

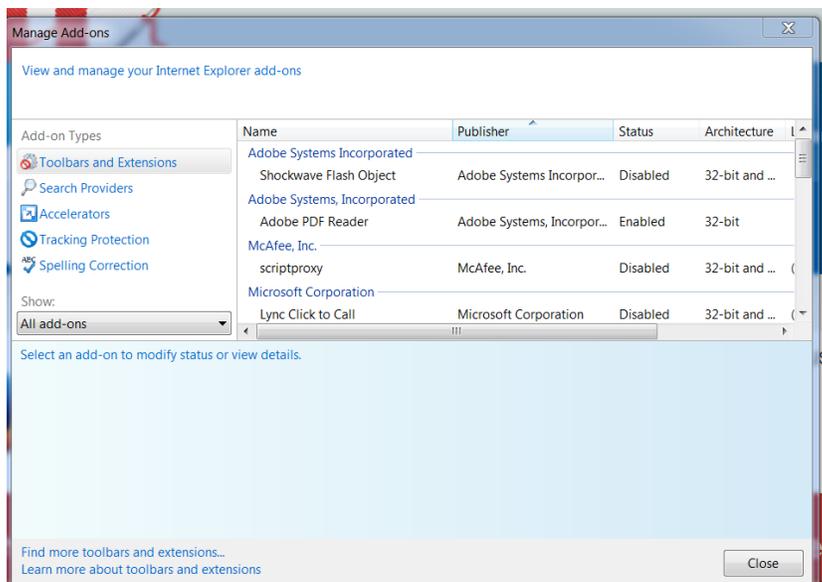
Recommended Browser Modifications to lessen the impact of IE Vulnerability

April 29, 2014

The following steps below are only temporary changes that are recommended until the IE Microsoft Patch is released. DAS BEST Security Team will notify agencies when the patch is available for download. Please assess the recommendations below to best suit your agency business requirements. We advise that you test these modifications before full deployment in any environment.

Option One:

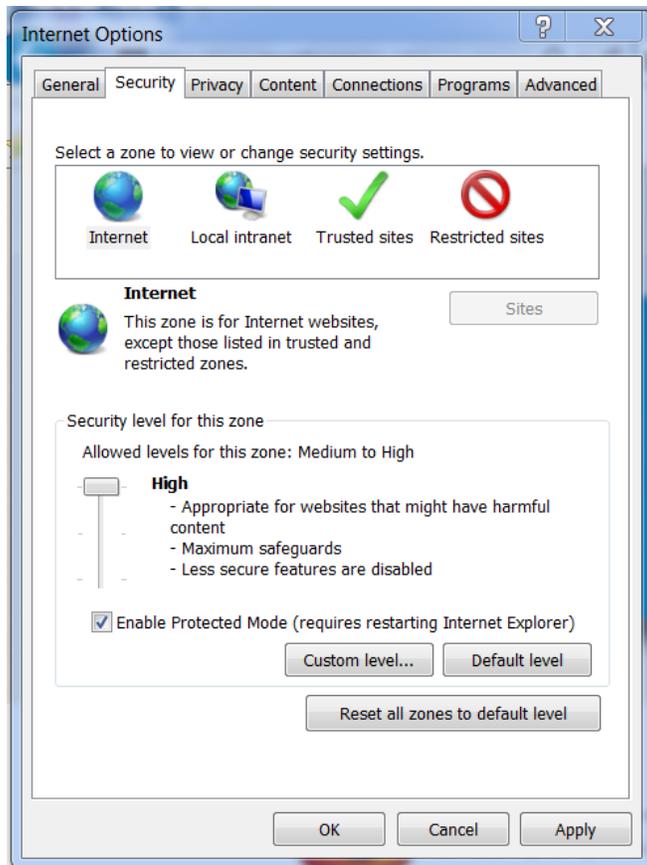
1. Modification of Internet Explorer to decrease the risks is recommended:
 - a. Go to Tools – Manage Add On, and Disable Shockwave Flash Object, under Adobe Systems Incorporated. Click Ok and Close Settings.



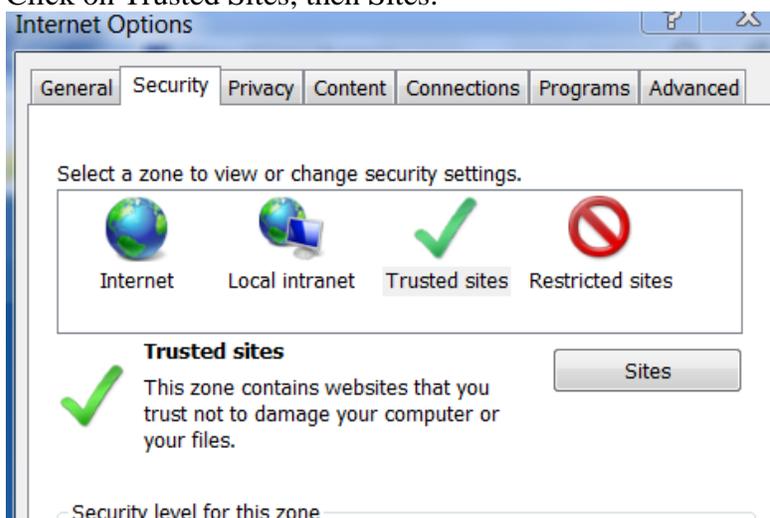
Known Risk: Disabling Adobe Shockwave Flash in IE will prevent the user from viewing certain websites from displaying properly.

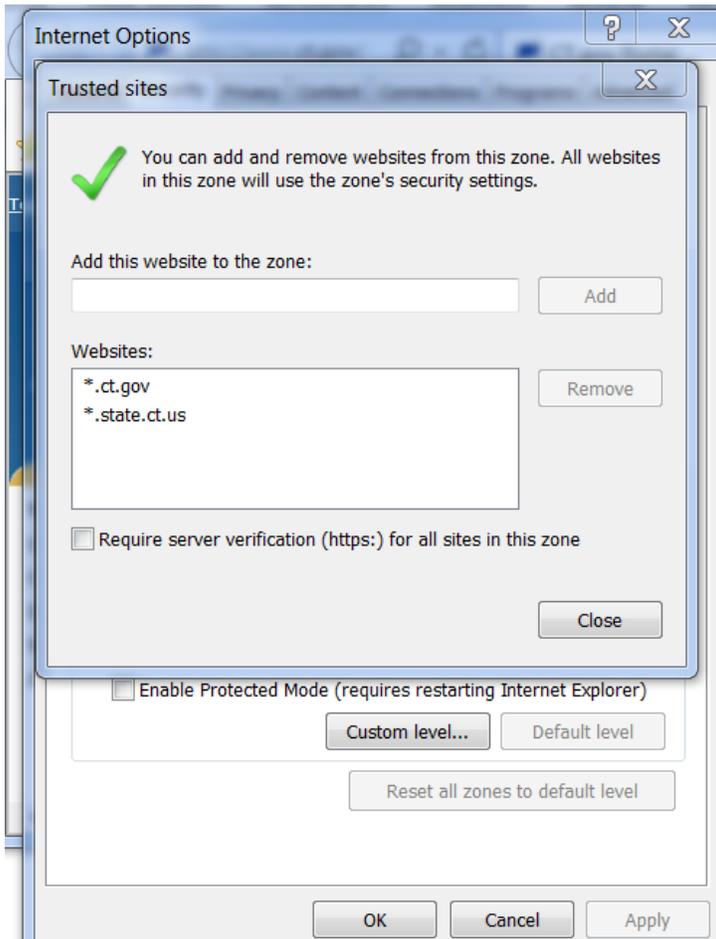
2. Set Internet and Local intranet security zone settings to "High" by clicking on Tools – Internet Options – Security tab. Next, set the level to High, click Apply.

Known Risk: Modifying the Security Settings to High will block various websites to your IE browser, such as Core-CT, unless you add the Trusted Sites as indicated below in Step 3.



3. Click on Trusted Sites, then Sites.



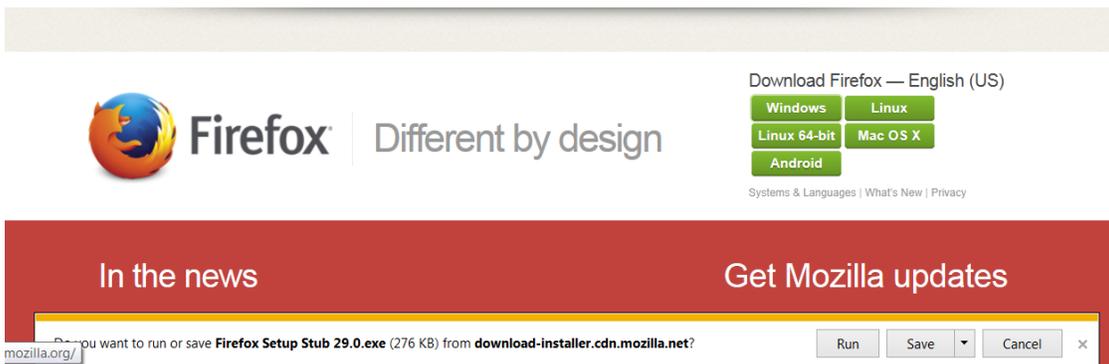


Add *.ct.gov and *.state.ct.us to the Trusted Sites. Click Close, then Apply, and OK.

Option Two:

1. External Website that you must go to that utilize Adobe Flash, download Mozilla Firefox via the direct link Mozilla.org as seen below.

<http://www.mozilla.org/en-US/>



Known Risk: Since Mozilla Firefox is not a state architectural standard browser, we cannot predict the potential behavior of the browser and websites.

Option Three:

1. If applicable, notify your agency Active Directory Administrator to discuss Group Policy changes that can globally modify the Internet Explorer settings to meet your agency needs.

Contact the DAS BEST HELP DESK at 860-622-2300 Option 9 if further assistance is needed.