Rev.1
December 1 2014

NEC

Express5800 series

Setup Manual for avoiding the vulnerability issue of SSL protocol 3.0

Introduction

When the SSL protocol 3.0 is used from browser or from Java applications launched from Java Applet and Java Web Start, a part of an encrypted communication data may be decrypted by the attack called CVE-2014-3566 POODLE (Padding Oracle On Downgraded Legacy Encryption).

This vulnerability can be avoided at the client by disabling the SSL protocol 3.0 of the browser and Java and enabling the TLS protocol 1.0 or later.

This setup manual describes the procedures for disabling the SSL protocol 3.0 of browser and Java at the client.

Target computer

Computers on which SSL protocol 3.0 supported browser and Java Runtime Environment are installed.

[Revision Record]

Rev.	Date	Main Contents of Revision
1	December 1, 2014	First Edition

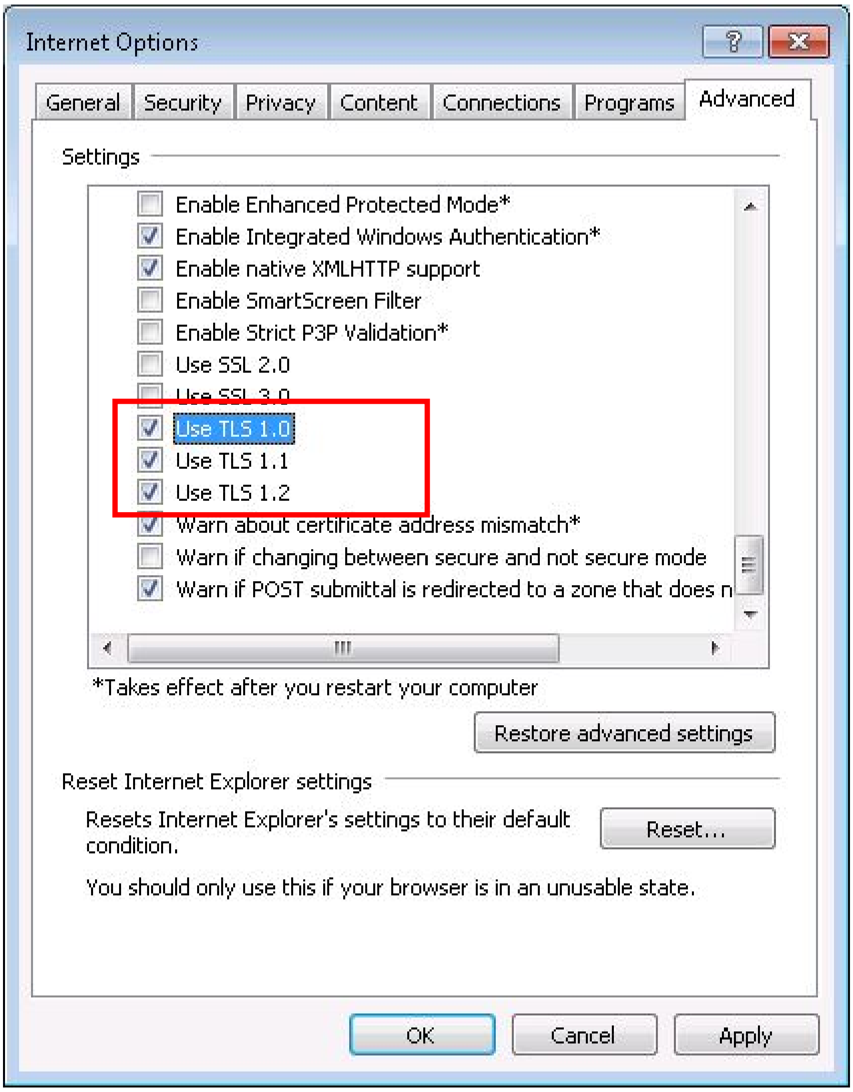
Contents

1. Setup the Web browser

The following steps are performed from the Web browser on the computer.

[Internet Explorer]

Please open “Security” menu of [Advanced]-[Internet Options]-[Tools] of Internet Explorer and then set TLS 1.0 or later enable at the items related to SSL/TLS as follows.



☐ Enable Enhanced Protected Mode*
☑ Enable Integrated Windows Authentication*
☑ Enable native XMLHTTP support
☐ Enable SmartScreen Filter
☐ Enable Strict P3P Validation*
☐ Use SSL 2.0
☐ Use SSL 3.0
☑ Use TLS 1.0
☑ Use TLS 1.1
☑ Use TLS 1.2
☑ Warn about certificate address mismatch*
☐ Warn if changing between secure and not secure mode
☑ Warn if POST submittal is redirected to a zone that does n

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Notice:

Please use the Internet Explorer other than Internet Explorer 9 for the following products.

- EXPRESSSCOPE Engine 3
  The following products are the target.

  R110e-1E、R110d-1E、R110g-1E、R110f-1E

  R120e-1M、R120d-1M、R120e-2M、R120d-2M、R120e-1E、R120d-1E、 R120e-2E、R120d-2E

T110g-E、T110f-E、T110g-S、T110f-S、T120d、T120e

E120d-1、E120d-M、E120e-M

GT110e、GT110d、GT110e-S、GT110d-S

B120d、B120d-h、B120e、B120e-h

- EXPRESSSCOPE Engine SP 3
  The following products are the target. (*)

  A1040b、A2040b、A2020b、A2010b

  (*) However, only if the firmware revision of EXPRESSSCOPE Engine SP 3 is applied to previous revision than 1.14

- EXPRESSSCOPE Engine 3 ft
  The following products are the target.

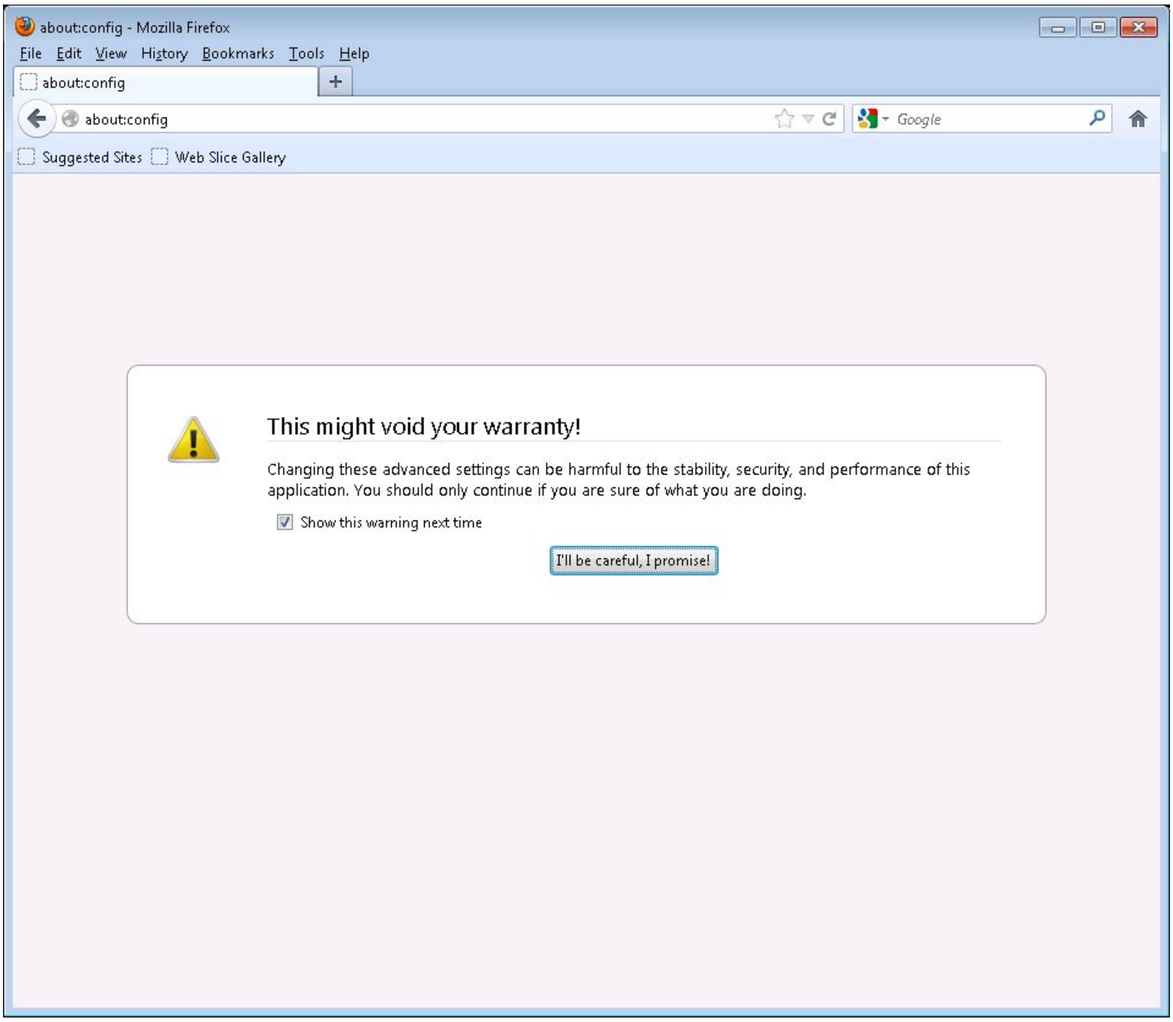
  R320c-E4、R320c-M4、R320d-M4

- EXPRESSSCOPE Engine SP 2
  The following products are the target.

  A1080a-S、A1080a-D、A1080a-E、A1040a

[Firefox ESR]

Input “about:config” to the address bar.



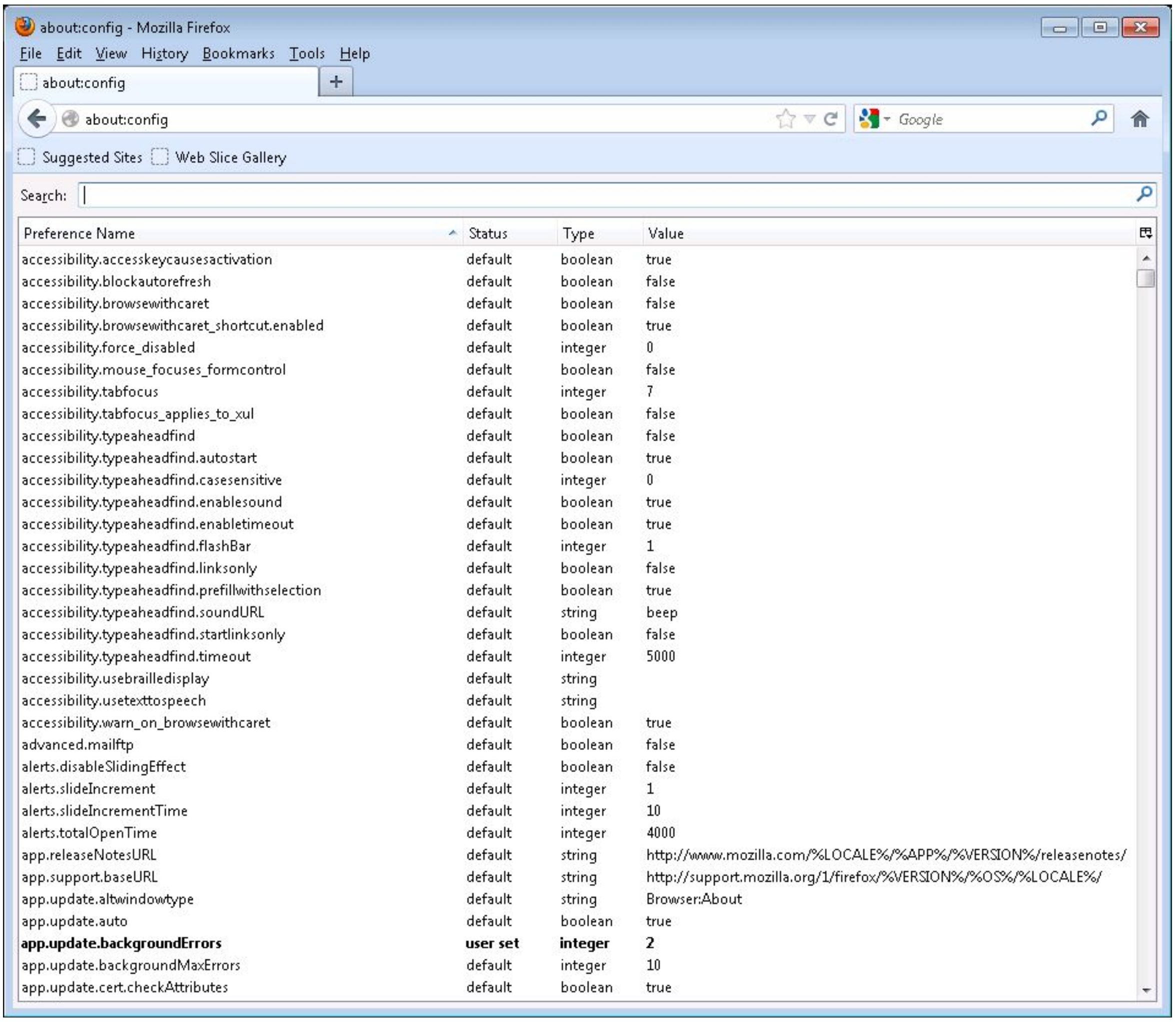
This might void your warranty!

Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:config
about:config
Google
Suggested Sites
Web Slice Gallery
I'll be careful, I promise!

The search window is displayed after “I’ll be careful, I promise!” button.



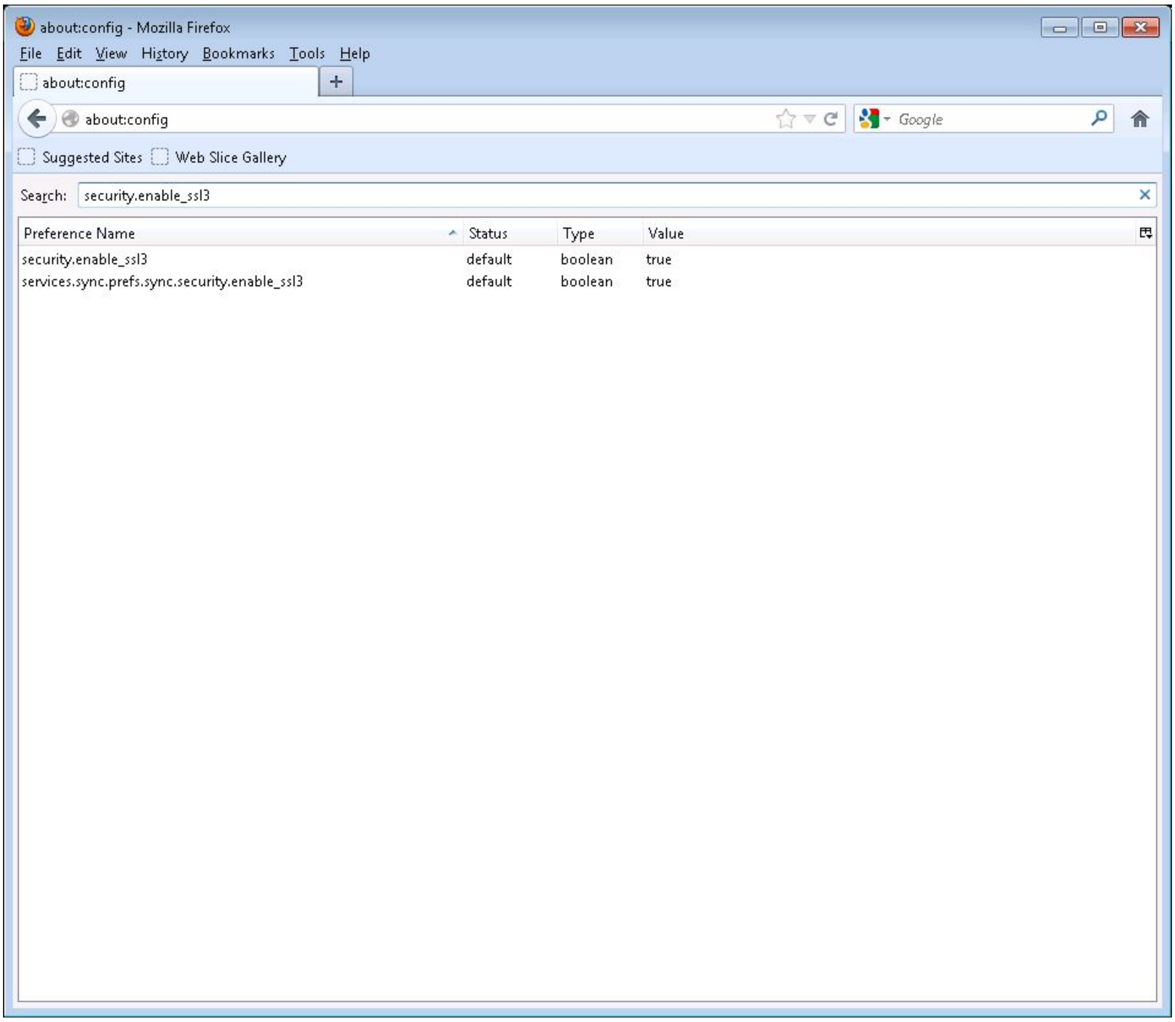
about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:config
about:config
Google
Suggested Sites
Web Slice Gallery

Search:

Preference Name	Status	Type	Value
accessibility.accesskeycausesactivation	default	boolean	true
accessibility.blockautorefresh	default	boolean	false
accessibility.browsewithcaret	default	boolean	false
accessibility.browsewithcaret_shortcut.enabled	default	boolean	true
accessibility.force_disabled	default	integer	0
accessibility.mouse_focuses_formcontrol	default	boolean	false
accessibility.tabfocus	default	integer	7
accessibility.tabfocus_applies_to_xul	default	boolean	false
accessibility.typeaheadfind	default	boolean	false
accessibility.typeaheadfind.autostart	default	boolean	true
accessibility.typeaheadfind.casesensitive	default	integer	0
accessibility.typeaheadfind.enablesound	default	boolean	true
accessibility.typeaheadfind.enabletimeout	default	boolean	true
accessibility.typeaheadfind.flashBar	default	integer	1
accessibility.typeaheadfind.linksonly	default	boolean	false
accessibility.typeaheadfind.prefillwithselection	default	boolean	true
accessibility.typeaheadfind.soundURL	default	string	beep
accessibility.typeaheadfind.startlinksonly	default	boolean	false
accessibility.typeaheadfind.timeout	default	integer	5000
accessibility.usebrailledisplay	default	string	
accessibility.usetexttospeech	default	string	
accessibility.warn_on_browsewithcaret	default	boolean	true
advanced.mailftp	default	boolean	false
alerts.disableSlidingEffect	default	boolean	false
alerts.slideIncrement	default	integer	1
alerts.slideIncrementTime	default	integer	10
alerts.totalOpenTime	default	integer	4000
app.releaseNotesURL	default	string	http://www.mozilla.com/%LOCALE%/%APP%/%VERSION%/releasenotes/
app.support.baseURL	default	string	http://support.mozilla.org/1/firefox/%VERSION%/%OS%/%LOCALE%/
app.update.altwindowtype	default	string	Browser:About
app.update.auto	default	boolean	true
app.update.backgroundErrors	**user set**	**integer**	**2**
app.update.backgroundMaxErrors	default	integer	10
app.update.cert.checkAttributes	default	boolean	true

In the case of ESR17

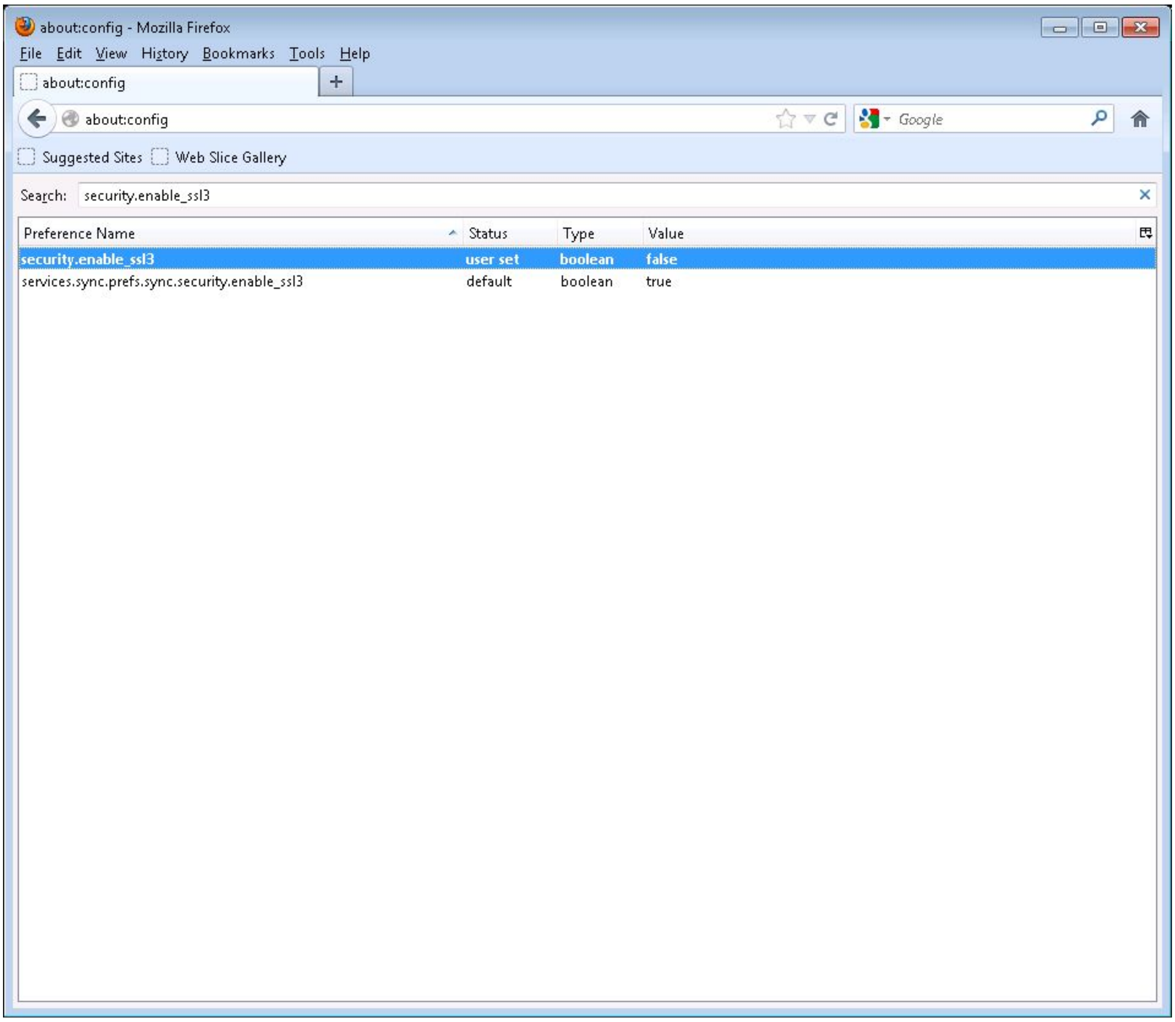
Input “security.enable_ssl3” to “Search:” area and check the value.


about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:config
about:config
Google
Suggested Sites
Web Slice Gallery

Search: security.enable_ssl3

Preference Name	Status	Type	Value
security.enable_ssl3	default	boolean	true
services.sync.prefs.sync.security.enable_ssl3	default	boolean	true

If “Value” of “security.enable_ssl3” is “true”, it turns to “false” when you double-click the “security.enable_ssl3”.



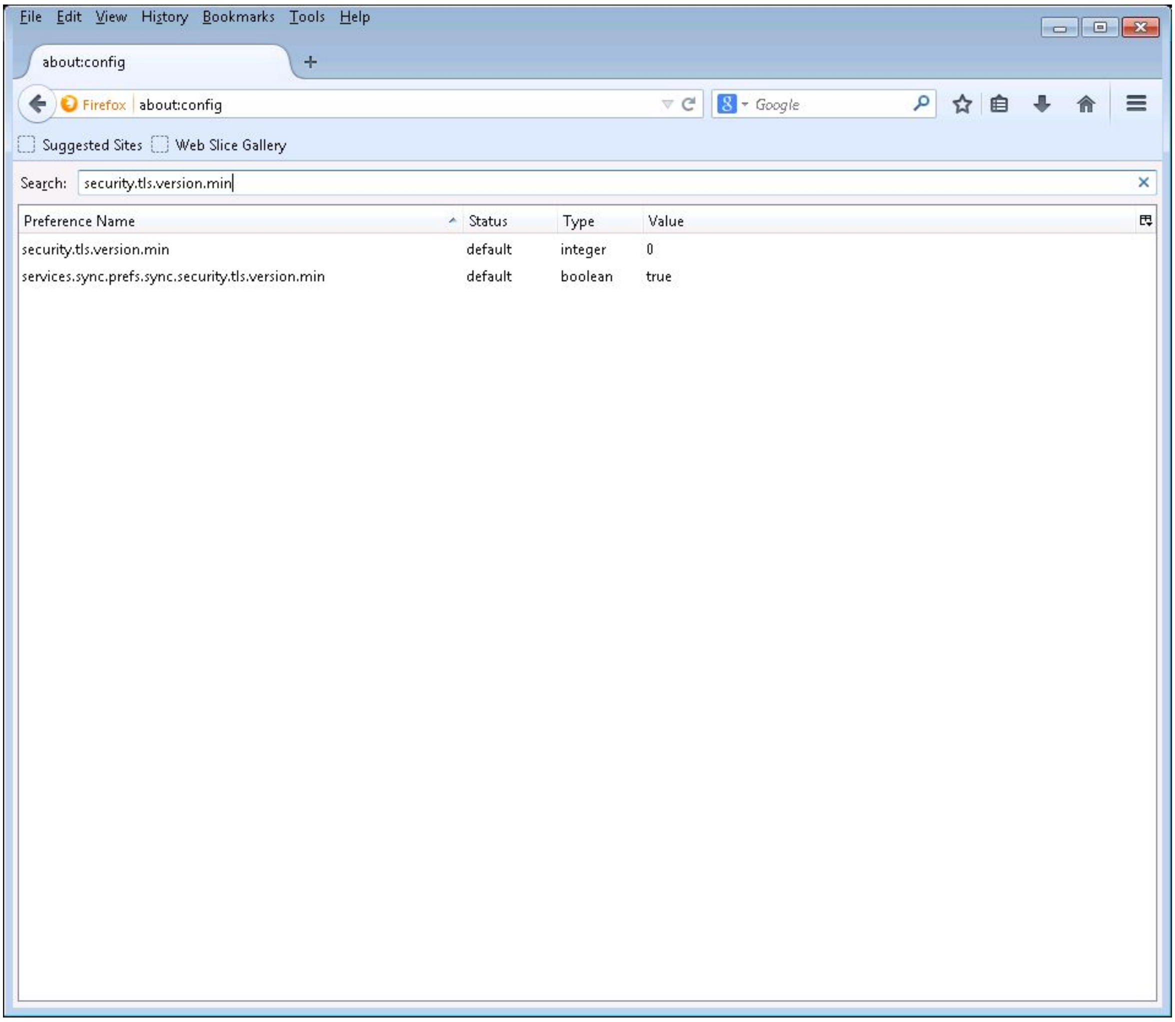
Search: security.enable_ssl3

Preference Name	Status	Type	Value
security.enable_ssl3	user set	boolean	false
services.sync.prefs.sync.security.enable_ssl3	default	boolean	true

Please restart your Web browser.

In the case of ESR24 or later

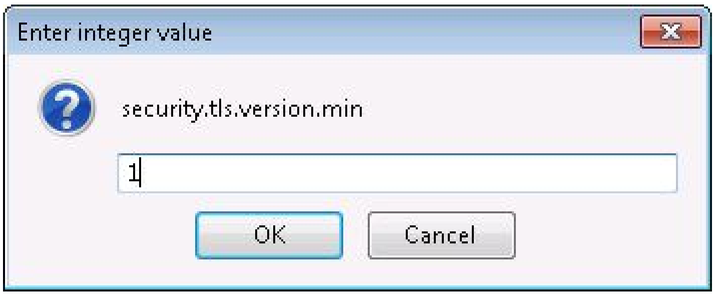
Input “security.tls.version.min” to “Search:” area and check “Value”.



Search: security.tls.version.min

Preference Name	Status	Type	Value
security.tls.version.min	default	integer	0
services.sync.prefs.sync.security.tls.version.min	default	boolean	true

If “Value” of “security.tls.version.min” is 0, please open the window which is displayed by double-click the “security.tls.version.min”, and then input “1” and press “OK” button.



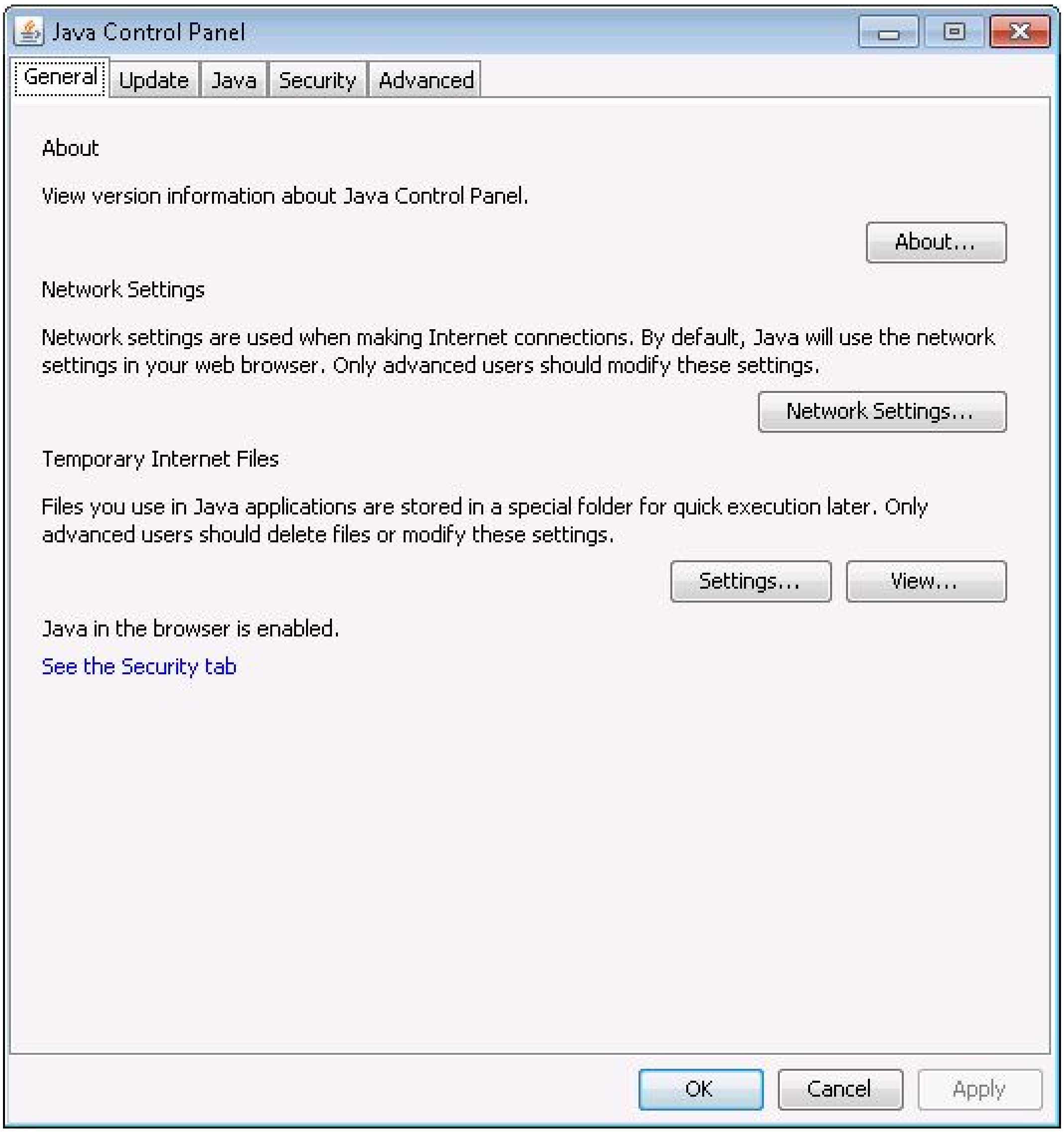
security.tls.version.min

1

Please restart your Web browser.

2 Setup the Java

Open "Java Control Panel" from "Control Panel" of the computer on which Java is installed.



About

View version information about Java Control Panel.

Network Settings

Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.

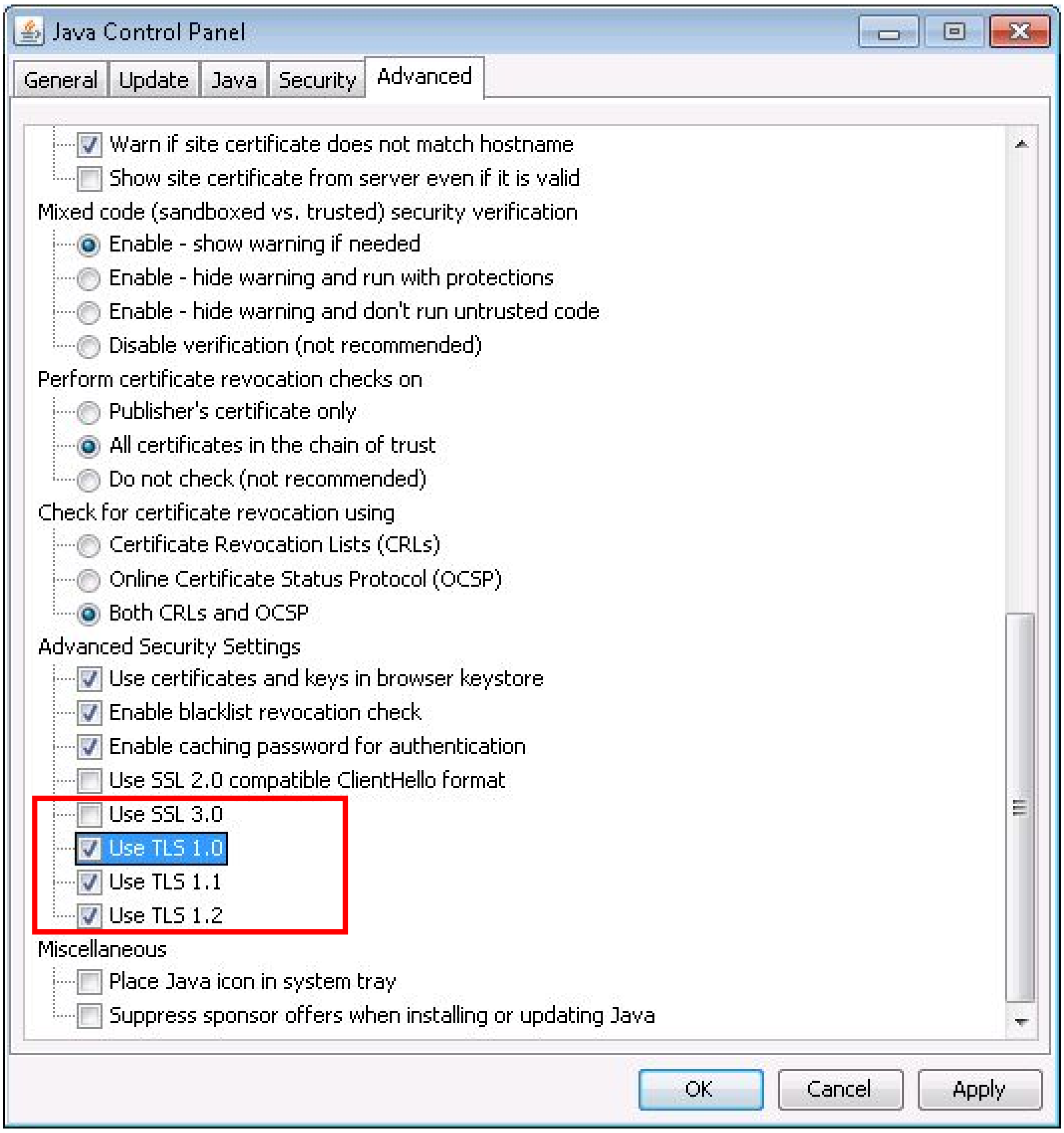
Temporary Internet Files

Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.

Java in the browser is enabled.

See the Security tab

Uncheck "Use SSL 3.0" from [Advanced Security Settings]-[Advanced], and then check the TLS protocol 1.0 or later.



- ☑ Warn if site certificate does not match hostname
- □ Show site certificate from server even if it is valid

Mixed code (sandboxed vs. trusted) security verification

- ● Enable - show warning if needed
- ○ Enable - hide warning and run with protections
- ○ Enable - hide warning and don't run untrusted code
- ○ Disable verification (not recommended)

Perform certificate revocation checks on

- ○ Publisher's certificate only
- ● All certificates in the chain of trust
- ○ Do not check (not recommended)

Check for certificate revocation using

- ○ Certificate Revocation Lists (CRLs)
- ○ Online Certificate Status Protocol (OCSP)
- ● Both CRLs and OCSP

Advanced Security Settings

- ☑ Use certificates and keys in browser keystore
- ☑ Enable blacklist revocation check
- ☑ Enable caching password for authentication
- □ Use SSL 2.0 compatible ClientHello format
- □ Use SSL 3.0
- ☑ Use TLS 1.0
- ☑ Use TLS 1.1
- ☑ Use TLS 1.2

Miscellaneous

- □ Place Java icon in system tray
- □ Suppress sponsor offers when installing or updating Java