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.	Go to Start Menu->	Control Panel + All Co	ontrol Panel Items 🕨	at the space has
	Programs-> Java->Configure java Or	Adjust your computer's settings	5	
	Or Control Panel -> Java Then you can see a window as shown	 Action Center Color Management Desktop Gadgets Ease of Access Center HomeGroup Java (32-bit) Mouse NVIDIA nView Desktop Manager Power Options Region and Language Speech Recognition Troubleshooting Windows Defender 	 Administrative Tools Credential Manager Device Manager Folder Options Indexing Options Indexing Options Keyboard Network and Sharing Center Performance Information and Tools Programs and Features RemoteApp and Desktop Connections Sync Center User Accounts Windows Firewall 	 AutoPlay Date and Time Devices and Printers Fonts Intel® Rapid Storage Technolog Location and Other Sensors Notification Area Lons Personalization Realtek HD Audio Manager SAP GUI Configuration System Windows Anytime Upgrade Windows Update
2.	Click on security tab and Enable the java content in the browser	Java Control Panel General Java Control Panel Security Level Java applications identified by a certificate Exception Site List Applications launched from the sites list security prompts. Cick Edit Site List. To add items to this list.	Very High Very High High (minimum recommended) Medium e from a trusted authority will be allowed to run. ted below will be allowed to run after the appropriat Edit Site List Restore Security Prompts Manage Certificate OK Cancel	e Acoty

3.		Java Control Panel
		General Java Security Advanced
	Make Security Level as	Prable Java content in the browser
	medium	Security Level
	incurum.	- Very High
•		
		· righ (minimum recommended)
		Medun
		Least secure setting - All Java applications wards allowed to run after presenting a security prompt.
		Exception Site List
		Applications automete from the sites listed below will be allowed to run after the appropriate security prompts.
		Click Edit Site List to add items to this list.
		Set the Security level to Restore Security Prompts Manage Certificates
		"Medium' and click on
		OK. OK Cancel Apply
4.	Add https://etender.ongc.co.in	General Update Java Security Advanced
		Enable Java content in the browser
	Through Edit site list	
		Constitutional for any function and an the Europeire Othe Rate
		Security level for applications not on the Exception Site list
		Very High - Only Java applications identified by a certificate from a trusted authority are allowed to give and apply if the partificate can be verified as not revelued.
		allowed to run, and only if the certificate can be verified as not revoked.
		High - Java applications identified by a certificate from a trusted authority are allowed to run, even if the revocation status of the certificate cannot be verified.
		Exception Site List
		Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.
		Click Edit Site List
		to add items to this list.
1		

		Exception Site List
		Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.
		Click Add to add an item to this list. Add Remove Add Remove FILE and HTTP protocols are considered a security risk. We recommend using HTTP's sites where available. OK Cancel
		General setting in JAVA
4.	Click on General tab	General setting in JAVA
4.	Click on General tab	General setting in JAVA
4.	Click on General tab	General setting in JAVA
4.	Click on General tab	General setting in JAVA
4.	Click on General tab	General setting in JAVA
4.	Click on General tab	General setting in JAVA
4.	Click on General tab	General setting in JAVA
4.	Click on General tab	General setting in JAVA
4.	Click on General tab	General setting in JAVA
4.	Click on General tab	General setting in JAVA
4.	Click on General tab	Seneral setting in JAVA Image: Security Advanced About View version information about Java Control Panel. About Network Settings Network Settings Network Settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings Image: Temporary Internet Files Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

5.	Click on Setting	🔊 Java Control Panel
0.		General Update Java Security Advanced
		About
		View version information about Java Control Panel.
		A <u>b</u> out
		Network Settings
		Network settings are used when making Internet connections. By default, Java will use the network
		settings in your web browser. Only advanced users should modify these settings.
		Temporary Internet Files
		Files you use in Java applications are stored in a special folder for quick execution later. Only
		advanced users should delete files or modify these settings.
		Settings
		See the Security tab
6.	Keep temporary files on my	🛃 Java Control Panel
•	computer –uncheck and then	General Update Java Security Advanced
	click on OK	About
		View version information about Java Control Panel.
		Temporany Filer Settings
		Keep temporary files on my computer.
		Location
		Select the location where temporary files are kept:
		Users\90298\AppData\LocalLow\Sun\Java\Deployment\cache Change
		a Disk Space
		Select the compression level for JAR files: None 🚽
		Set the amount of disk space for storing temporary files:
		32768 × MB
		Delete Files Restore Defaults
		OK Cancel
Advance setting in JAVA		

	Do the setting as per	🛓 Java Control Panel
7.	given screen shots.	General Update Java Security Advanced
		Debugging Enable tracing Show applet lifecycle exceptions Java console Show console Hide console Do not start console Default Java for browsers Microsoft Internet Explorer Mozilla family Shortcut Creation Always allow Always allow Prompt user Prompt user Prompt user Prompt user Never allow JNLP File/MIME Association Always allow Prompt user Never allow JNLP File/MIME Association Never allow JNLP File/MIME Association Never allow JNLP File/MIME Association Never allow JNLP File/MIME Association Never allow Always allow Never allow Application Installation Never allow Application Installation Never install

	Secure Execution Environment
	Allow user to grant permissions to signed content
	Show sandbox warning banner
	V Allow user to accept JNLP security requests
	Don't prompt for client certificate selection when no certificates or only one exists When if site particulate data activities have been activities
	Warn if site certificate does not match hostname
	Show site certificate from server even if it is valid
	Fixed code (sandboxed vs. trusted) security verification
	Enable - bide warning and run with protections
	Enable - hide warning and don't run untrusted code
	Disable verification (not recommended)
	Perform signed code certificate revocation checks on
	All certificates in the chain of trust
	O not check (not recommended)
	Check for signed code certificate revocation using
	Certificate Revocation Lists (CRLs)
	Online Certificate Status Protocol (OCSP)
	Perform TLS certificate revocation checks on
	Server certificate only All service setting a fit wat
	Check for TLS certificate revocation using
	Certificate Revocation Lists (CRLs)
	Online Certificate Status Protocol (OCSP)
	Check for TLS certificate revocation using
	Certificate Revocation Lists (CRLs)
	Online Certificate Status Protocol (OCSP)
	Both CRLs and OCSP
	Advanced Security Settings
	Enable blacklist revocation check
	Enable caching password for authentication
	Ilse SSL 2.0 compatible ClientHello format
	Use ILS 1.0
	Use TLS 1.1
	Use TLS 1.2
	Miscellaneous
	Suppress sponsor offers when installing or updating Java