Configure Browsers for Kerberos Authentication

By default, you will not be authenticated by Kerberos if you are using Mozilla® Firefox or Microsoft® Internet Explorer browser to access RiskVision Server. To allow a browser to support Kerberos AES 256 bit encryption, you must configure the settings specific to each browser type.

Mozilla Firefox

To configure Mozilla Firefox version 11.0:

- 1. Open the Firefox browser and enter "about:config" in the address bar. A warning message is displayed. Click **I'll be careful, I promise!** to accept the warning and continue.
- 2. Enter the string "negotiate" in the Search bar to search properties containing the string "negotiate." The browser displays the following properties:
 - network.negotiate-auth.delegation-uris
 - network.negotiate-auth.trusted-uris

🥹 about:config - Mozilla Firefox				
Eile Edit View History Bookmarks Tools Help				
about:config +				
e about:config				☆ ~ C
Search: negotiate				
Preference Name	- Status	Туре	Value	
network.negotiate-auth.using-native-gsslib	default	boolean	true	
network.negotiate-auth.trusted-uris	user set	string	https://RiskVisionURL	
network.negotiate-auth.gsslib	default	string		
network.negotiate-auth.delegation-uris	user set	string	https://Risk¥isionURL	
network.negotiate-auth.allow-proxies	user set	boolean	false	
network.negotiate-auth.allow-non-fqdn	user set	boolean	true	

3. Double-click or right-click each property, then click Modify. Specify the RiskVision URL.

Microsoft Internet Explorer

See Microsoft Internet Explorer for instructions. For information on debugging and troubleshooting Kerberos AES 256 bit encryption, see Debugging and Troubleshooting.