SIEMENS

SPC4xxx/5xxx/6xxx
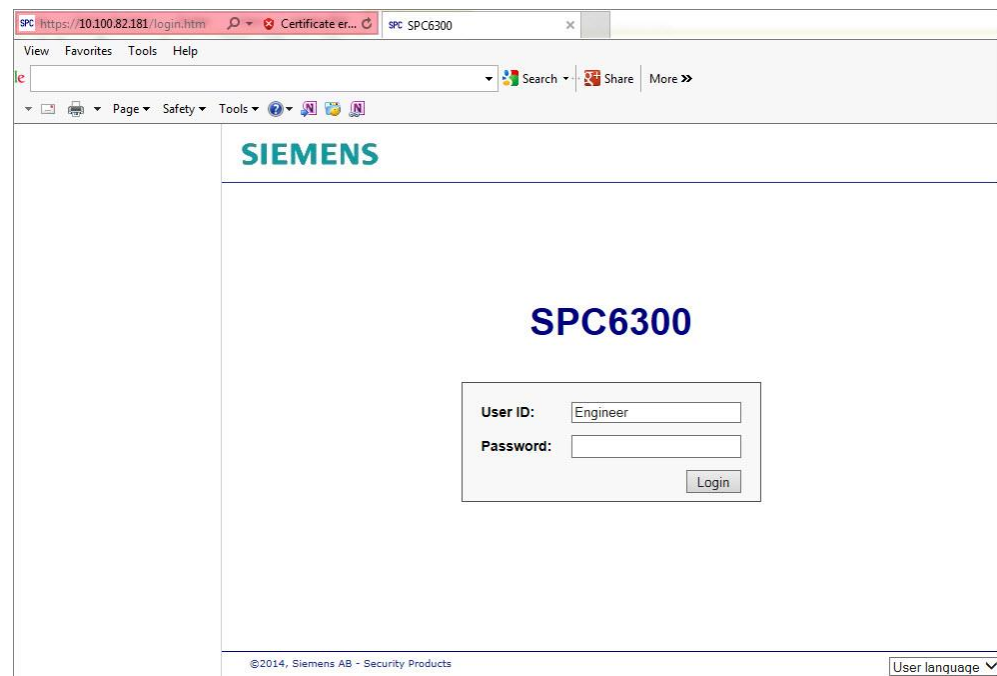
SSL Technical Note

V2.0

1 Background

In September 2014, Google announced "The Poodle Attack", an attack that can breach the security of SSL3. To combat this potential security breach, Mozilla Firefox have now released a patch to disable SSL3. Other browsers such as Google Chrome and Internet Explorer are likely to follow in quick succession. SSL3 is the security certificate implemented in the SPC web server for all firmware versions.

⚠	**⚠ WARNING**
	Enabling SSL3 for your browser leaves you vulnerable to the security attack announced by Google. For remote connections, we recommend that you use the SPC Connect portal interface, https://spcconnect.com, which provides highly secure SSL certification.

SPC Login Screen

Technical Note

2   Workaround 1 - Re-enable SSL3

SPC firmware uses SSL3. Browsers are starting to disable SSL3 by default. As a workaround, you must re-enable SSL3.

⚠	⚠ **WARNING**
	Enabling SSL3 for your browser leaves you vulnerable to the security attack announced by Google. For remote connections, we recommend that you use the SPC Connect portal interface, https://spcconnect.com, which provides highly secure SSL certification.

The following sections explain how to re-enable SSL3 for:

● Mozilla Firefox

● Internet Explorer

● Google Chrome

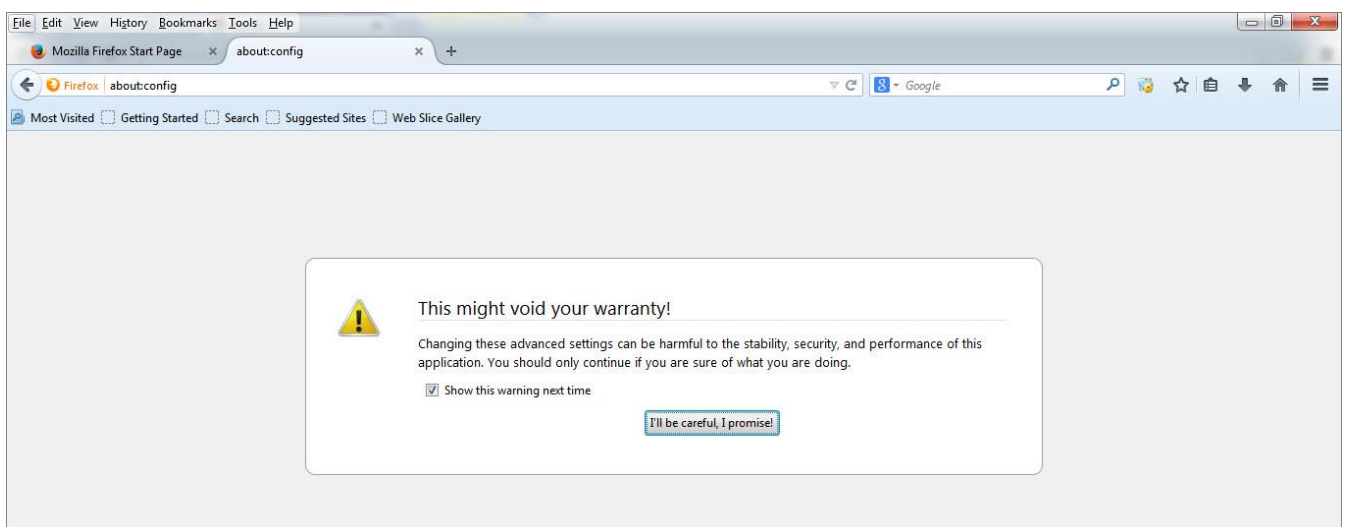| ⚠	⚠ **WARNING**
	When you enable SSL3 for your browser, you enable it for all sites and not just the SPC web server.

2.1   Mozilla Firefox

Rather than use individual checkboxes, Firefox now operates over a range of SSL/TLS protocols. These settings are accessed using the about:config preferences editor.
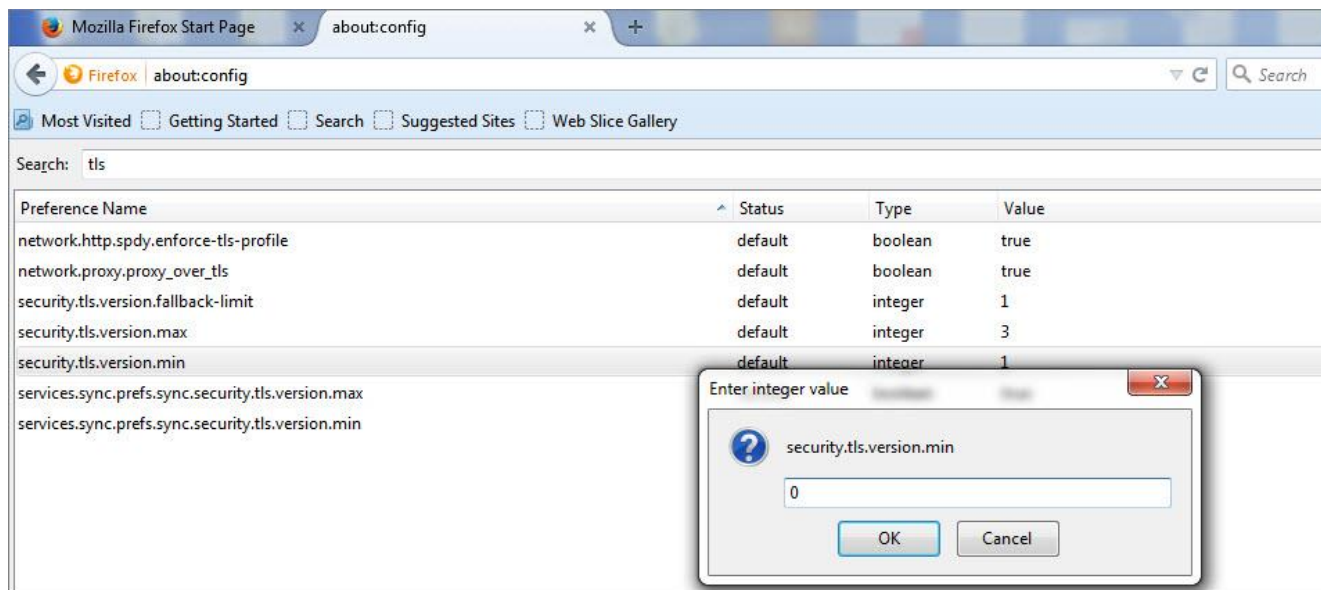
● Lowest Acceptable Protocol: security.tls.version.min (default SSL3.0 = 0)

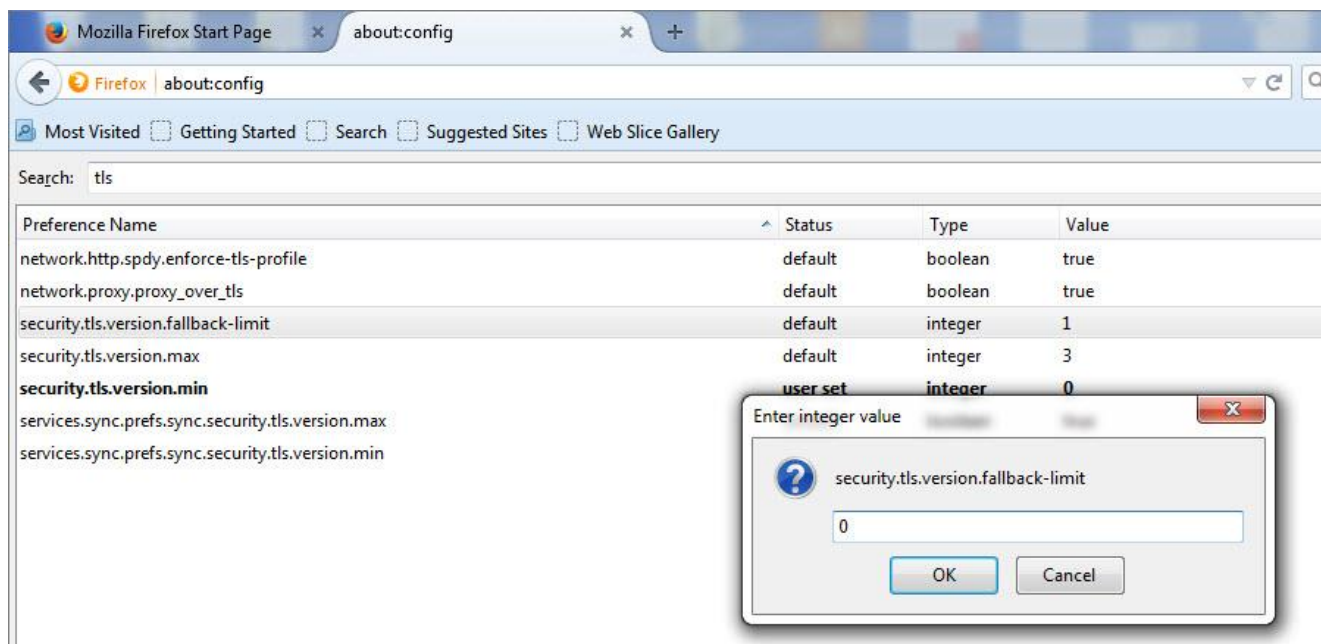● Highest Allowed Protocol: security.tls.version.max (default TLS1.0 = 1)

To modify:

1. In a new tab, type or paste **about:config** in the address bar and press Enter. Click the button promising to be careful.

Technical Note

2. In the **Search** box above the list, type or paste **tls** and pause while the list is filtered.

3. To enable SSL3, double-click **security.tls.version.min** and enter **0**. In Mozilla Firefox, the value 0 enables SSL3.0.

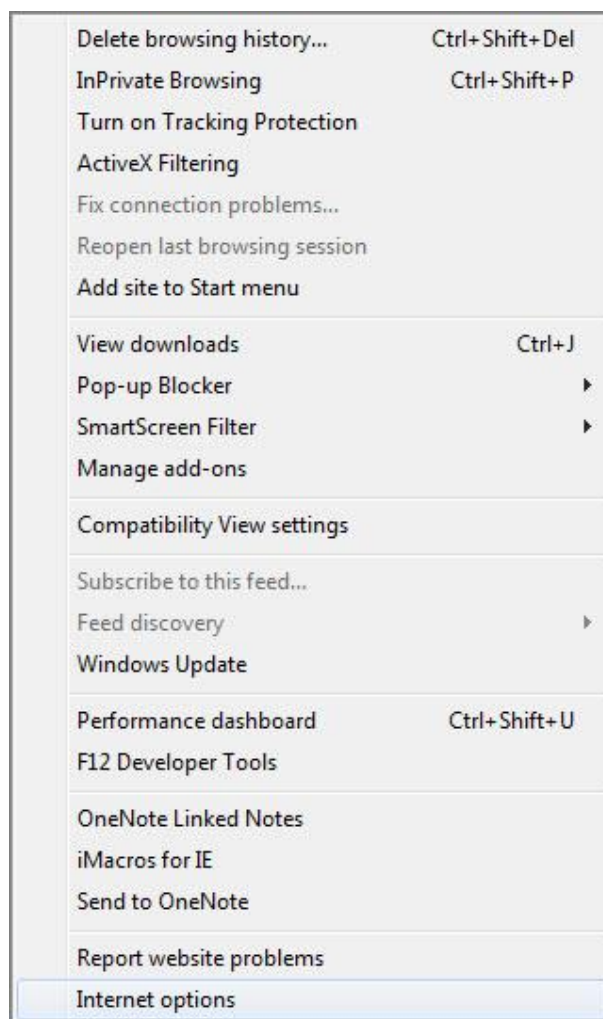4. Double-click **security.tls.version.fallback-limit** and enter **0**.

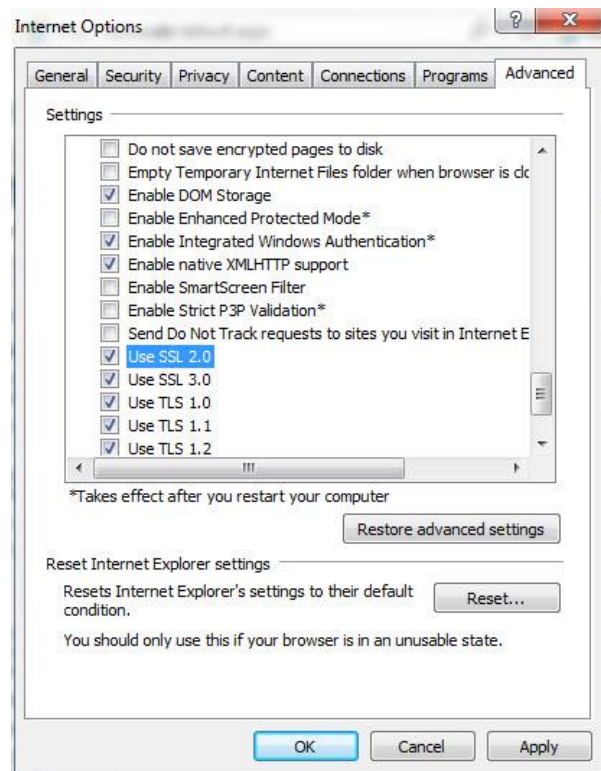| !	NOTICE
	For security reasons, please remove these settings when not connecting to an SPC panel.

2.2 Internet Explorer

1. In Internet Explorer, go to **Tools -> Internet Options**.

Internet Options

2. Click on the **Advanced** tab and scroll to the bottom of the screen.

3. Place a check mark in the boxes next to: **Use SSL3.0**

Advanced Options

4. Click **Apply**.

5. Click **OK**.

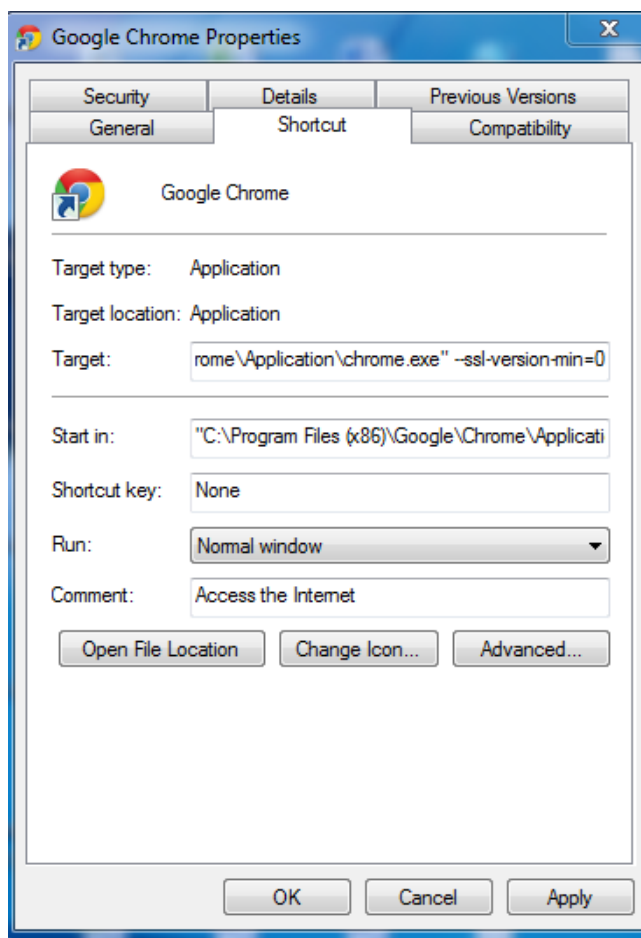6. Refresh your window by clicking **Refresh** or by pressing F5.

!	**NOTICE**
	For security reasons, please remove these settings when not connecting to an SPC panel.

2.3 Google Chrome

1. Right click your Chrome's desktop icon.
2. Click **Properties**.

Technical Note

Security Products   15.12.2014

3. At the end of the target field enter:
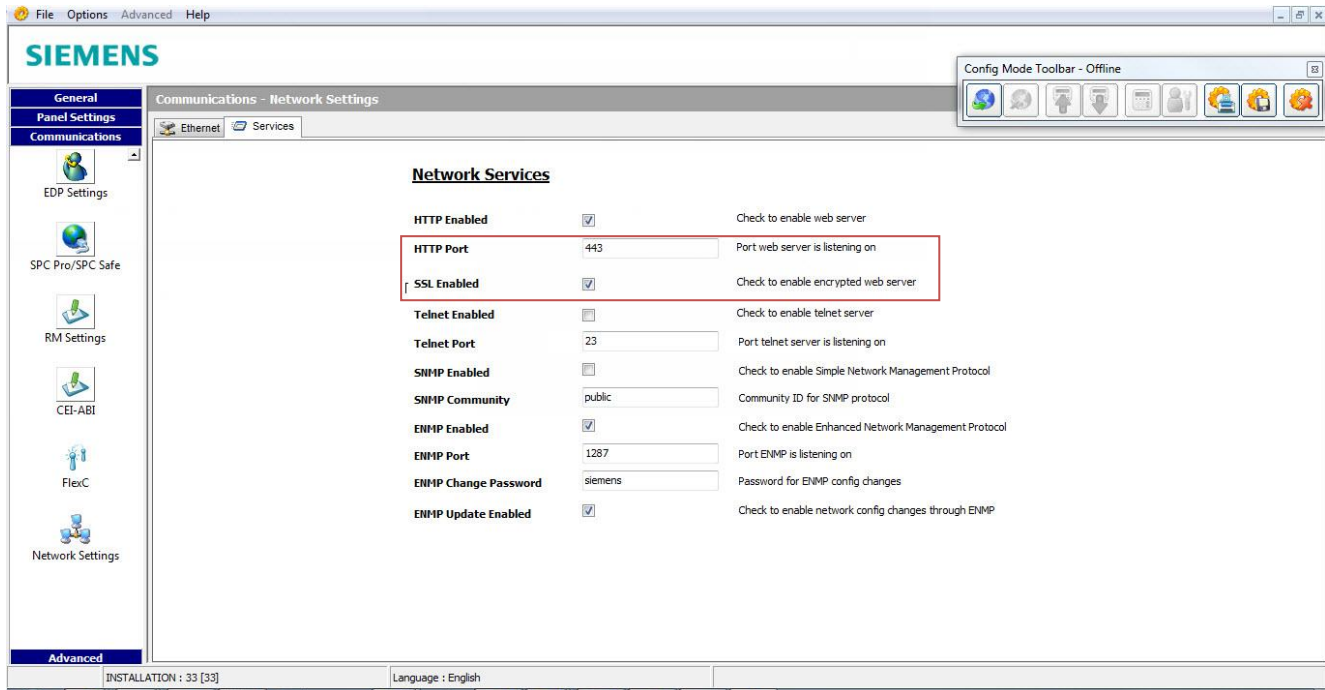4. " **--ssl-version-min=0 --ssl-version-fallback-min=ssl3**. If

!	NOTICE
	If " **--ssl-version-min=0** does not work, use " **--ssl-version-min=ssl3** as this is determined by the version of your browser.

5. **Apply**
6. Reboot Chrome completely via the menu or with [ctrl + shift + Q].

!	NOTICE
	For security reasons, we advise that you create a shortcut for Chrome SPC where you have made these changes. Use this shortcut to connect to the SPC panel only.

For security reasons, please remove these settings when not connecting to an SPC panel. |

3 Workaround 2 - Disable SSL3 on the Panel

To disable SSL3 on the panel, you must use SPC Pro.

1. In SPC Pro, select the menu **Communications – Network Settings.**
2. Select the **Services** tab.
3. To disable SSL, deselect the **SSL Enabled** checkbox and set the **HTTP Port** field to **80**.
4. To re-enable SSL, tick the **SSL Enabled** checkbox and set the **HTTP Port** field to **443**.

Edition   15.12.2014