eSuite Hardware/Software Requirements and Browser Configuration

Internet Explorer Configuration

1. **Open Internet Explorer 9 Options:** Click on Tools in the top navigation bar and select Internet Options from the drop down to open IE9 Options

![Internet Options](image)
2. Click the **Security** tab

3. In the **Select a zone to view or change security settings**, select **Trusted sites**

4. Click the **Sites** button
5. Type the URL http://*.pjm.com in the **Add this website to the zone** field and click **Add**
6. Type the URL https://*.pjm.com in the **Add this website to the zone** field and click **Add**
7. Uncheck the **Require server verification (https:) for all sites in this zone**
8. Click **Close** when finished

9. Click on **Custom Level**
10. Click on **Enable** for .NET Framework Loose XAML
11. Click on **Enable** for .NET Framework XAML browser applications
12. Click on **Enable** for .NET Framework XPS documents
13. Click on **High Safety** for .NET Framework-reliant components
Permissions for components with manifests

14. Click on **Enable** for .NET Framework-reliant components
Run components not signed with Authenticode

15. Click on **Enable** for .NET Framework-reliant components
Run components signed with Authenticode
16. Click on **Enable** for ActiveX controls and plug-ins Allow ActiveX Filtering

17. Click on **Enable** for Allow previously unused ActiveX controls to run without prompt

18. Click on **Enable** for Allow previously unused ActiveX controls to run without prompt

19. Click on **Enable** for Allow Scriptlets

20. Click on **Enable** for Automatic prompting for ActiveX controls
20. Click on **Enable** for Binary and script behaviors
21. Click on **Disable** for Display video and animation on a webpage that does not use external media player
22. Click on **Enable** for Download signed ActiveX controls
23. Click on **Enable** for Download unsigned ActiveX controls
24. Click **Enable** for initialize and script ActiveX controls not marked as safe for scripting
25. Click **Disable** for Only allow approved domains to use ActiveX without prompt
26. Click **Enable** Run ActiveX controls and plug-ins
27. Click **Enable** Script ActiveX controls marked safe for scripting*

*Takes effect after you restart Internet Explorer*
28. Click **Enable** for File Download
29. Click **Enable** for Font Download
30. Click **Enable** for Enable .Net Framework setup
31. Click **Enable** for Miscellaneous Access data sources across domains
32. Click **Enable** for Miscellaneous Allow META REFRESH
33. Click **Enable** for Miscellaneous Allow scripting of Microsoft web browser control
34. Click **Enable** for Miscellaneous Allow script-initiated windows without size or position constraints
35. Click **Prompt** for Allow webpages to use restricted protocols for active content

36. Click **Enable** for Allow websites to open windows without address or status bars

37. Click **Prompt** for Display mixed content

38. Click **Enable** for Don’t prompt for client certificate selection when no certificates or only one certificate exists
39. Click **Enable** for Drag and drop or copy and paste files
40. Click **Enable** for MIME Sniffing
41. Click **Enable** for Include local directory path when uploading files to a server
42. Click **Enable** for Launching applications and unsafe files
43. Click **Enable** for Launching programs and files in an IFRAME
44. Click **Enable** for Navigate windows and frames across different domains
45. Click **Enable** for Submit non-encrypted form data
46. Click **Disable** for Use Pop-up Blocker
47. Click **Disable** for Use SmartScreen Filter
48. Click **Enable** for Userdata persistence
49. Click **Prompt** for Websites in less privileged web content zone can navigate into this zone
50. Click **Enable** for Scripting Active scripting
51. Click **Enable** for Allow Programmatic clipboard access
52. Click **Enable** for Allow status bar updates via script
53. Click **Enable** for Allow websites to prompt for information using scripted windows
54. Click **Disable** for XSS filter
55. Click on **Enable** for Scripting of Java applets
56. Click **Automatic logon only in Intranet zone** for User Authentication Logon.
57. Click **OK**

58. Click **Yes** when prompted if you are sure you want to change the settings for this zone.
59. Click on **Advanced**
60. Under the **Advanced** tab ensure only the following items are checked:

**Accessibility** – Reset text size to medium for new windows and tabs

**Browsing** – Close unused folders in History and Favorites*

**Browsing** – Disable script debugging (Internet Explorer).

**Browsing** – Disable script debugging (Other)

* Takes effect after you restart Internet Explorer

[Internet Options dialog box showing advanced settings]
**Browsing** – Display Accelerator button on selection

**Browsing** – Enable automatic crash recovery*

**Browsing** – Enable FTP folder view (outside of Internet Explorer)

**Browsing** – Enable third-party browser extensions*

**Browsing** – Enable visual styles on buttons and controls in webpages

**Browsing** – Show friendly HTTP error messages

* Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

 Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.
Browsing — Click **Always** for Underline links

Browsing — Click Use inline AutoComplete (outside of Internet Explorer)

Browsing — Click Use smooth scrolling

Browsing — Click Use HTTP 1.1 for HTTP 1.1 settings
International – Send IDN server names for Intranet addresses

International – Send UTF-8 URLs

Multimedia – Enable alternative codecs in HTML 5 media elements*

Multimedia – Enable automatic image resizing

Multimedia – Play animations in webpages*

Multimedia – Play sounds in webpages*

Multimedia – Show Pictures

* Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Reset Internet Explorer’s settings to their default condition.

You should only use this if your browser is in an unusable state.
Security – Allow active content from CDs to run on My Computer*

Security – Check for signatures on downloaded programs

Security – Enable DOM storage

Security – Enable Integrated Windows Authentication*

Security – Enable memory protection to help mitigate online attacks*
**Security** – Use SSL 2.0

**Security** – Use SSL 3.0

**Security** – Use TLS 1.0

**Security** – Warn if POST submittal is redirected to a zone that does not permit posts

61. Click OK
62. Close the browser and re-open
63. Open the PJM website
64. When prompted for security requirements click NO