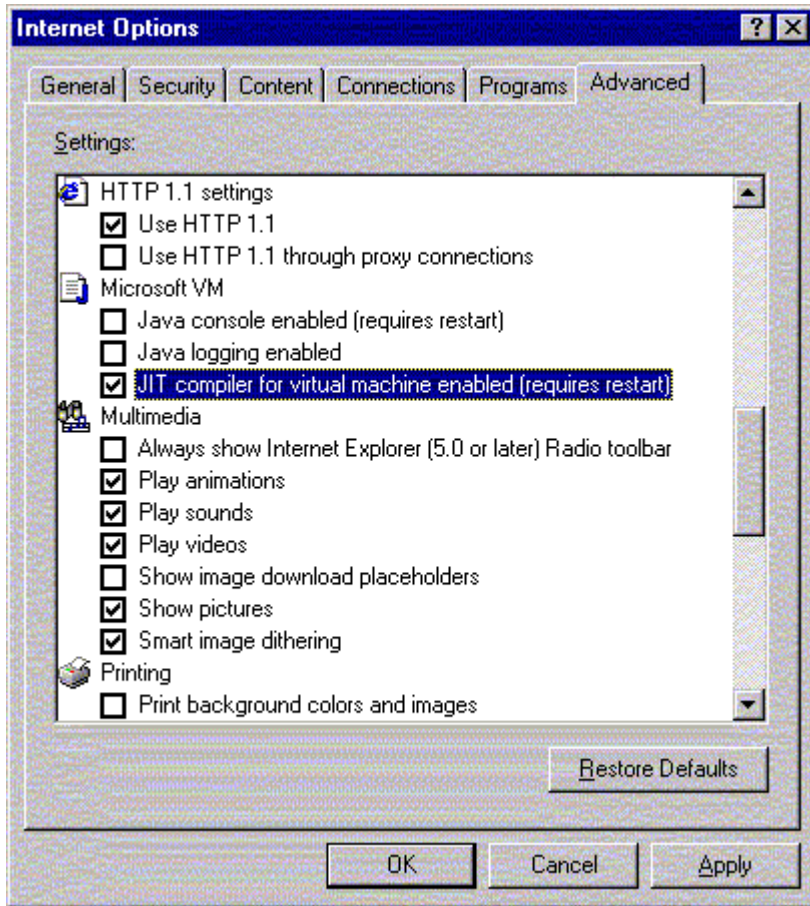
7) Enable Java support

Open "Internet Explorer", goto "Tools" menu item, click "Internet Options".



Select "Advanced" Tab, then goto Microsoft VM section under "Settings".

Check the option "JIT compiler for Virtual Machine Enabled (requires restart)", then click the "Apply" button. The Internet Explorer is needed to restart in order to make this option taking effect.



*Advanced Settings Reference

