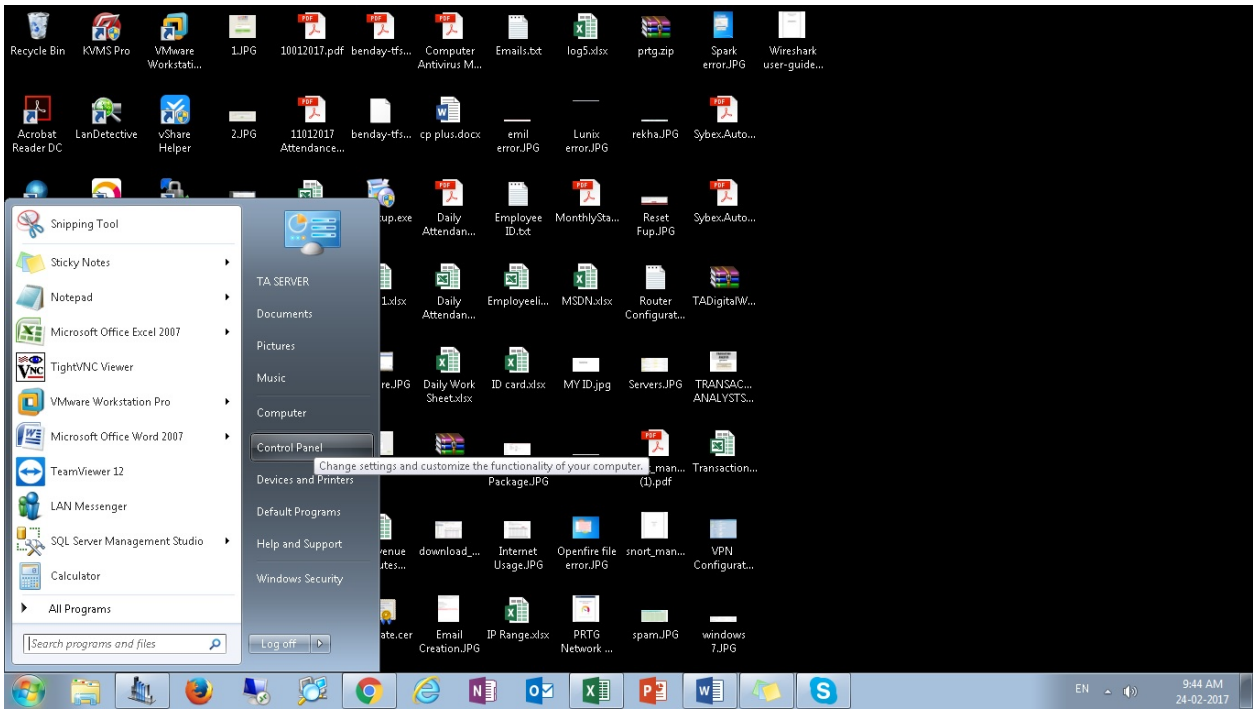
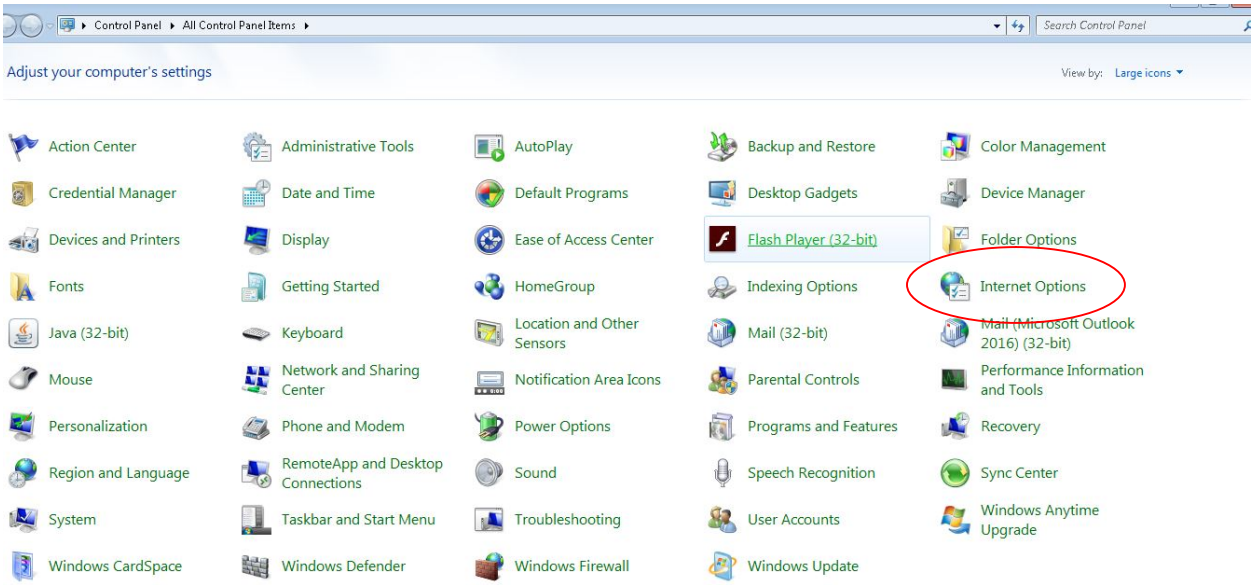
Active X Configuration

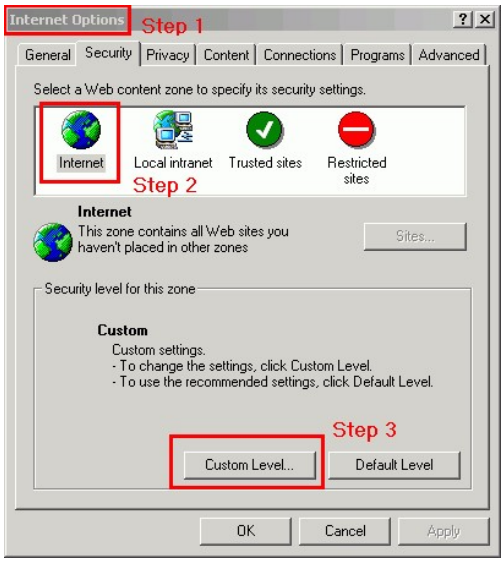
⇨ Click Start button and open control panel.



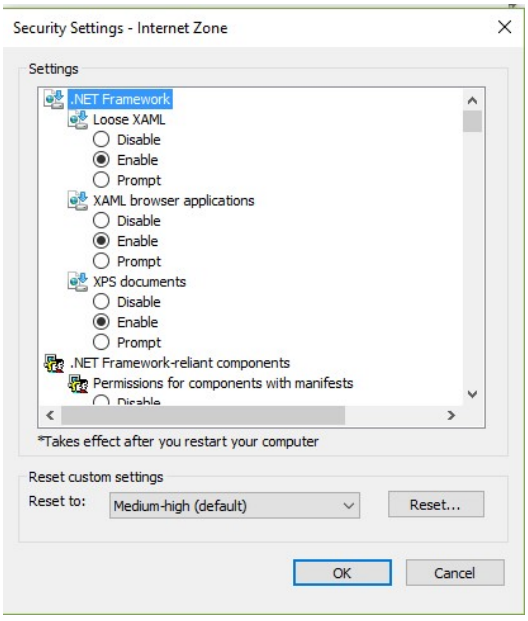
⇨ In Control Panel, Open Internet Options.



- ⇨ After the Internet Options is enabled, click on Security tab.
- ⇨ Then Select INTERNET option and then Custom Level.



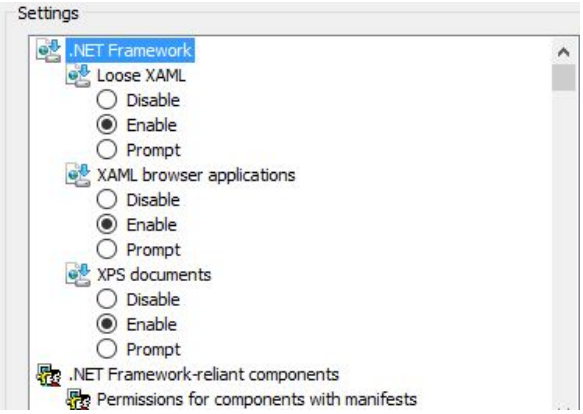
- ⇨ On selecting Custom level, Security Settings window is Displayed.



- ⇨ Now in the security settings window the below mentioned configuration need to be done.

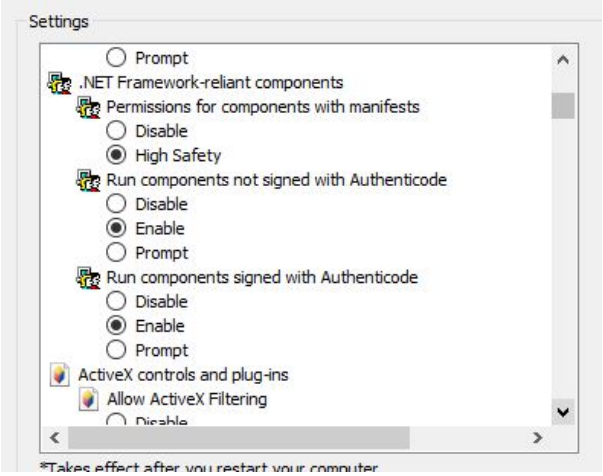
Under .NET Framework

1. Loose XAML **ENABLE**
2. XAML browser application **ENABLE**
3. XPS documents **ENABLE**



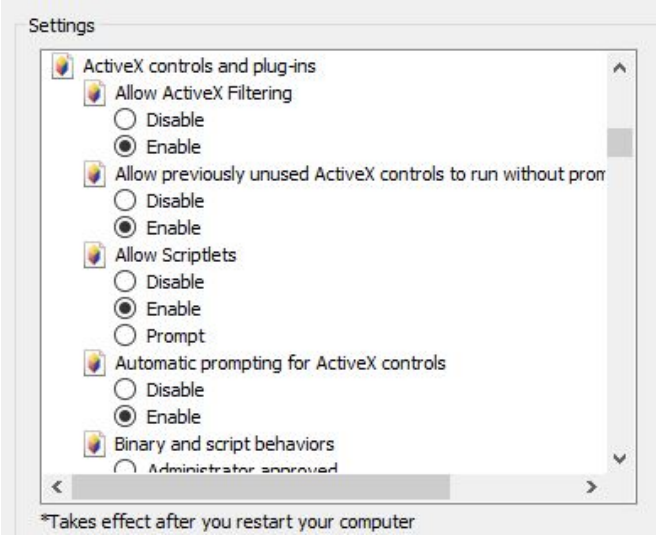
Under .NET Framework-reliant components

1. Permissions for components with manifests **High Safety**
2. Run components not signed with Authenticode **Enable**
3. Run components signed with Authenticode **Enable**



Under ActiveX controls and plug –INS

1. Allow ActiveX Filtering **Enable**
2. Allow previously unused ActiveX controls to run without program **Enable**
3. Allow Script lets **Enable**
4. Automatic prompting for ActiveX controls **Enable**

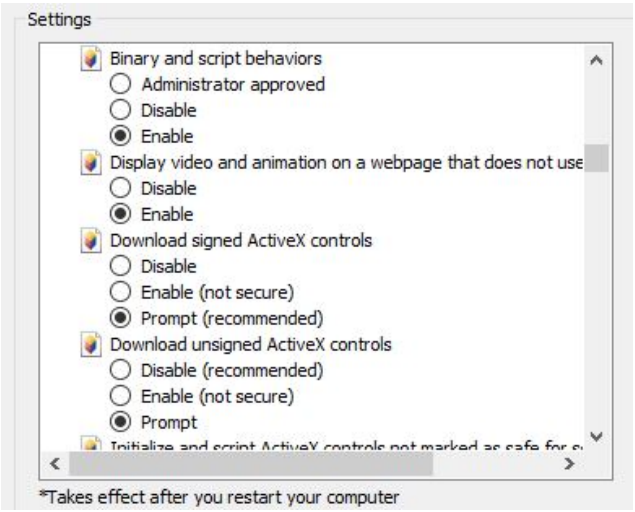


5. Binary and script behaviors **Enable**

6. Display video and animation on a webpage that does not use **Enable**

7. Download signed ActiveX controls **Prompt**

8. Download unsigned ActiveX controls **Prompt**

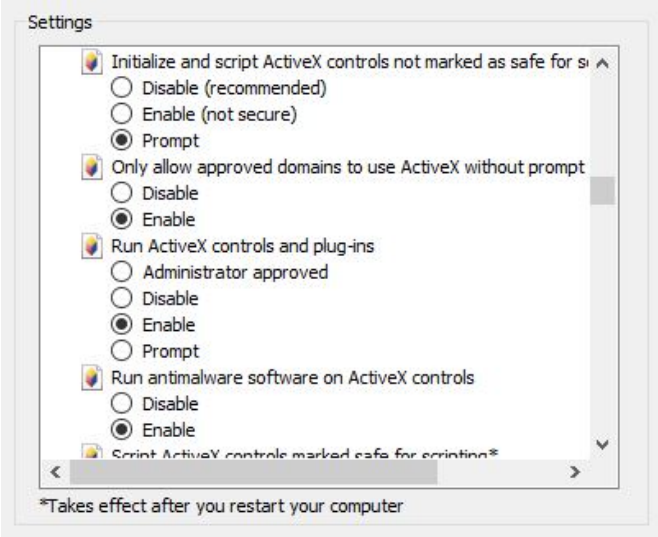


9. Initialize and script ActiveX controls not marked as safe **Prompt**

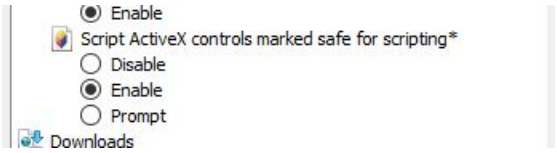
10. Only allow approved domains to use ActiveX without prompt **Enable**

11. Run ActiveX controls and plug-ins **Enable**

12. Run antimalware software on ActiveX controls **Enable**



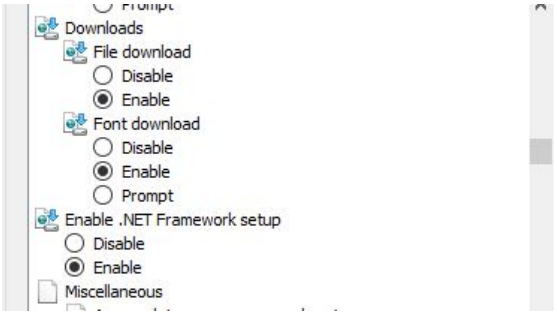
13. Script ActiveX controls marked safe for scripting **Enable**



Under Downloads

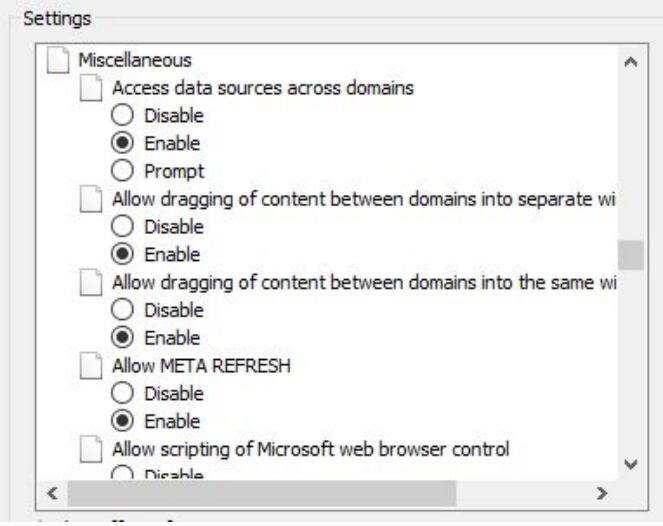
1. File download **Enable**
2. Font download **Enable**

Enable .NET framework setup Enable



Under Miscellaneous

1. Access data sources across domains **Enable**
2. Allow dragging of content between domains into separate **Enable**
3. Allow dragging of content between domains into same **Enable**
4. Allow META REFRESH **Enable**



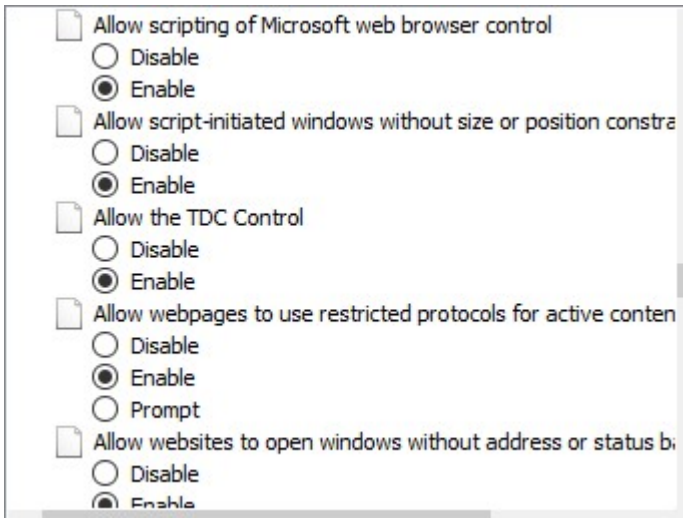
5. Allow scripting of Microsoft web browser control **ENABLE**

6. Allow script-initiated windows without size or position **ENABLE**

7. Allow the TDC Control **ENABLE**

8. Allow WebPages to use restricted protocols for active content **ENABLE**

9. Allow website to open windows without address or status bar **Enable**

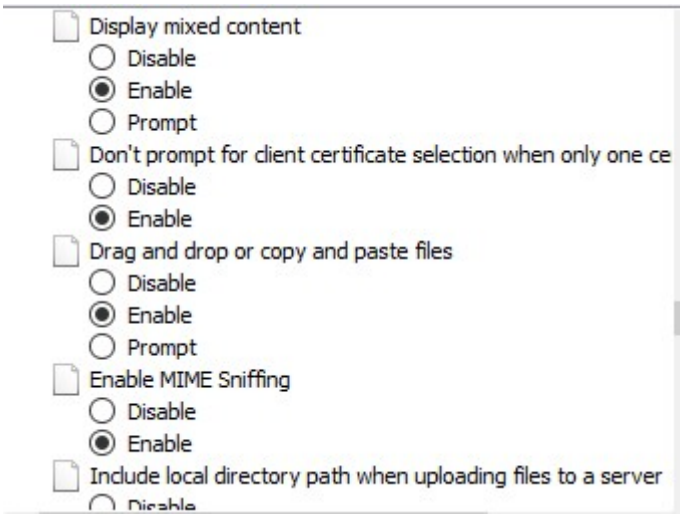


10. Display mixed content **Enable**

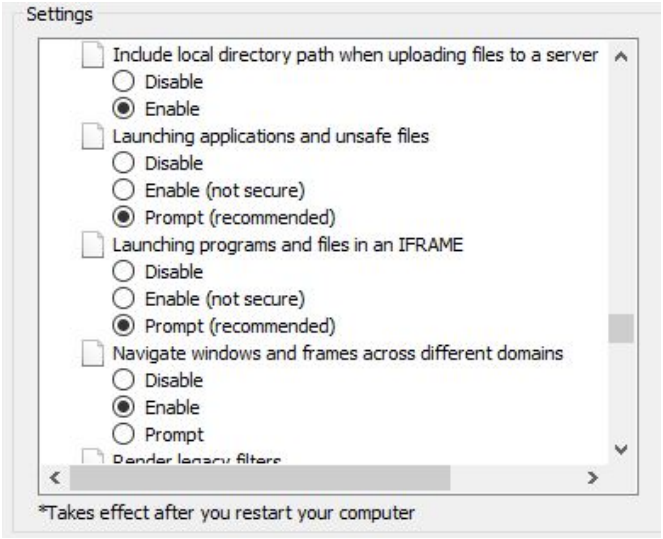
11. Don't prompt for client certificate selection when only one **Enable**

12. Drag and drop or copy and paste files **Enable**

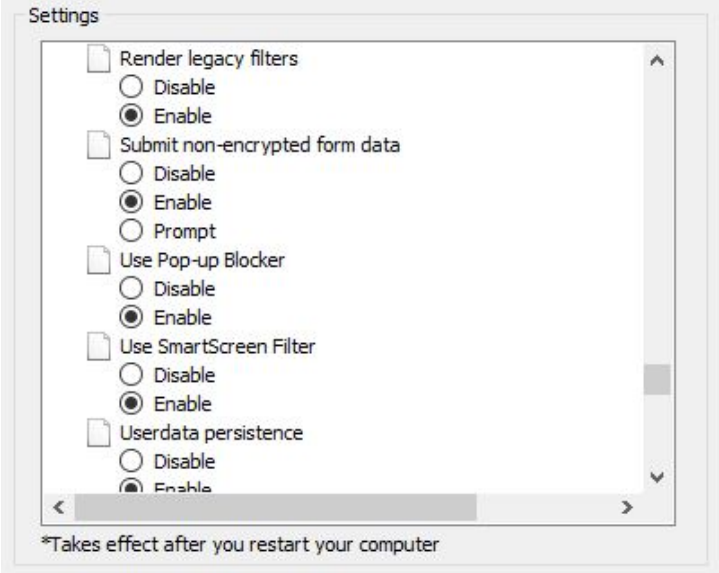
13. Enable MIME Sniffing **Enable**



14. Include local directory path when uploading files to server **ENABLE**
15. Launching application and unsafe files **Prompt (recommended)**
14. Launching programs and files in and IFRAME **Prompt (recommended)**
15. Navigate windows and frames across different domains **ENABLE**



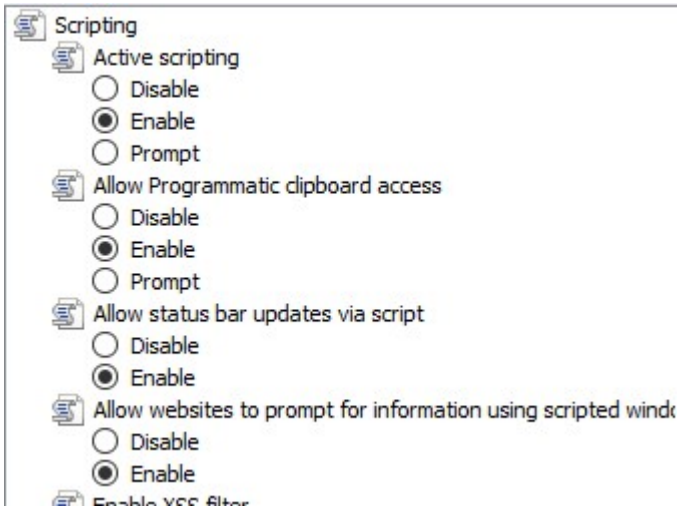
16. Render legacy filter **Enable**
17. Submit non-encrypted from data **Enable**
18. Use Pop-up Blocker **Enable**
19. Use Smart Screen Filter **Enable**
20. User data persistence **Enable**



21. Website in less privileged web content zone can navigate **Enable**

Under Scripting

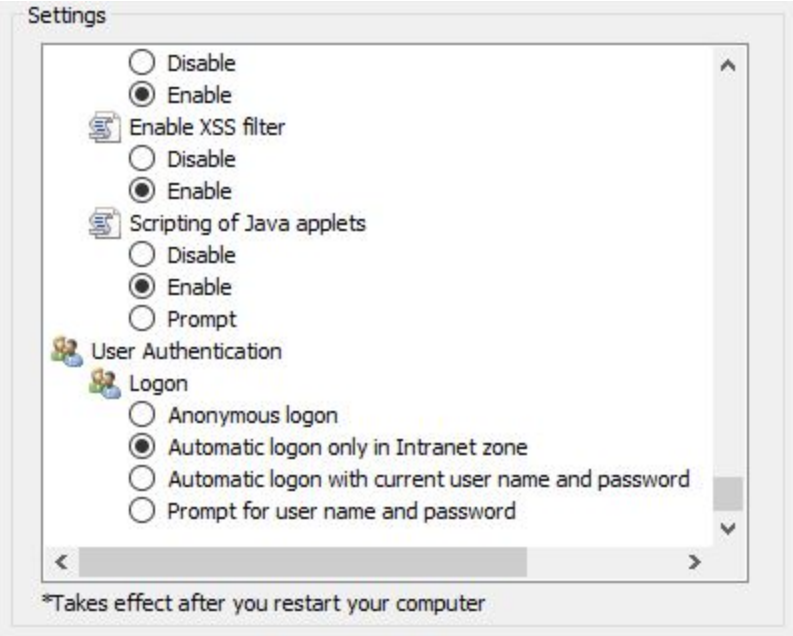
1. Active scripting **Enable**
2. Allow Programmatic clipboard access **Enable**
3. Allow status bar updates via script **Enable**
4. Allow website to prompt for information using scripted windows **Enable**



5. Enable XSS filter **Enable**
6. scripting of java applets **Enable**

User Authentication

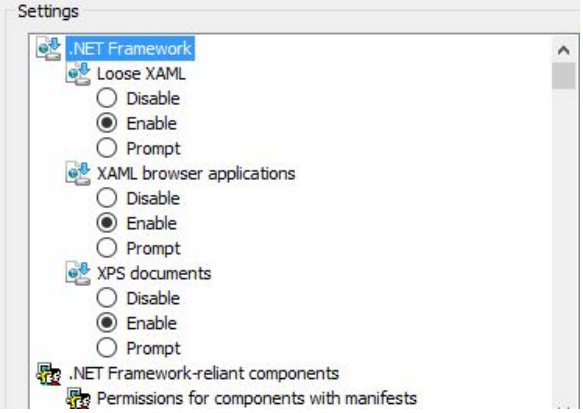
1. Select Automatic logon only in Intranet zone



Local Internet

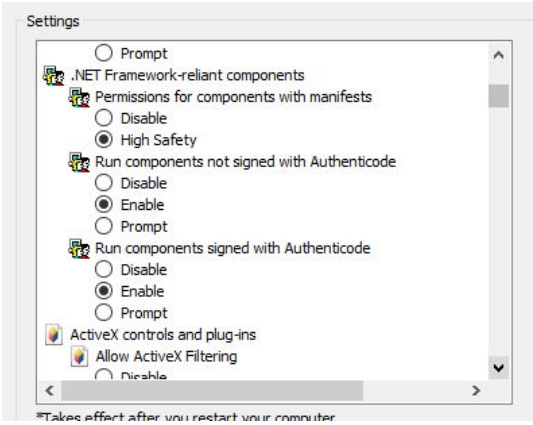
Under .NET Framework

1. Loose XAML **Enable**
2. XAML browser application **Enable**
3. XPS documents **ENABLE**



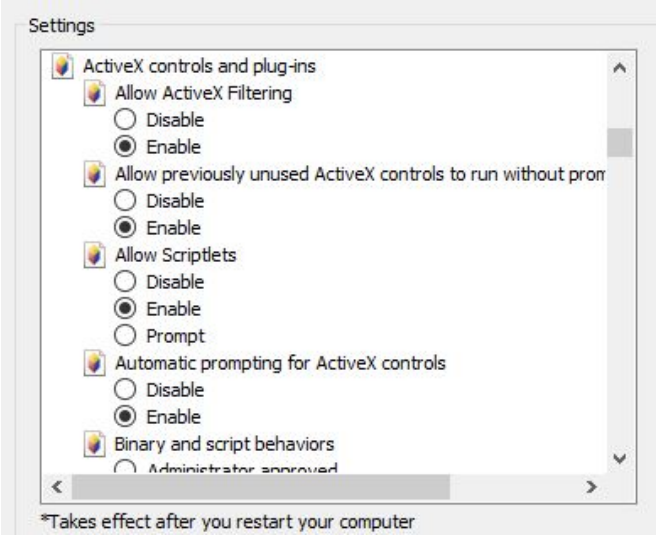
Under .NET Framework-reliant components

1. Permissions for components with manifests **High Safety**
2. Run components not signed with Authenticode **Enable**
3. Run components signed with Authenticode **Enable**



Under ActiveX controls and plug –INS

1. Allow ActiveX Filtering **Enable**
2. Allow previously unused ActiveX controls to run without program **Enable**
3. Allow Script lets **Enable**
4. Automatic prompting for ActiveX controls **Enable**

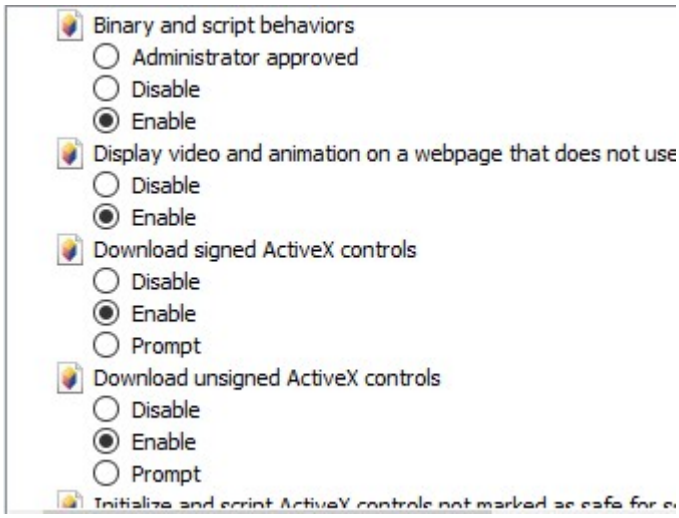


5. Binary and script behaviors **Enable**

6. Display video and animation on a webpage that does not use **Enable**

7. Download signed ActiveX controls **Enable**

8. Download unsigned ActiveX controls **Enable**

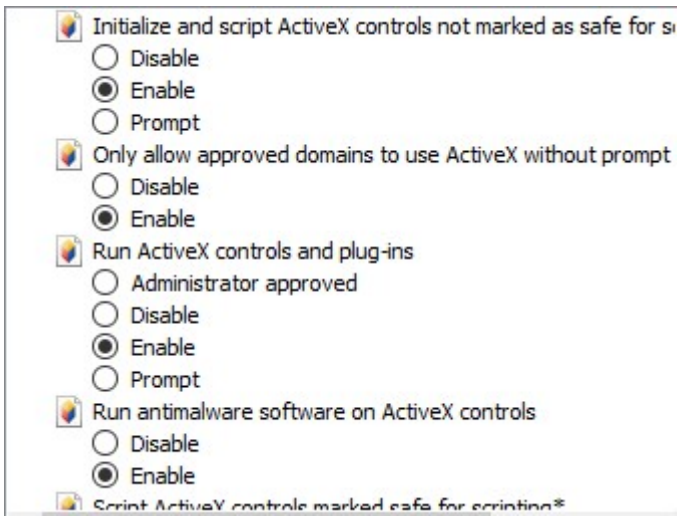


9. Initialize and script ActiveX controls not marked as safe **Enable**

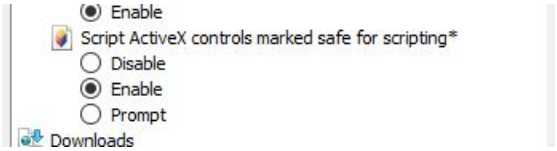
10. Only allow approved domains to use ActiveX without prompt **Enable**

11. Run ActiveX controls and plug-ins **Enable**

12. Run antimalware software on ActiveX controls **Enable**



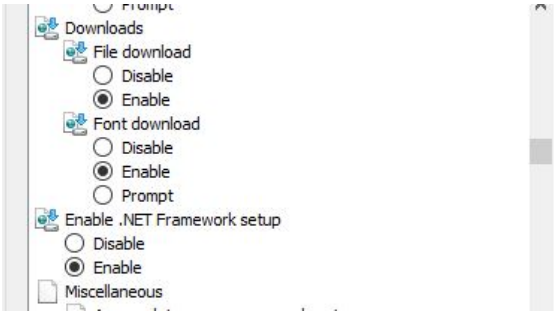
13. Script ActiveX controls marked safe for scripting **Enable**



Under Downloads

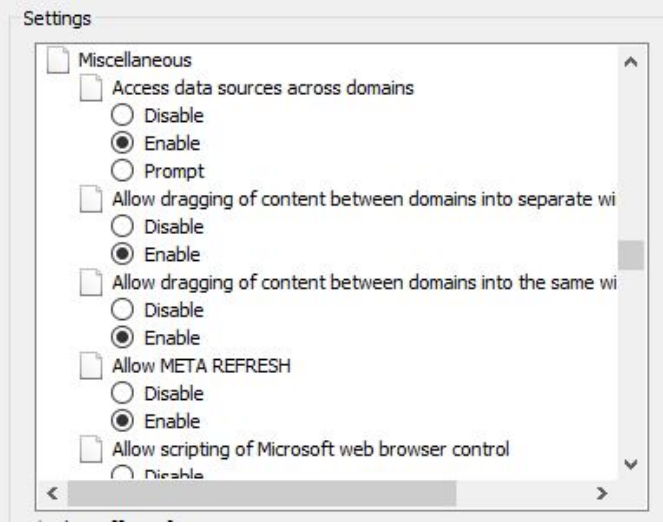
1. File download **Enable**
2. Font download **Enable**

Enable .NET framework setup Enable



Under Miscellaneous

1. Access data sources across domains **Enable**
2. Allow dragging of content between domains into separate **Enable**
3. Allow dragging of content between domains into same **Enable**
4. Allow META REFRESH **Enable**



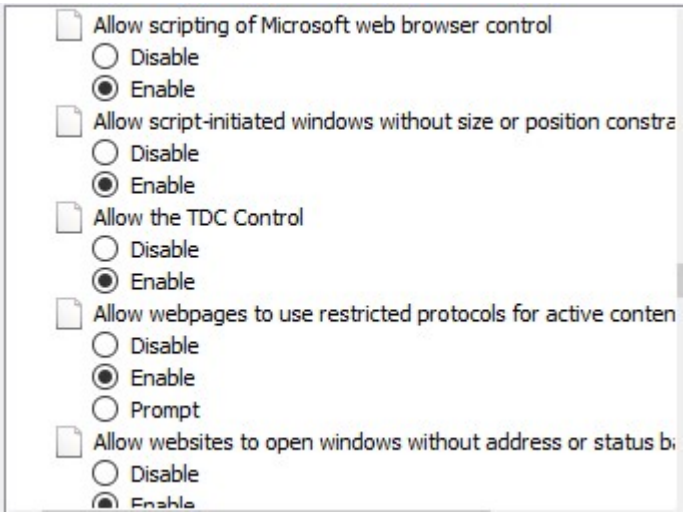
5. Allow scripting of Microsoft web browser control **ENABLE**

6. Allow script-initiated windows without size or position **ENABLE**

7. Allow the TDC Control **ENABLE**

8. Allow Webpages to use restricted protocols for active content **Enable**

9. Allow website to open windows without address or status bar **Enable**

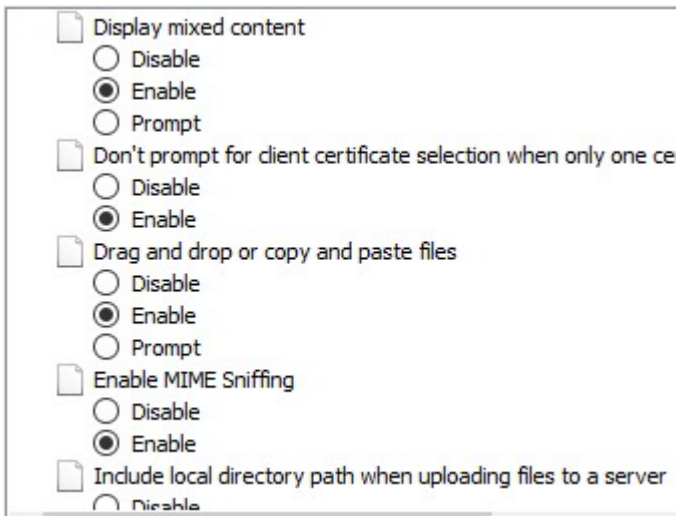


10. Display mixed content **Enable**

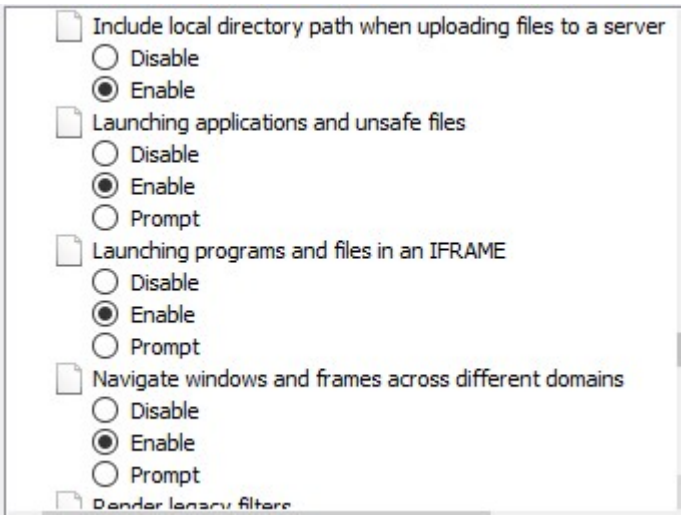
11. Don't prompt for client certificate selection when only one **Enable**

12. Drag and drop or copy and paste files **Enable**

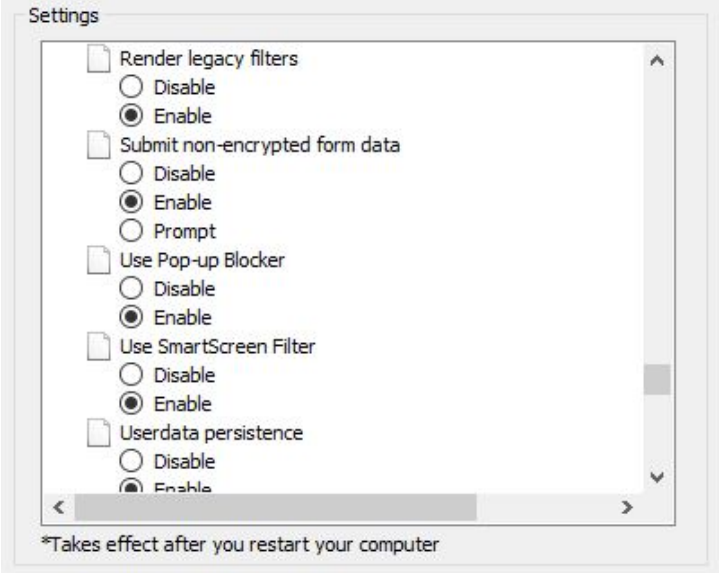
13. Enable MIME Sniffing **Enable**



14. Include local directory path when uploading files to server **ENABLE**
15. Launching application and unsafe files **Enable**
14. Launching programs and files in and IFRAME **Enable**
15. Navigate windows and frames across different domains **ENABLE**



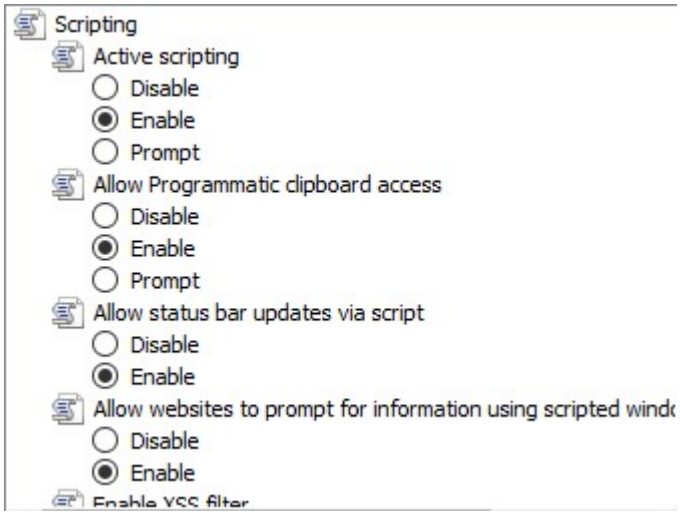
16. Render legacy filter **Enable**
17. Submit non-encrypted from data **Enable**
18. Use Pop-up Blocker **Enable**
19. Use Smart Screen Filter **Enable**
20. User data persistence **Enable**



21. Website in less privileged web content zone can navigate **Enable**

Under Scripting

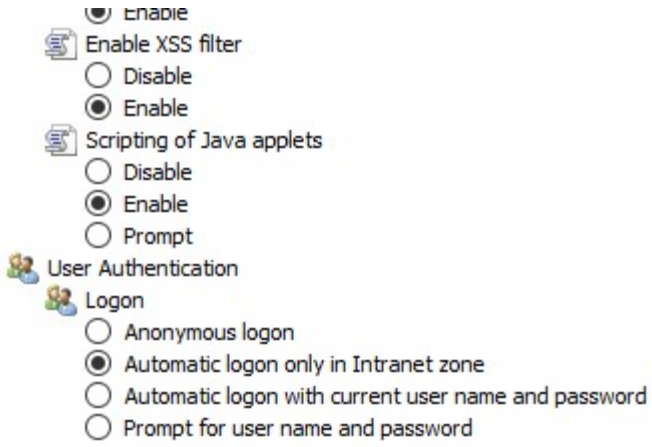
1. Active scripting **Enable**
2. Allow Programmatic clipboard access **Enable**
3. Allow status bar updates via script **Enable**
4. Allow website to prompt for information using scripted windows **Enable**



5. Enable XSS filter **Enable**
6. scripting of java applets **Enable**

User Authentication

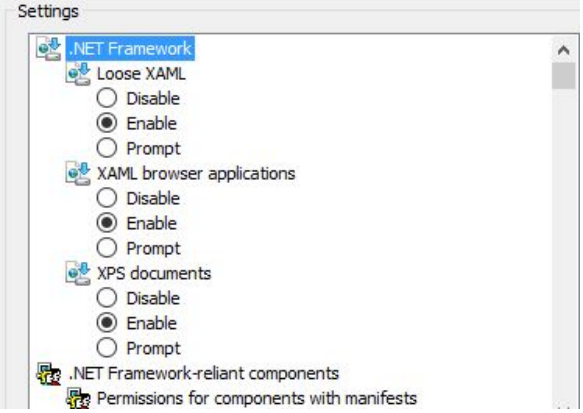
1. Select Automatic logon only in Intranet zone



Trusted Sites

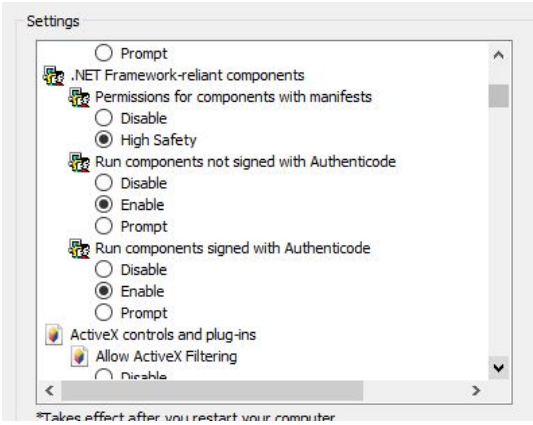
Under .NET Framework

1. Loose XAML **Enable**
2. XAML browser application **Enable**
3. XPS documents **ENABLE**



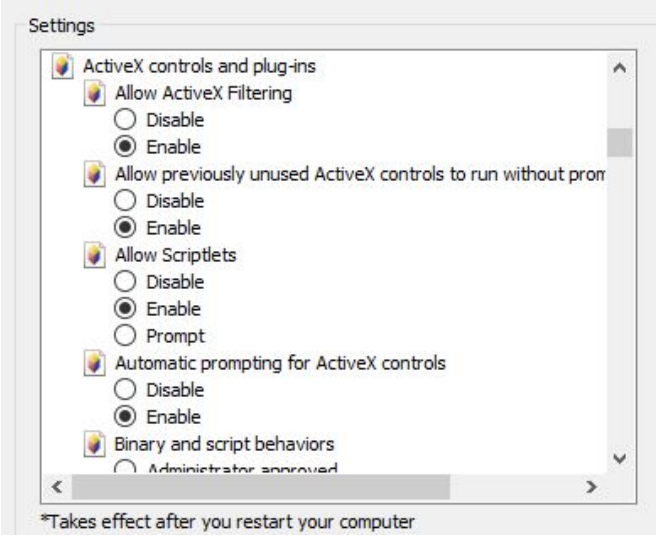
Under .NET Framework-reliant components

1. Permissions for components with manifests **High Safety**
2. Run components not signed with Authenticode **Enable**
3. Run components signed with Authenticode **Enable**



Under ActiveX controls and plug –INS

1. Allow ActiveX Filtering **Enable**
2. Allow previously unused ActiveX controls to run without program **Enable**
3. Allow Script lets **Enable**
4. Automatic prompting for ActiveX controls **Enable**

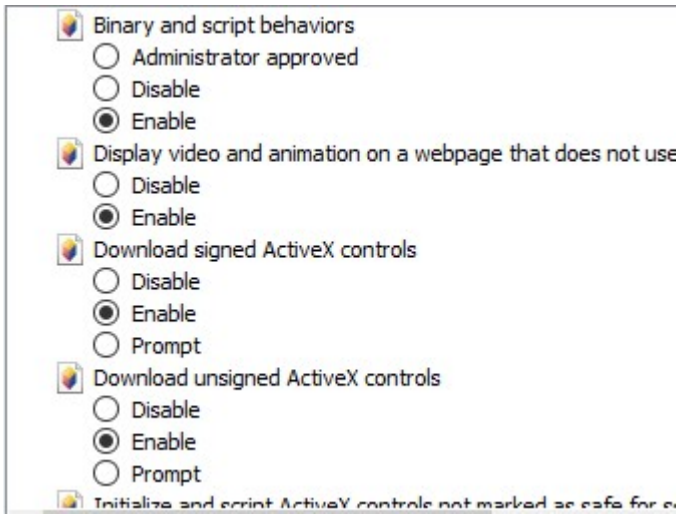


5. Binary and script behaviors **Enable**

6. Display video and animation on a webpage that does not use **Enable**

7. Download signed ActiveX controls **Enable**

8. Download unsigned ActiveX controls **Enable**

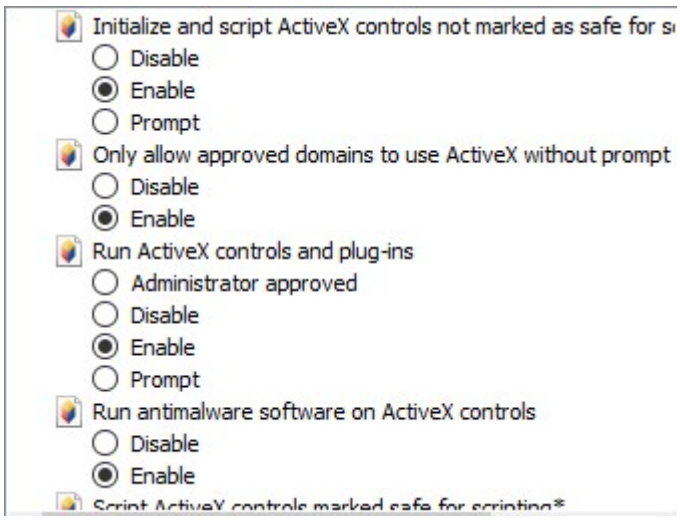


9. Initialize and script ActiveX controls not marked as safe **Enable**

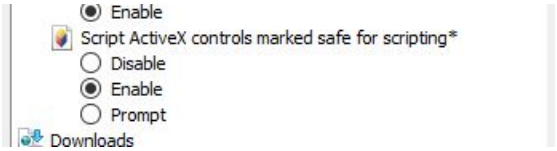
10. Only allow approved domains to use ActiveX without prompt **Enable**

11. Run ActiveX controls and plug-ins **Enable**

12. Run antimalware software on ActiveX controls **Enable**



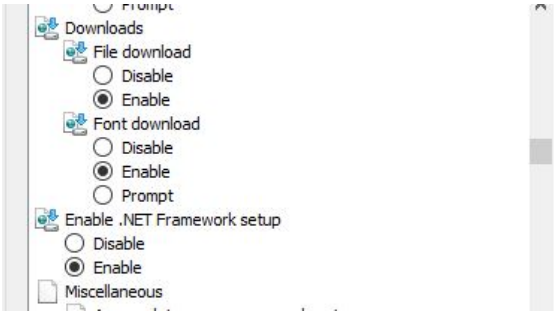
13. Script ActiveX controls marked safe for scripting **Enable**



Under Downloads

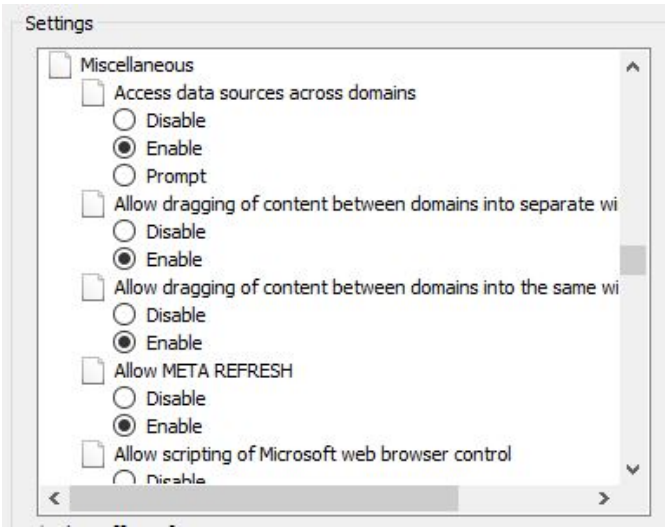
1. File download **Enable**
2. Font download **Enable**

Enable .NET framework setup Enable



Under Miscellaneous

1. Access data sources across domains **Enable**
2. Allow dragging of content between domains into separate **Enable**
3. Allow dragging of content between domains into same **Enable**
4. Allow META REFRESH **Enable**



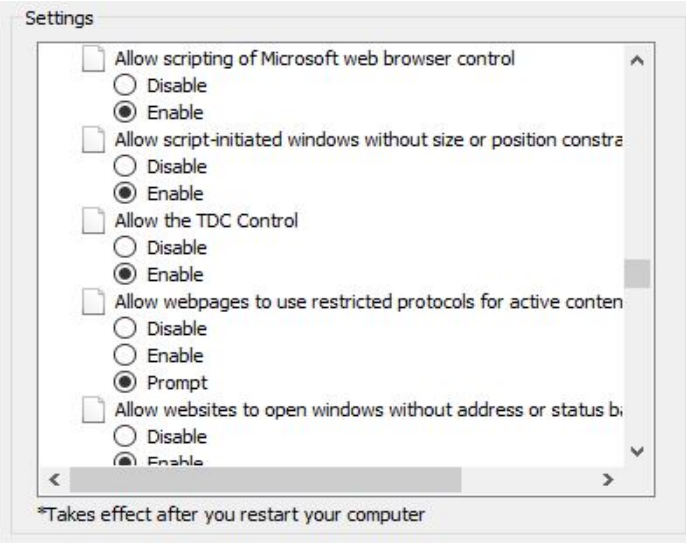
5. Allow scripting of Microsoft web browser control **ENABLE**

6. Allow script-initiated windows without size or position **ENABLE**

7. Allow the TDC Control **ENABLE**

8. Allow Webpages to use restricted protocols for active content **Enable**

9. Allow website to open windows without address or status bar **Enable**

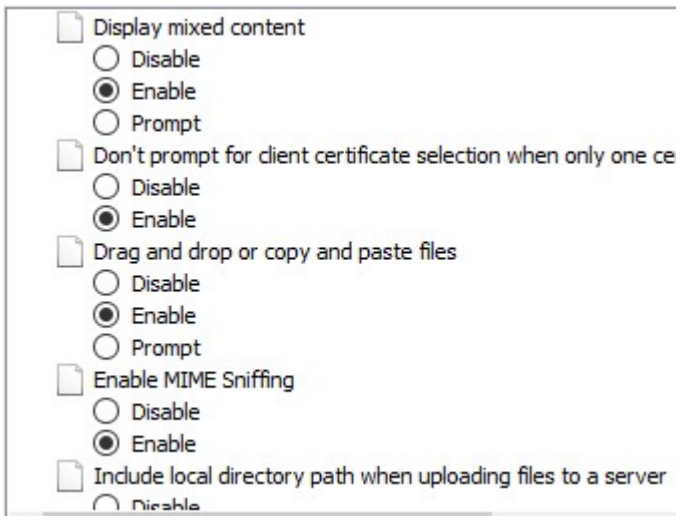


10. Display mixed content **Enable**

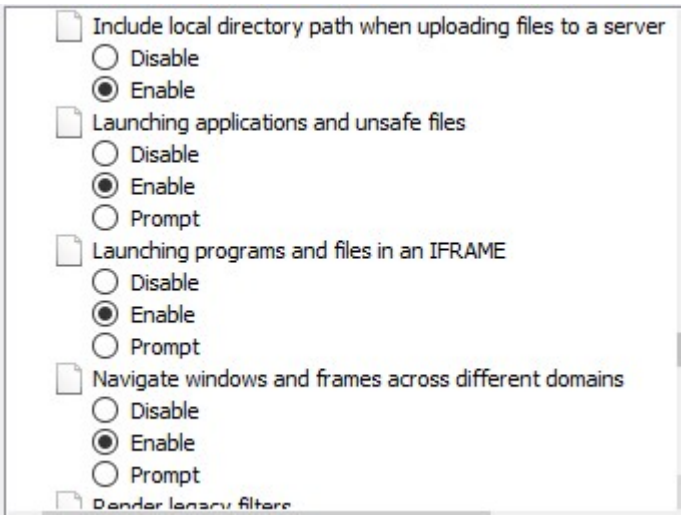
11. Don't prompt for client certificate selection when only one **Enable**

12. Drag and drop or copy and paste files **Enable**

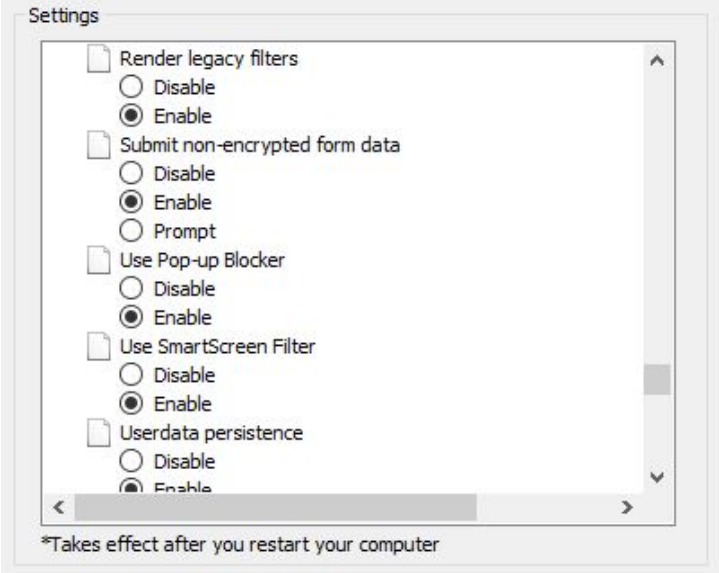
13. Enable MIME Sniffing **Enable**



14. Include local directory path when uploading files to server **ENABLE**
15. Launching application and unsafe files **Enable**
14. Launching programs and files in and IFRAME **Enable**
15. Navigate windows and frames across different domains **ENABLE**



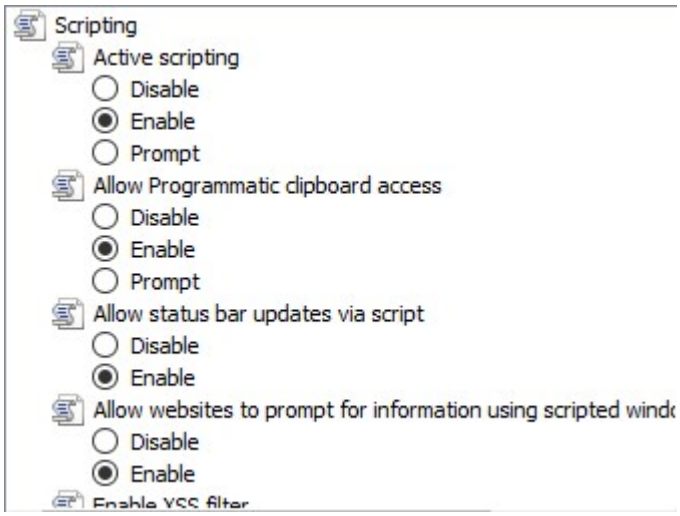
16. Render legacy filter **Enable**
17. Submit non-encrypted from data **Enable**
18. Use Pop-up Blocker **Enable**
19. Use Smart Screen Filter **Enable**
20. User data persistence **Enable**



21. Website in less privileged web content zone can navigate **Enable**

Under Scripting

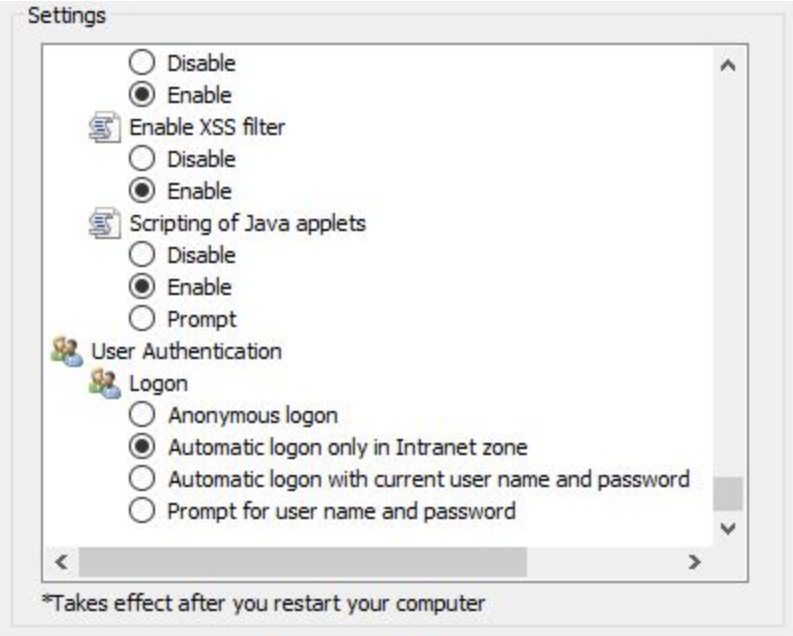
1. Active scripting **Enable**
2. Allow Programmatic clipboard access **ENABLE**
3. Allow status bar updates via script **Enable**
4. Allow website to prompt for information using scripted windows **Enable**



5. Enable XSS filter **Enable**
6. scripting of java applets **Enable**

User Authentication

1. Select Automatic logon only in Intranet zone



Trusted Sites: -

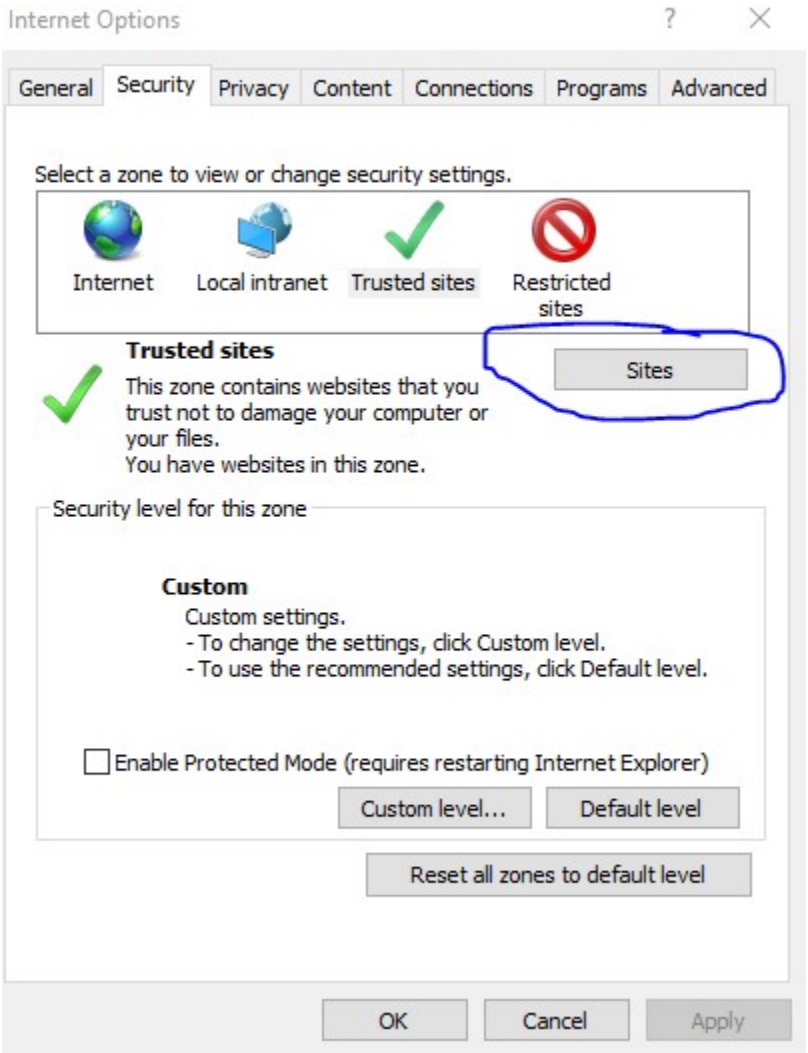
⇨ Once the above configuration is done, Add the Below URL's in Trusted Sites.

URL 1:- https://tservicegateway.azurewebsites.net

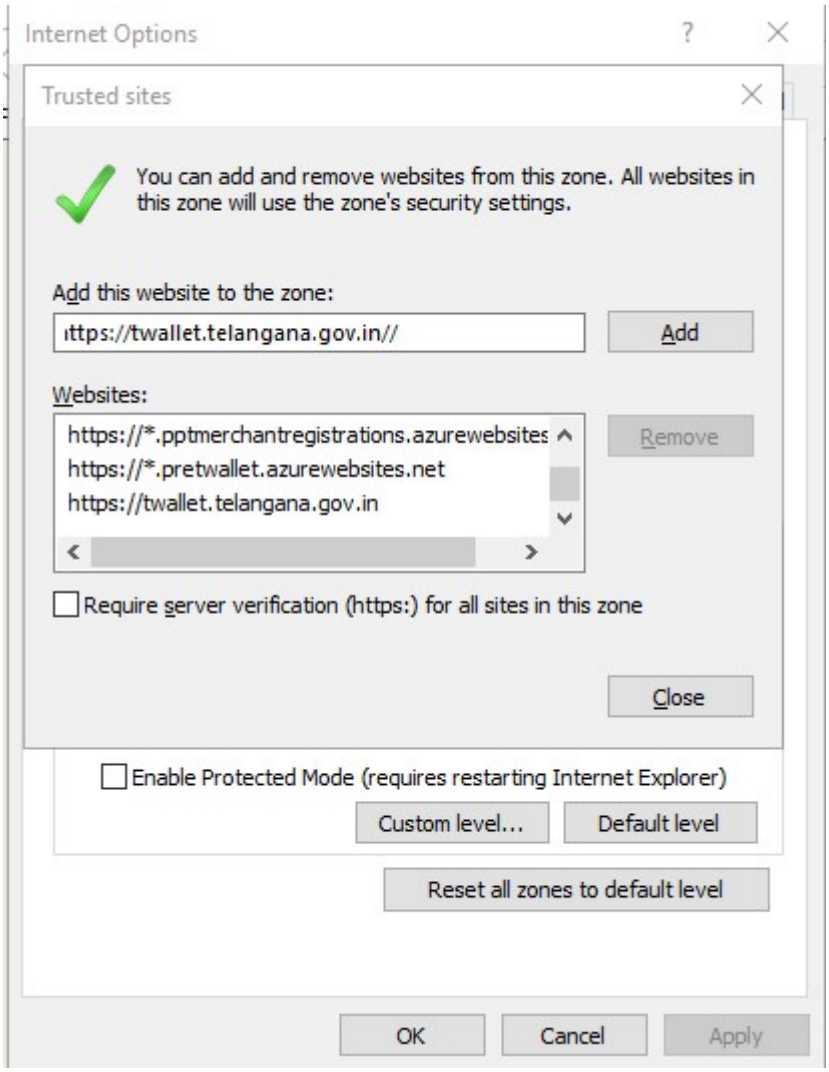
URL 2:- https://merchantregistrations.azurewebsites.net

URL 3:- https://twallet.telangana.gov.in

⇨ Click on **Sites** button under **Trusted Sites** tab,



⇨ In the **sites** window, add the above three URL's.


Internet Options
Trusted sites
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Add this website to the zone:
ıttps://twallet.telangana.gov.in//
Add
Websites:
https://*.pptmerchantregistrations.azurewebsites
https://*.pretwallet.azurewebsites.net
https://twallet.telangana.gov.in
Remove
Require server verification (https:) for all sites in this zone
Close
Enable Protected Mode (requires restarting Internet Explorer)
Custom level...
Default level
Reset all zones to default level
OK
Cancel
Apply