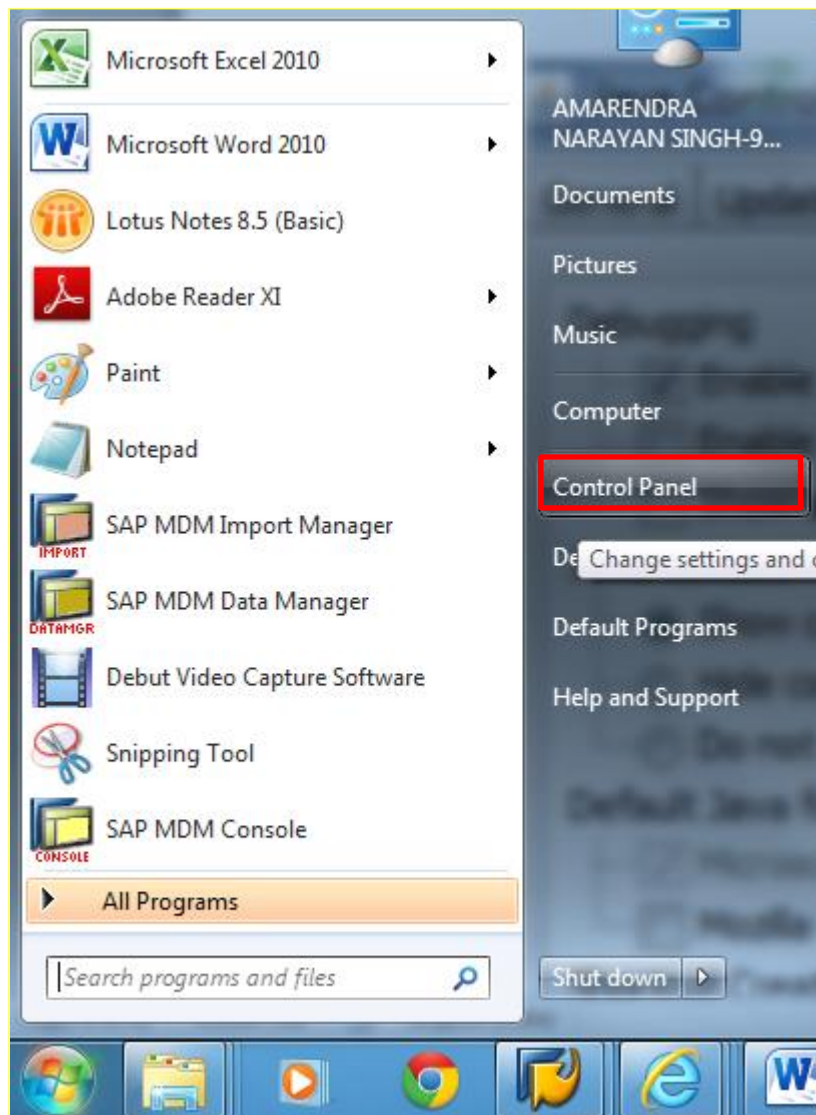
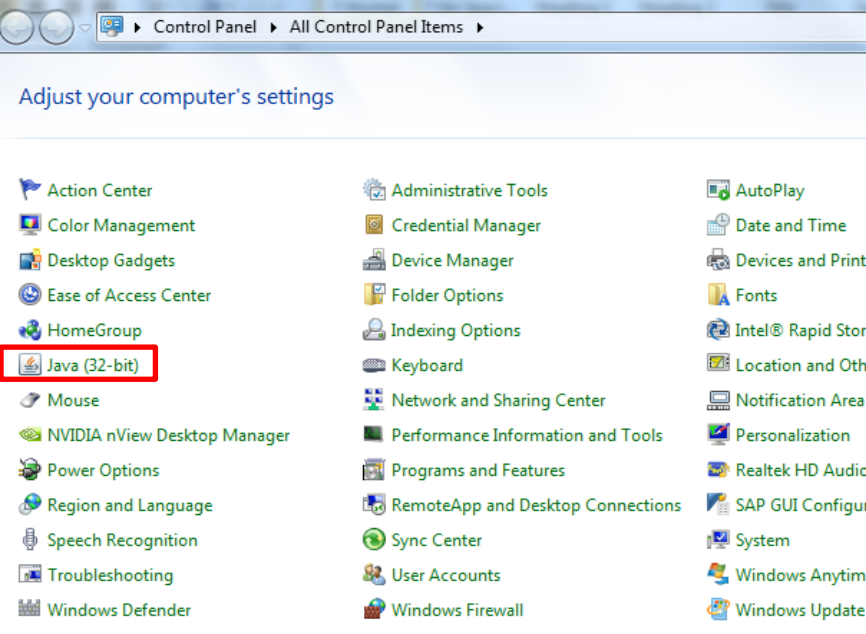
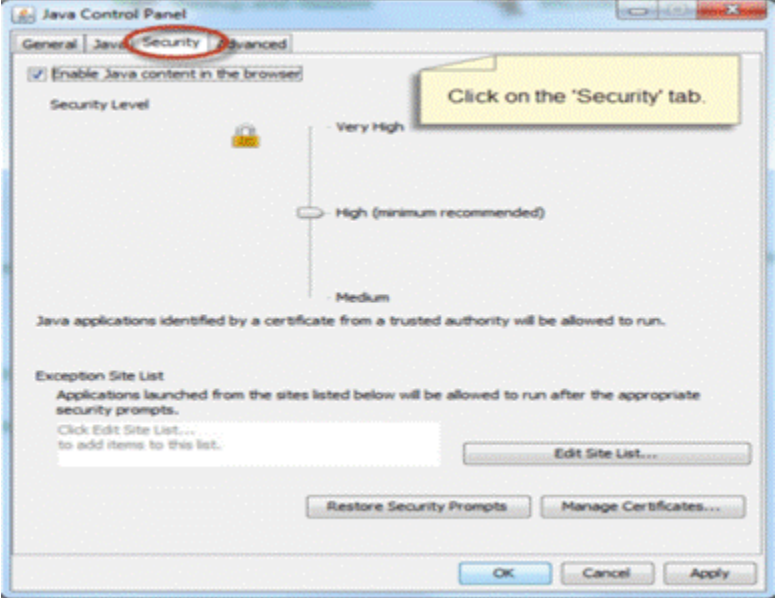


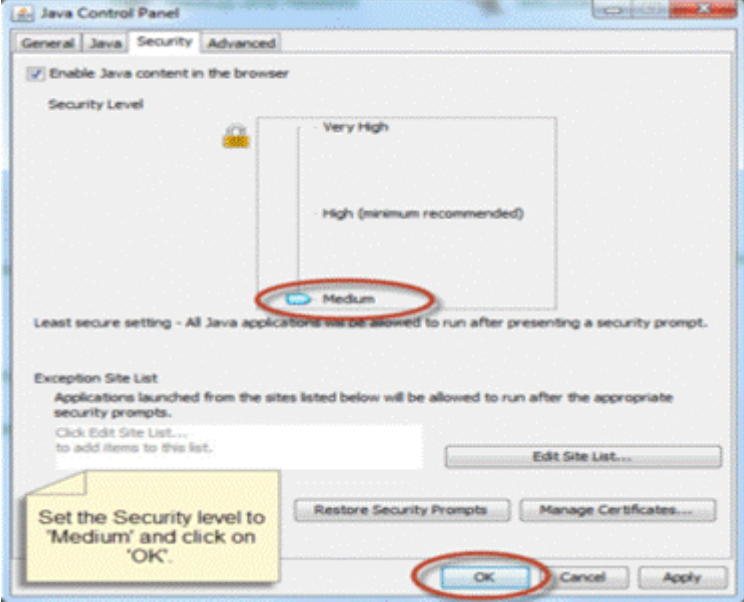
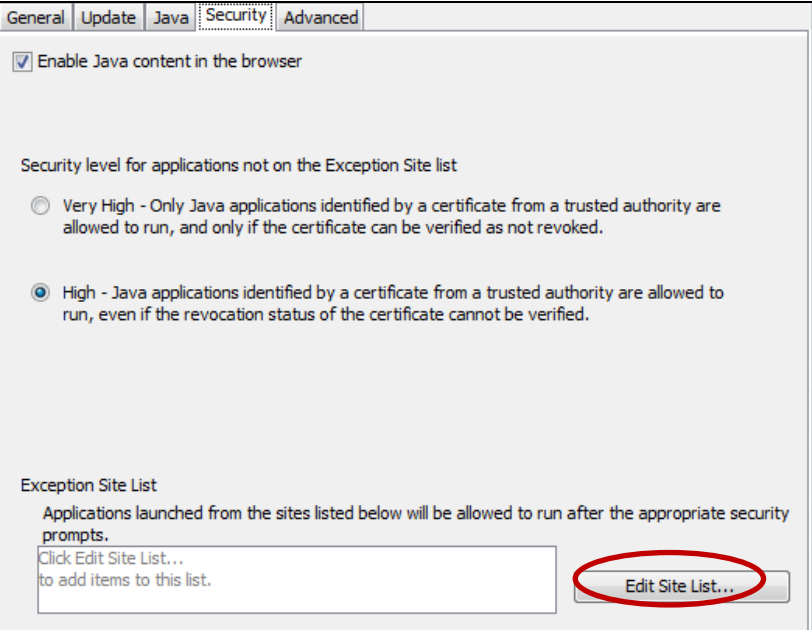
Manual for JAVA Setting for the Reverse Auction

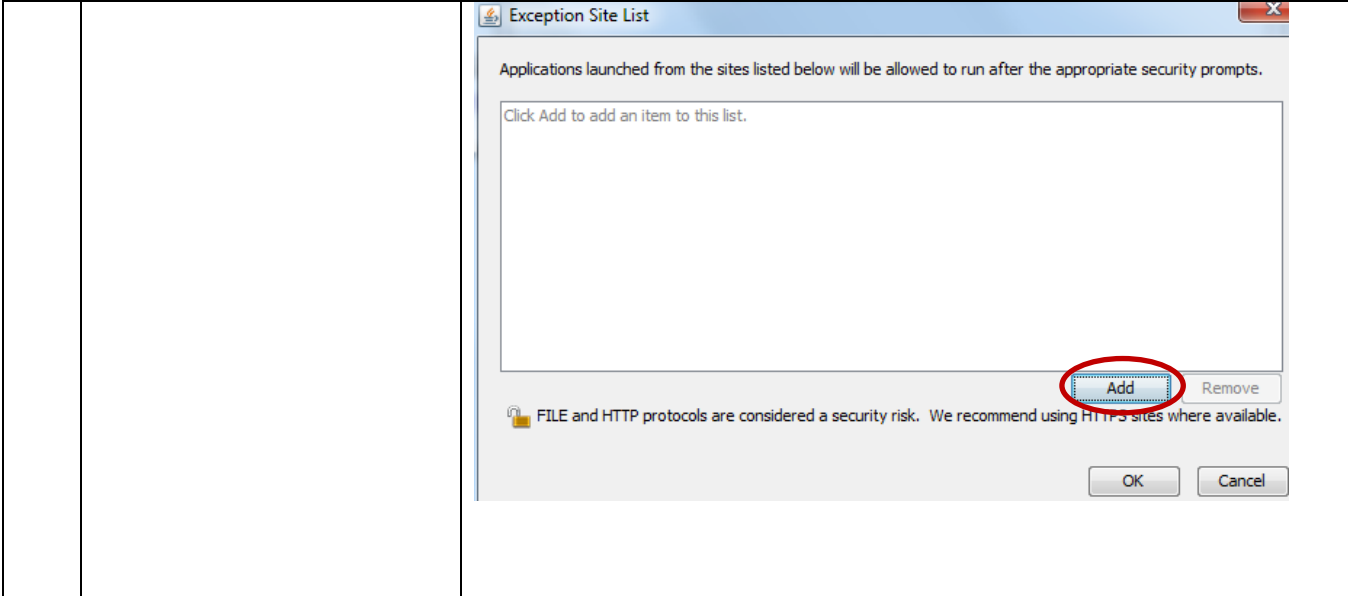
Open 'Control Panel' of the Windows and click on 'Java'. 'Java Control Panel' as shown below will open.



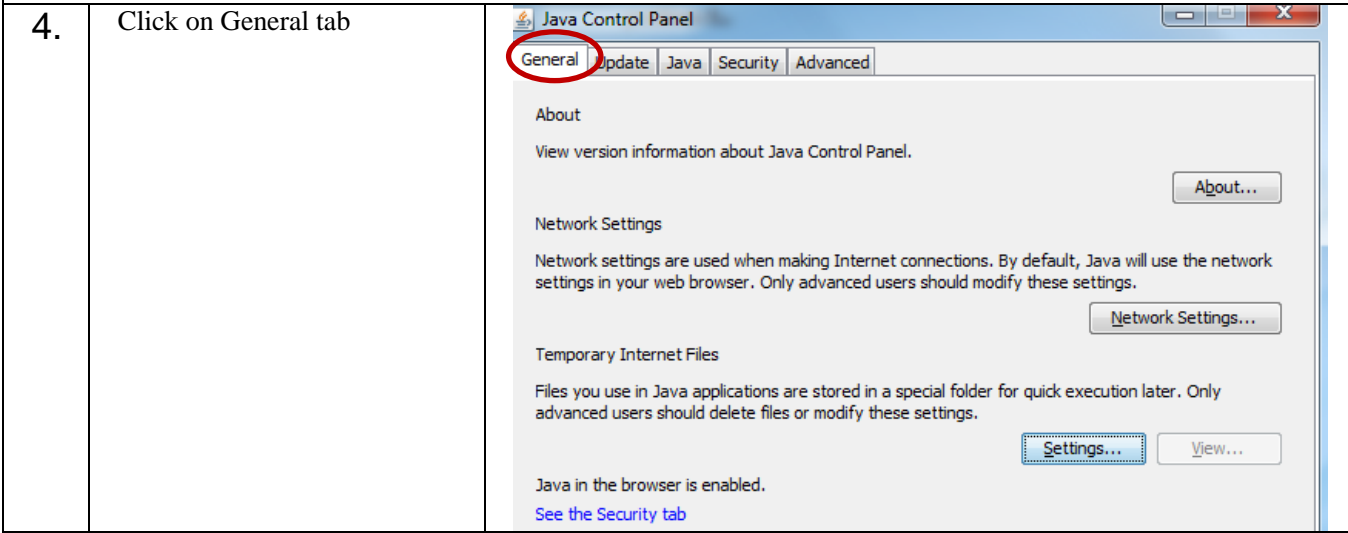
Security setting in JAVA

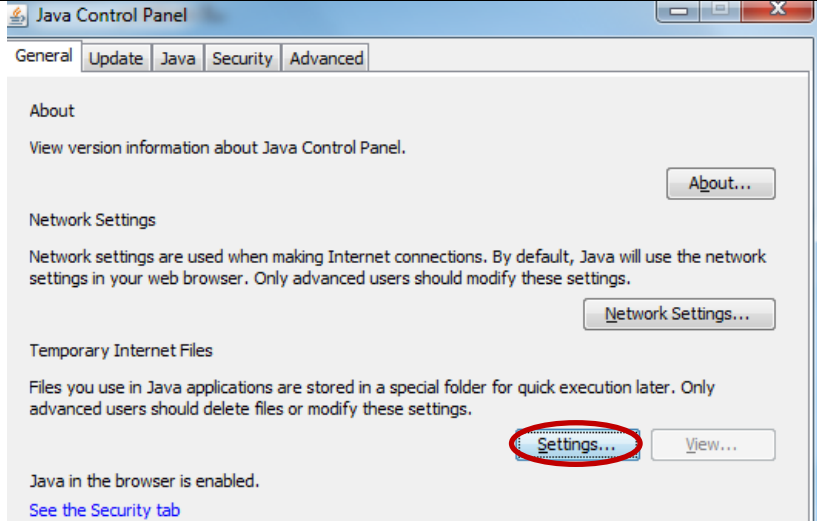
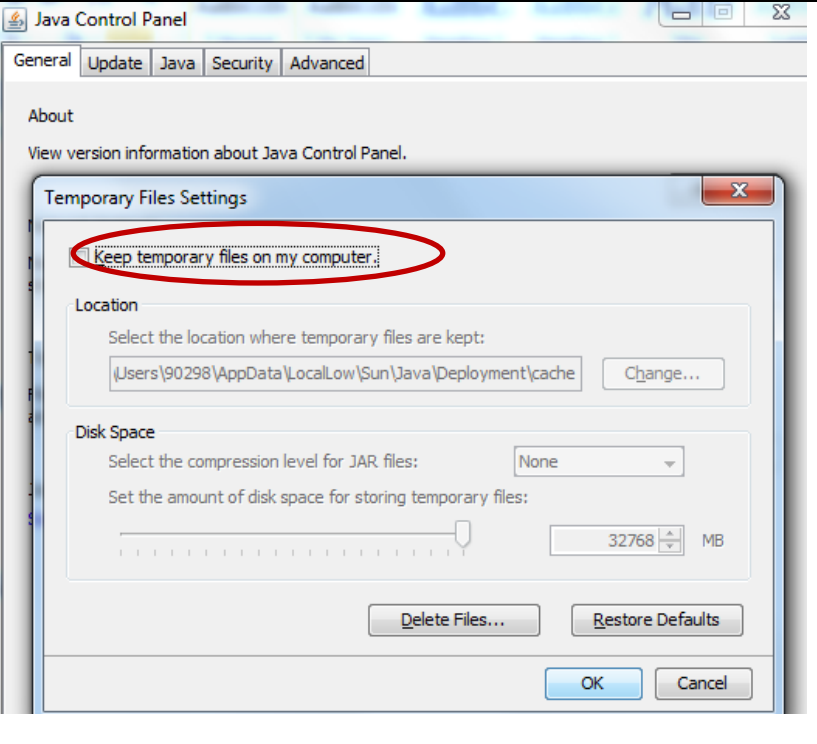
	PROCEDURE	SCREEN SHOT
1.	<p>Go to Start Menu-> Programs-> Java->Configure java Or Control Panel -> Java</p> <p>Then you can see a window as shown</p>	 <p>The screenshot shows the Windows Control Panel window titled 'Adjust your computer's settings'. The 'All Control Panel Items' view is active. A grid of settings icons is displayed, with 'Java (32-bit)' highlighted by a red rectangular box. Other visible settings include Action Center, Administrative Tools, AutoPlay, Color Management, Credential Manager, Date and Time, Desktop Gadgets, Device Manager, Devices and Printers, Ease of Access Center, Folder Options, Fonts, HomeGroup, Indexing Options, Intel® Rapid Storage Technology, Location and Other Sensors, Mouse, Keyboard, Notification Area Icons, NVIDIA nView Desktop Manager, Network and Sharing Center, Personalization, Power Options, Performance Information and Tools, Realtek HD Audio Manager, Region and Language, Programs and Features, SAP GUI Configuration, Speech Recognition, RemoteApp and Desktop Connections, System, Troubleshooting, Sync Center, User Accounts, Windows Defender, Windows Firewall, Windows Anytime Upgrade, and Windows Update.</p>
2.	<p>Click on security tab and Enable the java content in the browser</p>	 <p>The screenshot shows the 'Java Control Panel' window with the 'Security' tab selected. The 'Enable Java content in the browser' checkbox is checked. The 'Security Level' is set to 'High (minimum recommended)', indicated by a slider and a yellow callout box that says 'Click on the 'Security' tab.'. Below the slider, it states 'Java applications identified by a certificate from a trusted authority will be allowed to run.' There is also an 'Exception Site List' section with an 'Edit Site List...' button. At the bottom, there are buttons for 'Restore Security Prompts', 'Manage Certificates...', 'OK', 'Cancel', and 'Apply'.</p>

<p>3.</p>	<p>Make Security Level as medium.</p>	
<p>4.</p>	<p>Add https://etender.ongc.co.in Through Edit site list</p>	



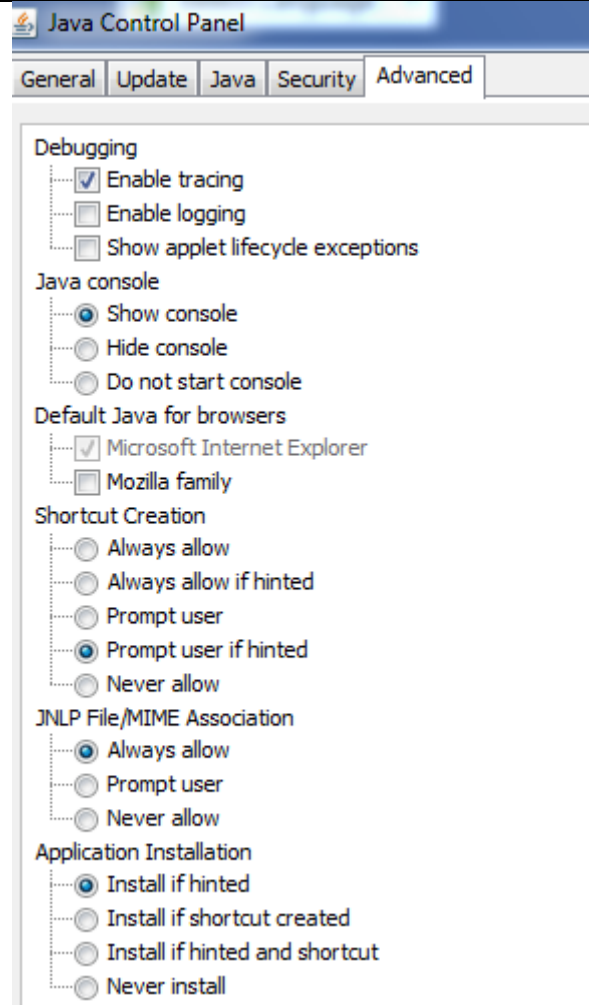
General setting in JAVA



<p>5.</p>	<p>Click on Setting</p>	 <p>The screenshot shows the Java Control Panel window with the 'Temporary Internet Files' section selected. The 'Settings...' button is circled in red.</p>
<p>6.</p>	<p>Keep temporary files on my computer –uncheck and then click on OK</p>	 <p>The screenshot shows the 'Temporary Files Settings' dialog box. The checkbox 'Keep temporary files on my computer' is circled in red.</p>
<p>Advance setting in JAVA</p>		

7.

Do the setting as per given screen shots.



		<p>Secure Execution Environment</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Allow user to grant permissions to signed content<input checked="" type="checkbox"/> Show sandbox warning banner<input checked="" type="checkbox"/> Allow user to accept JNLP security requests<input checked="" type="checkbox"/> Don't prompt for client certificate selection when no certificates or only one exists<input checked="" type="checkbox"/> Warn if site certificate does not match hostname<input type="checkbox"/> Show site certificate from server even if it is valid <p>Mixed code (sandboxed vs. trusted) security verification</p> <ul style="list-style-type: none"><input checked="" type="radio"/> Enable - show warning if needed<input type="radio"/> Enable - hide warning and run with protections<input type="radio"/> Enable - hide warning and don't run untrusted code<input type="radio"/> Disable verification (not recommended) <p>Perform signed code certificate revocation checks on</p> <ul style="list-style-type: none"><input type="radio"/> Publisher's certificate only<input type="radio"/> All certificates in the chain of trust<input checked="" type="radio"/> Do not check (not recommended) <p>Check for signed code certificate revocation using</p> <ul style="list-style-type: none"><input type="radio"/> Certificate Revocation Lists (CRLs)<input type="radio"/> Online Certificate Status Protocol (OCSP)<input checked="" type="radio"/> Both CRLs and OCSP <p>Perform TLS certificate revocation checks on</p> <ul style="list-style-type: none"><input type="radio"/> Server certificate only<input checked="" type="radio"/> All certificates in the chain of trust<input type="radio"/> Do not check (not recommended) <p>Check for TLS certificate revocation using</p> <ul style="list-style-type: none"><input type="radio"/> Certificate Revocation Lists (CRLs)<input type="radio"/> Online Certificate Status Protocol (OCSP)<input checked="" type="radio"/> Both CRLs and OCSP <hr/> <p>Check for TLS certificate revocation using</p> <ul style="list-style-type: none"><input type="radio"/> Certificate Revocation Lists (CRLs)<input type="radio"/> Online Certificate Status Protocol (OCSP)<input checked="" type="radio"/> Both CRLs and OCSP <p>Advanced Security Settings</p> <ul style="list-style-type: none"><input checked="" type="checkbox"/> Use certificates and keys in browser keystore<input checked="" type="checkbox"/> Enable blacklist revocation check<input checked="" type="checkbox"/> Enable caching password for authentication<input checked="" type="checkbox"/> Use SSL 2.0 compatible Client-hello format<input checked="" type="checkbox"/> Use TLS 1.0<input checked="" type="checkbox"/> Use TLS 1.1<input checked="" type="checkbox"/> Use TLS 1.2 <p>Miscellaneous</p> <ul style="list-style-type: none"><input type="checkbox"/> Place Java icon in system tray<input type="checkbox"/> Suppress sponsor offers when installing or updating Java
--	--	--