

Setting up Internet Explorer 7 for use with **VUEWorks**

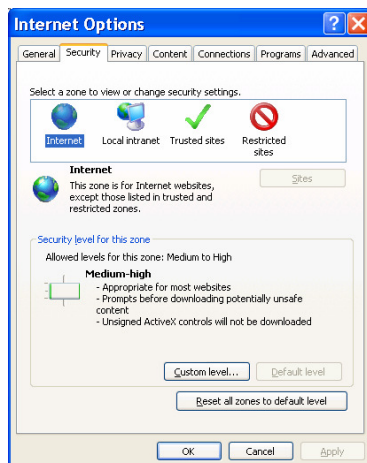
VUEWorks Version 2.5 and above is designed to work with Internet Explorer 6 SP1 and Internet Explorer 7. However, Internet Explorer 7 introduced many new security settings that may make VUEWorks more difficult to use if left at the default settings. The purpose of this document is to show how to best set up Internet Explorer 7 for use with VUEWorks. Users of Internet Explorer 6 are advised to follow these procedures too – just ignore any settings that you do not have an option for.

For users who access VUEWorks over the Internet

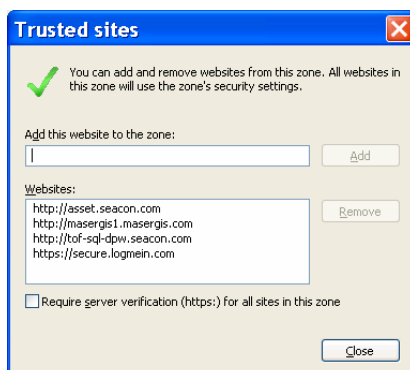
Skip this section if you access VUEWorks through a local network

You need to make sure your VUEWorks site is listed as a Trusted Site in Internet Explorer. To do this, follow these instructions:

1. Open Internet Explorer and select Tools...Internet options. Then select the Security tab. You should see a screen that looks like this:



2. Add your VUEWorks site to the Trusted Sites zone. You need to know the main path to your site and then enter it in the list of Trusted Sites. Click once on the Trusted Sites icon, then click on the Sites button to see a screen that looks like this:



Type in the box the main http: path to your site. If you do not know the path, check with your VUEWorks administrator.

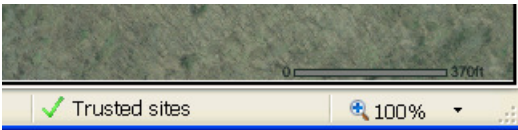
Make sure the 'Require server verification (https:) for all sites in this zone is checked off
Press Close when done to return to the previous window

For all users: Set the proper settings for your zone

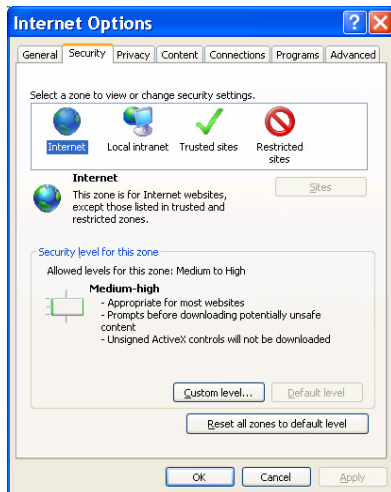
If your VUEWorks server is located on your local network then you are accessing it through the Local Intranet zone. To verify your zone, log on to VUEWorks and then look at the lower right corner of the Internet Explorer window. It should say either 'Local intranet' or 'Trusted sites':



-or-



After you have verified your zone, exit VUEWorks, open a fresh instance of Internet Explorer and open Internet Options as described in step one in the previous section.



If your zone is Local intranet, then select the Local intranet icon. If your zone is Trusted sites, the select the Trusted sites icon.

Now press the Custom level... button. On the following page is a list of how all the settings should be. Proceed to make your settings the same. If you have a setting that is not listed here then please contact VUEWorks.

VUEWorks recommended settings for custom level security

IMPORTANT:

USE THESE SETTINGS ONLY FOR LOCAL INTRANET AND/OR TRUSTED SITES ZONES. NEVER USE THESE SETTINGS FOR THE INTERNET ZONE

Settings that are known to cause issues with VUEWorks if incorrectly set are bracketed in red

The screenshot displays the Internet Explorer Security Settings window, organized into several categories. The following table summarizes the settings shown, with those highlighted in red in the original image marked as 'Red Boxed'.

Category	Setting Name	Selected Option	Red Boxed
.NET Framework	Loose XAML	Enable	
	XAML browser applications	Enable	
	XPS documents	Enable	
	.NET Framework-reliant components	Run components not signed with Authenticode: Enable	
		Run components signed with Authenticode: Enable	
	ActiveX controls and plug-ins	Allow previously unused ActiveX controls to run without prompt: Enable	
		Allow Scriptlets: Enable	
		Automatic prompting for ActiveX controls: Enable	
		Binary and script behaviors: Administrator approved	
		Display video and animation on a webpage that does not have the video or animation: Enable	
		Download signed ActiveX controls: Prompt	
		Download unsigned ActiveX controls: Prompt	Red Boxed
		Initialize and script ActiveX controls not marked as safe for scripting: Enable	
		Run ActiveX controls and plug-ins: Administrator approved	
		Script ActiveX controls marked safe for scripting: Enable	
Downloads	Automatic prompting for file downloads: Enable		
	File download: Enable		
	Font download: Enable		
	Enable .NET Framework setup: Enable		
	Miscellaneous	Access data sources across domains: Enable	
		Allow META REFRESH: Enable	
		Allow scripting of Internet Explorer web browser control: Enable	
	Allow script-initiated windows without size or position constraints: Enable		
	Content Advisor	Allow script-initiated windows without size or position constraints: Enable	
		Allow webpages to use restricted protocols for active content: Enable	
Allow websites to open windows without address or status bar: Enable			
Display mixed content: Enable			
Don't prompt for client certificate selection when no certificate is available: Enable			
Drag and drop or copy and paste files: Enable			
Include local directory path when uploading files to a server: Enable			
Installation of desktop items: Prompt			
Launching applications and unsafe files: Prompt			
Launching programs and files in an IFRAME: Prompt			
Navigate sub-frames across different domains: Enable			
Open files based on content, not file extension: Enable			
Software channel permissions: Low safety			
Submit non-encrypted form data: Enable			
Use Phishing Filter: Disable		Red Boxed	
Use Pop-up Blocker: Disable		Red Boxed	
Userdata persistence: Enable			
Websites in less privileged web content zone can navigate to more privileged zones: Enable			
Scripting		Active scripting: Enable	
		Allow Programmatic clipboard access: Enable	Red Boxed
		Allow status bar updates via script: Enable	
Allow websites to prompt for information using scripted windows: Enable			
Scripting of Java applets: Enable			
User Authentication		Logon: Automatic logon only in Intranet zone	
			Automatic logon with current user name and password
		Prompt for user name and password	
		Anonymous logon	