Setting Up Pro/Web.Link

This section instructions to setup Pro/Web.Link.

See the *Pro/ENGINEER Installation and Administration Guide* for information on how to install Pro/Web.Link.

Topic

Supported Hardware

For Pro/ENGINEER Wildfire 2.0, Pro/Web.Link supports both Windows and UNIX platforms. On Windows you can use Pro/Web.Link in the embedded browser. On UNIX platforms you can use Pro/Web.Link in the Mozilla embedded browser.

Supported Software

Pro/Web.Link in the embedded browser supports the browsers supported by Pro/ENGINEER, specified at http://www.ptc.com/partners/hardware/current/proe.htm

Security on Windows

Operations performed using Pro/Web.Link in the embedded browser can read and write information in the Pro/ENGINEER session and from the local disk. Because of this, Pro/Web.Link in Pro/ENGINEER Wildfire uses three levels of security:

- Pro/Web.Link code only functions in web pages loaded into the Pro/ENGINEER embedded browser. Pages containing Pro/Web.Link code will not work if the user browses to them using external web browsers.
- Pro/Web.Link is disabled by default using a Pro/ENGINEER configuration option.
- The Pro/Web.Link ActiveX control has been created as not safe for scripting. This requires that security settings be enabled in Internet Explorer, allowing only certain sites access to the Pro/Web.Link methods and objects.

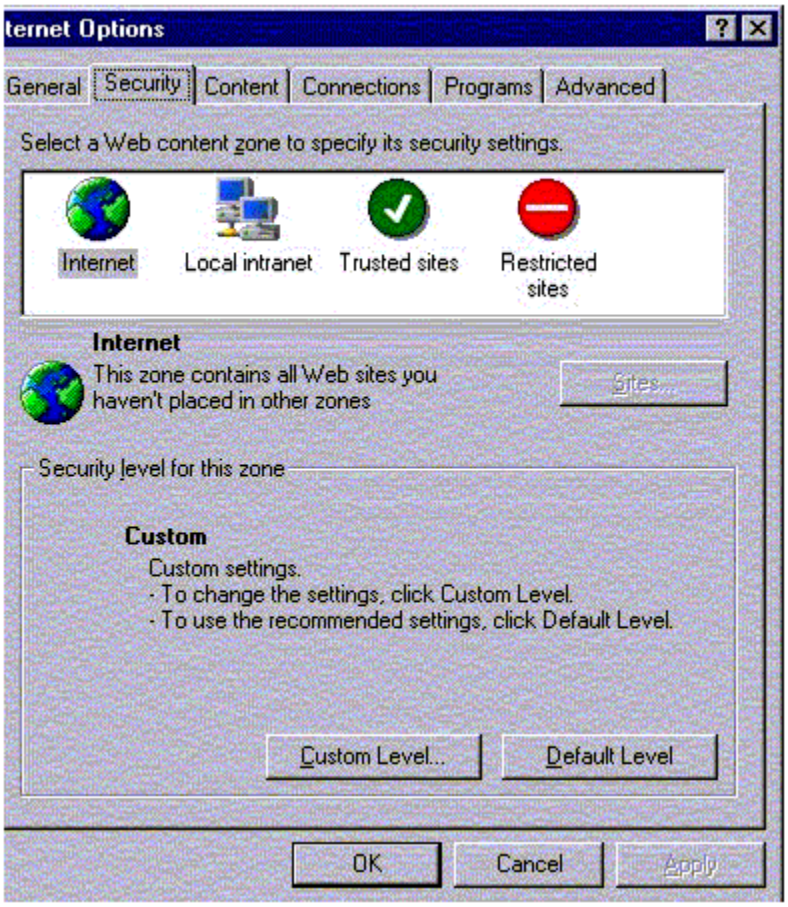
Enabling Pro/Web.Link

The configuration option `web_enable_javascript` controls whether the Pro/ENGINEER session is able to load the ActiveX control. Set `web_enable_javascript` to ON to enable Pro/Web.Link, and set it to OFF to disable it. The default value for the Pro/ENGINEER session is OFF. If Pro/Web.Link applications are loaded into the embedded browser with the configuration option turned off, the applications will throw a **pfcXNotConnectedToProE** exception.

Setting Up Browser Security

Follow the procedure below to change the security settings:

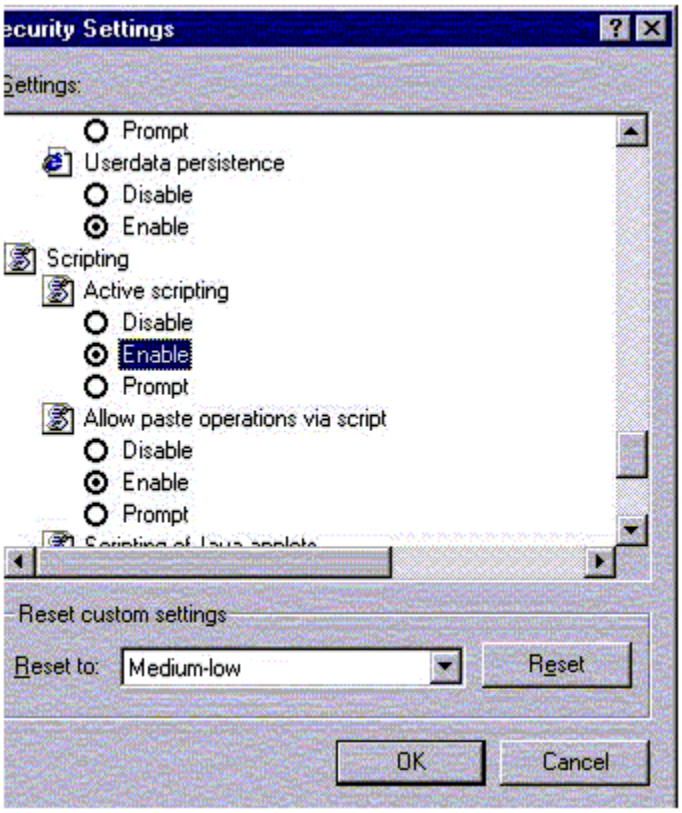
1. In Internet Explorer, select "Tools ->Internet Options". Click the "Security" tab as shown in the following figure.



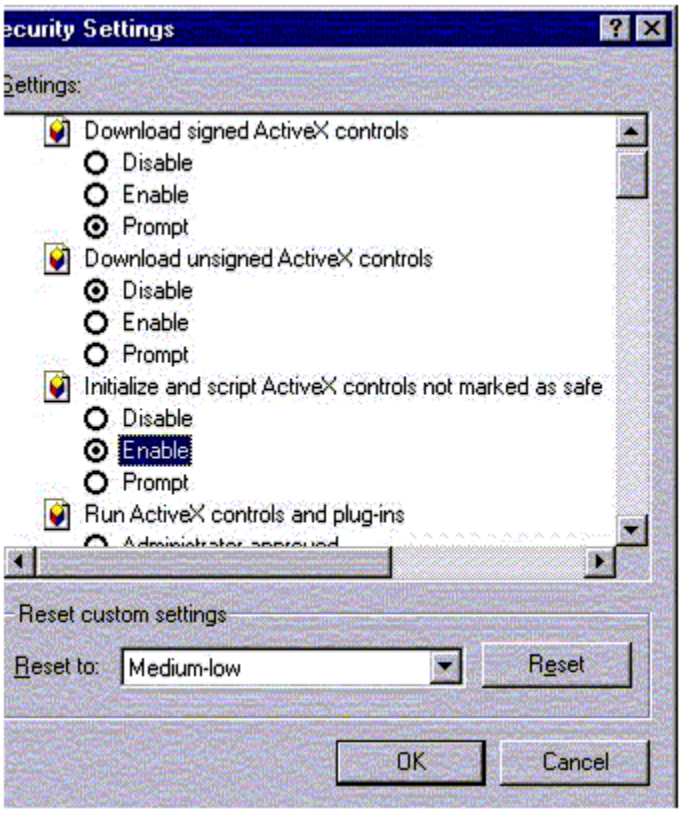
1. Select a zone for which you want to change security settings.

2. Click "Custom Level...".

3. Change the setting for "Initialize and Script ActiveX controls not marked as safe" under "ActiveX controls and plugins" to Enable, as shown in the following figure.



1. Change the setting for "Active Scripting" under "Scripting" to Enable as shown in the following figure.



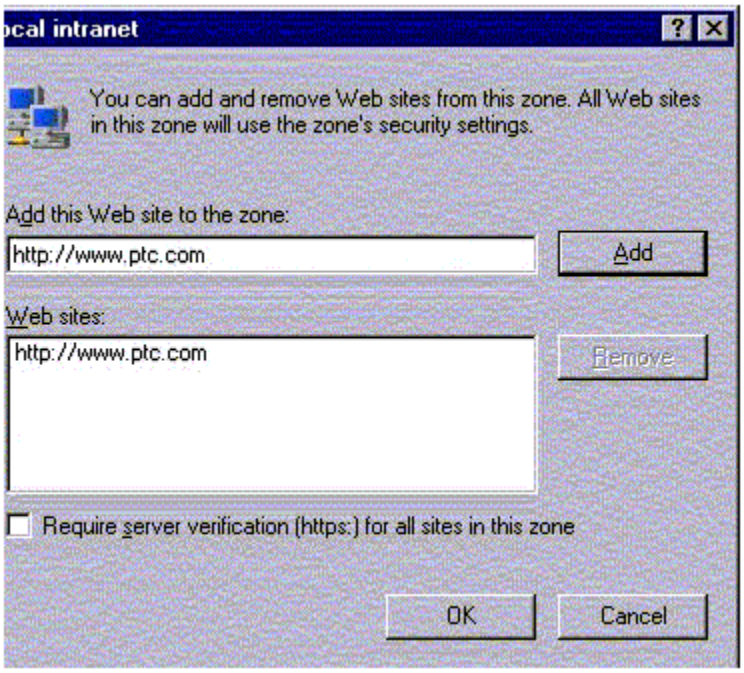
Add and Remove Sites to Security Zones

Follow the procedure below to add sites to the security zones:

1. In Internet Explorer, select "Tools ->Internet Options".

2. Click the "Security" tab.
3. Select the security zone to which you want to add sites.
4. Click "Sites...".
5. Click "Advanced...", this option is available only for the local intranet.
6. Enter the name of site.
7. Click "Add".

The site is added to the security zone as shown in the figure below:



Enabling Security Settings

To run Pro/Web.Link in the embedded browser security set the following in Microsoft Internet Explorer:

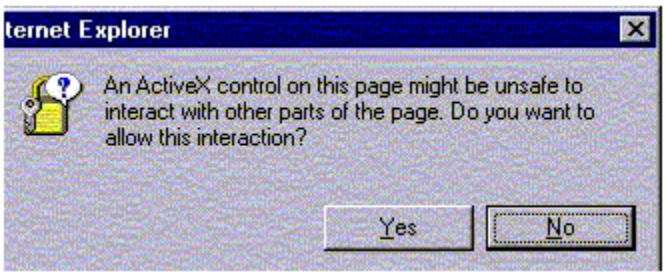
- Allow scripting of ActiveX controls not marked as safe
- Allow active scripting

These security features can be set to the following values:

- Disable--The activity is not permitted. Attempting to load a Pro/Web.Link page will result in the following exception:

"`Automation server can't create object`"

- Prompt--Each time the browser loads a web page that tries to access Pro/Web.Link methods and objects, you are prompted to allow the interaction activity as shown in the following figure.



- Enable--The interaction activity is always permitted

Script security can be independently assigned to four domains:

- Intranet--The organization's local intranet, including all access via file:// URLs and selected internal web servers.
- Trusted sites--Web sites designated as trusted.
- Restricted sites--Web sites designated as untrusted.
- Internet--All other sites accessed via the Internet.

Advanced Setup

The ActiveX control must be registered with Windows in order to be available to Pro/ENGINEER.

Note:
To register the ActiveX control for the first time you must have the permission to create new keys under the Windows registry key HKEY_CLASSES_ROOT.

If the configuration option `web_enable_javascript` is enabled, ActiveX control is registered automatically when Pro/ENGINEER starts.

Pro/ENGINEER does not unregister the ActiveX control automatically. If the control is already registered, Pro/ENGINEER will not register the DLL again, unless it is a different version of the application.

For multiple installations of Pro/ENGINEER Wildfire on a particular machine, you need to manually unregister the ActiveX control, to ensure that Pro/ENGINEER locates the correct version of the installation. To unregister the ActiveX control manually use the following command:

```
C:\winnt\system32\regsvr32 /u [/s] <Pro/ENGINEER loadpoint>\i486_nt\obj\pfcscom.dll
```

Use the "/s" flag to unregister without displaying a confirmation dialog box.

Security on UNIX

Pro/Web.Link in the Mozilla embedded browser uses XPCOM capability to connect the JavaScript calls to Pro/ENGINEER. Mozilla requires that web pages request privilege to execute the JavaScript calls. In JavaScript code this request appears as:

```
netscape.security.PrivilegeManager.enablePrivilege ("UniversalXPConnect");
```

The request for this privilege must be made in the topmost function called within a Web page that is loaded by the browser, as well as in the topmost function call made in an auxiliary file. For example, if Pro/ENGINEER loads a page that has three JavaScript callback functions

invoked by different buttons on the Web form, each callback function must request the privilege, if it needs to do any work with Pro/Web.Link classes or objects, including caught exceptions. If one of the callback functions calls into a secondary loaded `.JS` file, the topmost function call made by this file must also request the privilege.

Mozilla will prompt the user interactively to accept, or deny, the privilege. Users have the option to enable the privilege for all pages loaded from a particular location.

Note:
The privilege can always be requested from a local domain (file://). To request privilege in pages from other protocols a signed script is required, and may also require changes to Mozilla security settings. Visit http://www.mozilla.org/ for more information on Mozilla security options and settings.

Running Pro/Web.Link On Your Machine

To run Pro/Web.Link on your machine do the following:

- Edit your config.pro file to enable Pro/Web.Link on the local machine.
- Optionally setup browser security for your local intranet settings.
- Run Pro/ENGINEER Wildfire 2.0.

Load web pages containing Pro/Web.Link functions and application code into the embedded browser of Pro/ENGINEER.

Troubleshooting

The following table describes some common errors and how to resolve them.

Error	Explanation
pfcXNotConnectedToProE exception	The web page was loaded into a web browser that is not the Pro/ENGINEER embedded web browser. OR The web page was loaded into the embedded web browser but the configuration option "`web_enable_javascript`" is not "`on`".
Nothing happens when JavaScript is invoked; or "Automation server can't create object."	The Internet Explorer or Mozilla security is not configured to allow the web page to run Pro/Web.Link, or the page was loaded from an insecure site on UNIX.