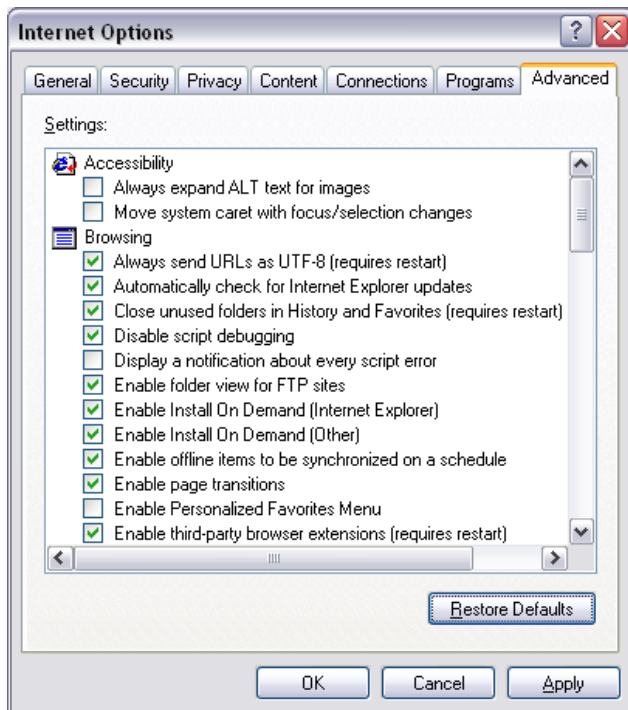


Configuring Advanced IE Options

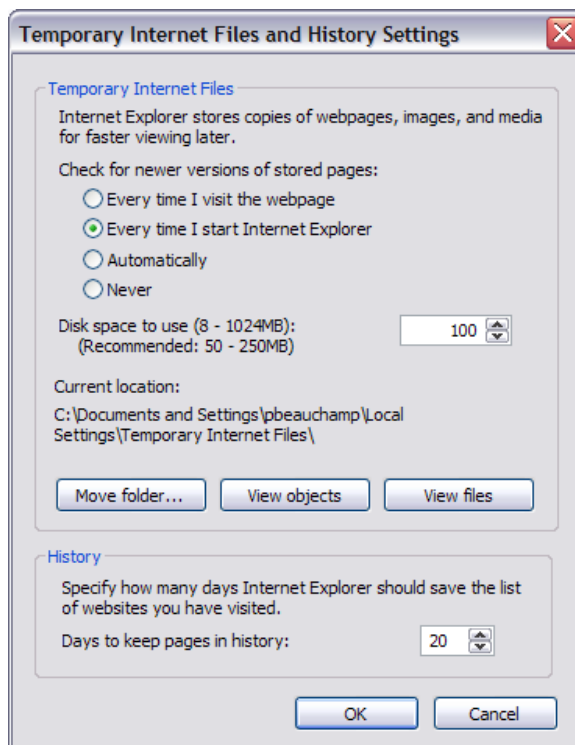
1. Open IE, Select Tools/**Internet Options** menu.
2. On **Advanced** tab, click **Restore Defaults** button.
3. Ensure "Enable third-party browser extensions" is checked.
4. Ensure "Use smooth scrolling" is unchecked (for performance reasons)
5. Uncheck Do not save encrypted pages to disk
6. Optional; Uncheck "Disable script debugging"
7. Optional; Uncheck "Show friendly HTTP error messages"

Note: 6 & 7 above are helpful in troubleshooting problems errors within TouchWorks.



Configuring General IE Options

1. Open IE, Select Tools/**Internet Options** menu.
2. On General tab, section Temporary Internet files, click Settings button (located under browsing history for IE7) and set the option for “Check for newer versions of stored pages:” to **“Every time you start Internet Explorer”**.
3. Allow between 75 and 100 MB for temporary files. Save your settings by clicking OK
4. **Save** your new configuration by clicking Apply and OK buttons.
5. **Install the ActiveX controls** for TouchWorks per your preferred method – Push Technology strongly suggested.
(ref: [ActiveX Deployment Options](#))



Configuring Security IE Settings

Internet explorer comes with 4 pre defined security zones. The URL which is used to access the TouchWorks web application must appear in either the Trusted Sites or Local Intranet Zone. Allscripts recommends always accessing the TouchWorks Application via a FQDN and therefore suggests using the Trusted Site Zone. Regardless of what zone you define the TouchWorks URL in, security settings in those zones may need to be adjusted. Below is a summary of the settings that may be required in a local PC's Internet Explorer Zone Configuration.

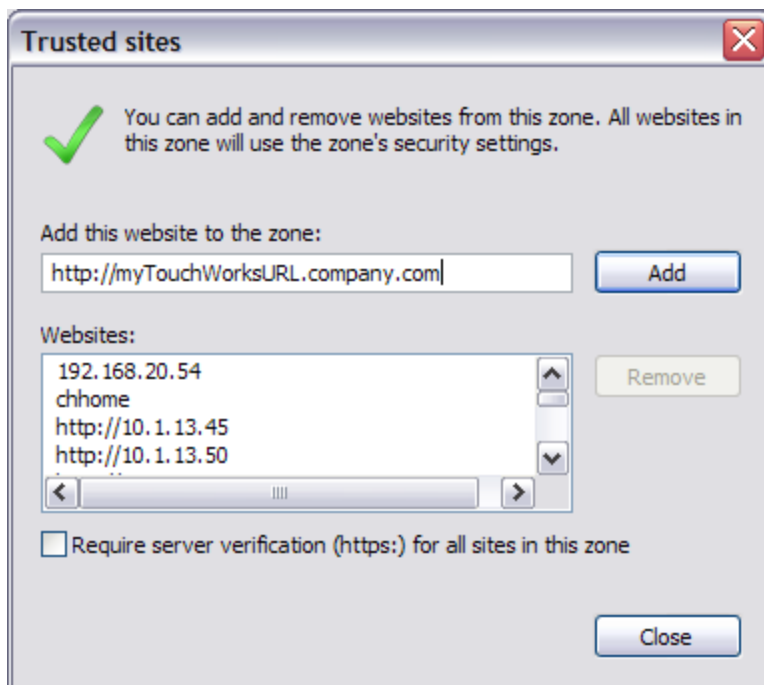
You can either use the Allscripts provided "[IETrustedSites.msi](#)" kit which runs a wizard interface to set up a client PC, or you may add the site manually. Group Policy or the IEAK can be used to manage client IE settings as well.



The Procedures below indicate the settings steps for manually configuring a PC's IE Security Zones for TouchWorks

Manually add TouchWorks URL to Trusted Sites zone

1. Open IE, Select Tools/**Internet Options** menu.
2. Click on the Security Tab and then select *Trusted Sites*
3. Click the Sites button
4. Type in your TouchWorks URL and then click Add
5. Click the Close Button



Configure Trusted Site Security

Now that your TouchWorks URL has been added to the Trusted Site Zone, you will need to verify that the security level for this zone has been set up with all of the configurations needed for running TouchWorks on your PC.

1. From within the Security Tab of Internet Options, click 'Custom Level' (make sure you have Trusted sites highlighted prior to doing this)
2. Configure the Security settings per the table below:
 *** Settings pertaining to the downloading of ActiveX controls are optional. They can be set to Disable if there is a policy in place to install ActiveX controls via push technology.

Category	Setting	Default	TouchWorks Setting
.NET Framework	Loose XAML	Enable	Enable
	XAML browser applications	Enable	Enable
	XPS documents	Enable	Enable
.NET Framework-reliant components	Run components not signed with Authenticode	Enable	Enable
	Run components signed with Authenticode	Enable	Enable
ActiveX Controls and Plug-ins	Allow previously unused ActiveX controls to run without prompt	Disable	Prompt
	Allow Scriptlets	Disable	Enable
	Automatic prompting for ActiveX controls	Disable	Enable
	Binary and script behaviors	Enable	Enable
	Display video and animation on a webpage that does not use external media player	Disable	Disable
	Download signed ActiveX controls	Prompt	Enable***
Download unsigned ActiveX controls	Disable	Prompt***	

	Initialize and script ActiveX controls not marked as safe for scripting	Disable	Disable
	Run ActiveX controls and plug-ins	Enable	Enable
	Script ActiveX controls marked safe for scripting	Enable	Enable
Downloads	Automatic prompting for file downloads	Disable	Disable
	File download	Enable	Enable
	Font download	Enable	Enable
Enable .NET Framework setup	Enable .NET Framework setup	Enable	Enable
Miscellaneous	Access data sources across domains	Disable	Enable
	Allow META REFRESH	Enable	Enable
	Allow scripting of Internet Explorer web browser control	Disable	Disable
	Allow script-initiated windows without size or position constraints	Disable	Enable
	Allow webpages to use restricted protocols for active content	Prompt	Prompt
	Allow websites to open windows without address or status bars	Disable	Enable
	Display mixed content	Prompt	Enable
	Don't prompt for client certificate selection when no certificates or only one certificate exists	Disable	Disable
	Drag and drop or copy and paste files	Enable	Enable

	Include local directory path when uploading files to a server	Enable	Enable
	Installation of desktop items	Prompt	Prompt
	Launching applications and unsafe files	Prompt	Prompt
	Launching programs and files in an IFRAME	Prompt	Prompt
	Navigate sub-frames across different domains	Disable	Disable
	Open files based on content, not file extension	Enable	Enable
	Software channel permissions	Medium safety	Medium safety
	Submit non-encrypted form data	Enable	Enable
	Use Phishing Filter	Enable	Enable
	Use Pop-up Blocker	Enable	Disable
	Userdata persistence	Enable	Enable
	Websites in less privileged web content zone can navigate into this zone	Enable	Enable
	Scripting	Active scripting	Enable
Allow Programmatic clipboard access		Prompt	Prompt
Allow status bar updates via script		Disable	Disable
Allow websites to prompt for information using scripted windows		Disable	Disable
Scripting of Java applets		Enable	Enable
User Authentication	Logon	Automatic logon only in Intranet	Automatic logon only in Intranet zone

