For CitiDirect Users:

Enabling TLS in Browser and Java settings

November 2014

Table of Contents

Introduction

This document is intended for CitiDirect end users, and also IT security administrators as needed.

On **January 10, 2015**, a protocol known as Secure Sockets Layer version 3 (SSL 3.0) will be disabled on CitiDirect Web Servers. The information in this document provides guidance on how to ensure each user's computer is properly configured to run CitiDirect Online Banking and CitiDirect Services after SSL 3.0 is disabled on **January 10, 2015**.

On each user's computer, there are two things that should be checked: **Java setting** and **Browser setting**. To assist each individual user, this document provides the required steps for the Java and browser versions that we currently support.

Background

A weakness in the SSL 3.0 protocol was recently discovered and the attack that demonstrates this weakness is named **POODLE (Padding Oracle On Downgraded Legacy Encryption)**. The vulnerability is with the SSL 3.0 protocol itself and any web site or service that supports SSL 3.0 is exposed to being impacted by a POODLE attack.

Disabling SSL 3.0 in system/application configurations is the most viable solution to removing the POODLE vulnerability currently available – according to United States Computer Emergency Readiness Team (www.us-cert.gov/ncas/alerts/TA14-290A).

Transport Layer Security (TLS) is not impacted by this SSL 3.0 vulnerability and not subject to POODLE attacks. To avoid this vulnerability, the **TLS 1.0 protocol must be enabled in both your Browser and Java settings**. While all modern browsers and Java support the use of TLS, users can disable it in the settings of most browsers and Java. Thus, it is critical that you check your settings to ensure TLS 1.0 is enabled.

This issue has been assigned CVE-2014-3566. Common Vulnerabilities and Exposures (CVE®) is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities. More information about CVE can be found at:

https://cve.mitre.org/about/index.html

For Oracle's guidance on POODLE vulnerability, please click on this link:
http://www.oracle.com/technetwork/topics/security/poodlecve-2014-3566-2339408.html

Again, the remediation for this SSL 3.0 issue is to disallow the use of SSL 3.0 and force the use of TLS on any web site or service where SSL 3.0 s in use. While all modern browsers and Java versions support the use of TLS, **users have the capability to turn it off in the settings on most browsers and Java**.

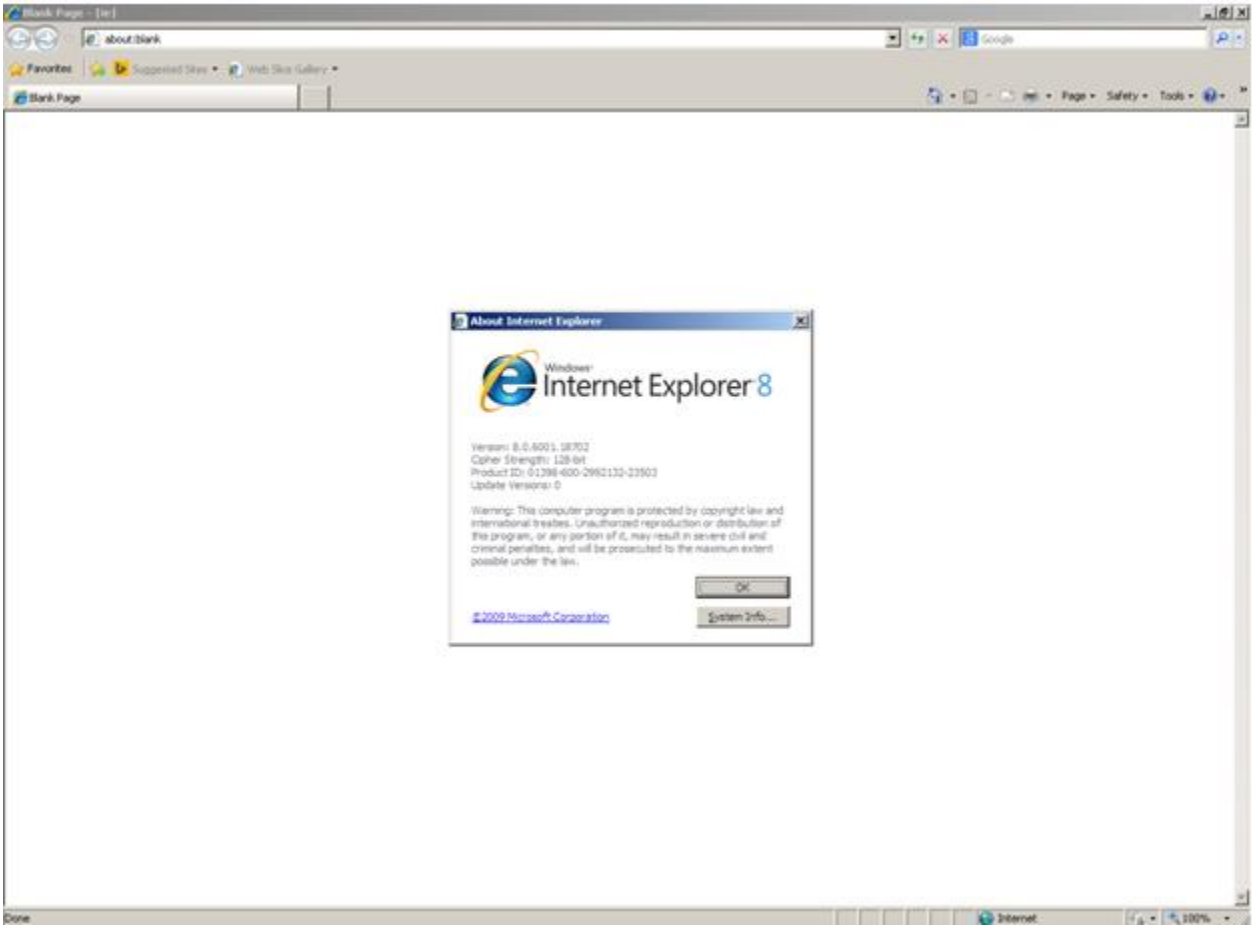
If a user's browser is configured to support only SSL 3.0 and they attempt to access a site where SSL 3.0 has been disabled, the browser will not be able to open a connection to the site.

What browser version do I have?

To determine the browser version currently installed on your computer see the steps below:

Internet Explorer

• Open Internet Explorer and navigate to Help menu → About Internet Explorer



Based on the browser version installed, select the relevant link from the list below to view the actions required.

- Internet Explorer (IE) 8, 9
- Internet Explorer (IE) 10, 11
- MAC Safari

What Java version do I have?

To determine the Java version currently installed on your computer see the steps below:

- Open Internet Explorer and go to the following website:
  http://www.java.com/en/download/installed.jsp?detect=jre

If Java is correctly installed, it will display the current Java version on your computer similar to the screenshot below.

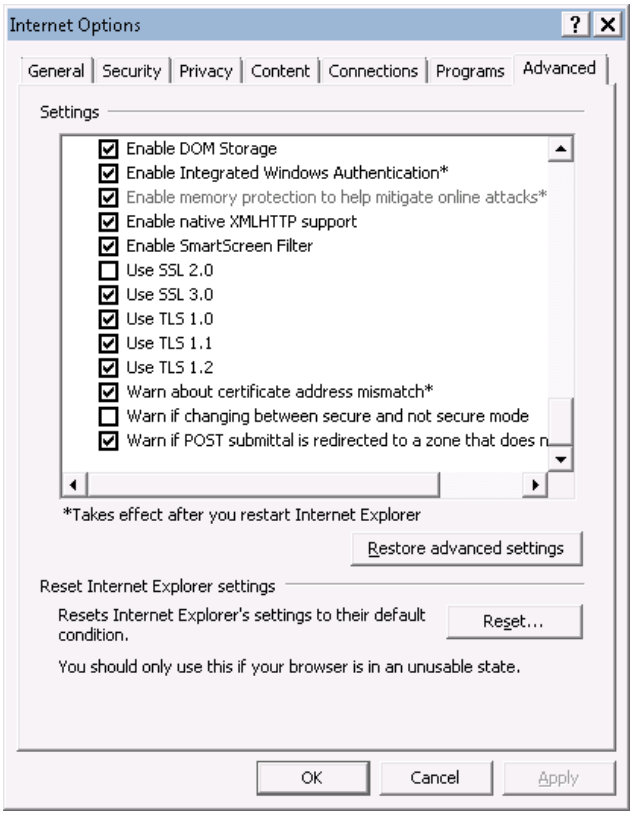
Based on the Java version installed, select the relevant link from the list below to view the actions required (**applicable for both Windows and MAC operating systems**)

- Java 1.5.0 to 1.5.0_04
- Java 1.5.0_6 to 1.5.0_21
- Java 1.5.0_22 to 1.5.0_28
- Java 1.6.0 to 1.6.0_18
- Java 1.6.0_19 to 1.6.0_45
- Java 1.7.0_0 to 1.7.0_9
- Java 1.7.0_10 to latest Java version 1.8

Note: Latest Java / Browser versions enable TLS 1.0 by default. However, it is recommended to check Java / Browser settings to make sure TLS 1.0 is enabled.

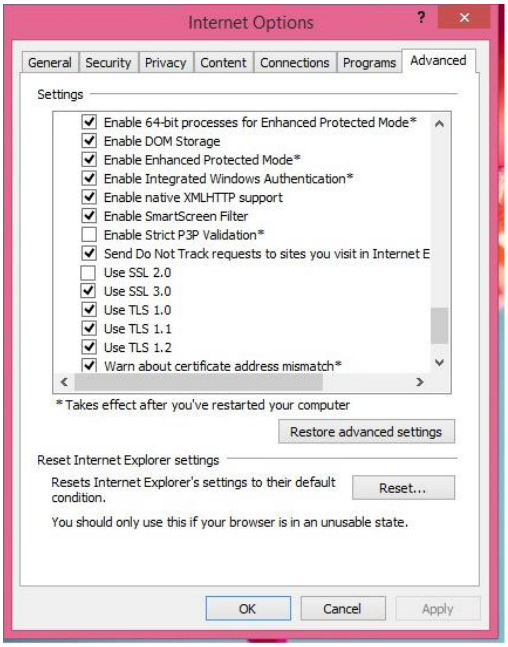
Internet Explorer (IE) 8, 9 version

1. Open "Internet Explorer" and click on “Tools” in the top menu bar of the IE browser
2. Click on “Internet Options”
3. Click on the “Advanced” tab within the Internet Options window
4. Scroll down in the “Advanced” tab and select “**TLS 1.0**” checkbox
5. Click “Apply” in the Internet Options tab



Internet Explorer (IE) 10, 11 version

1. Open "Internet Explorer" and click on “Tools” in the top menu bar of the IE browser
2. Click on “Internet Options”
3. Click on the “Advanced” tab within the Internet Options window
4. Scroll down in the “Advanced” tab and select “**TLS 1.0**” checkbox
5. Click “Apply” in the Internet Options tab



MAC Safari

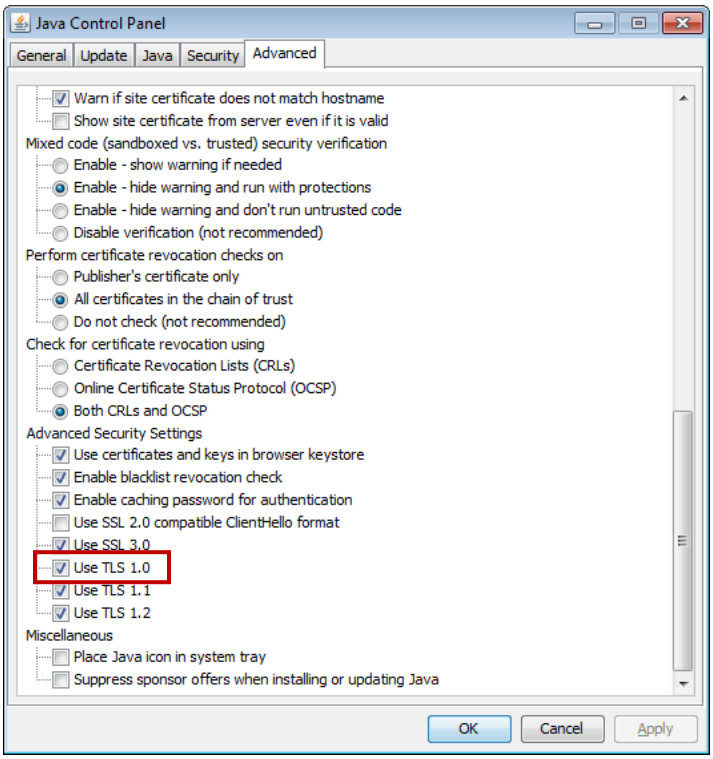
No explicit setting change is required.

Java 7 and 8 Versions (1.7 Update xx and 1.8 Update xx)

Based on the minor version installed, the actions to be taken vary and are listed below:

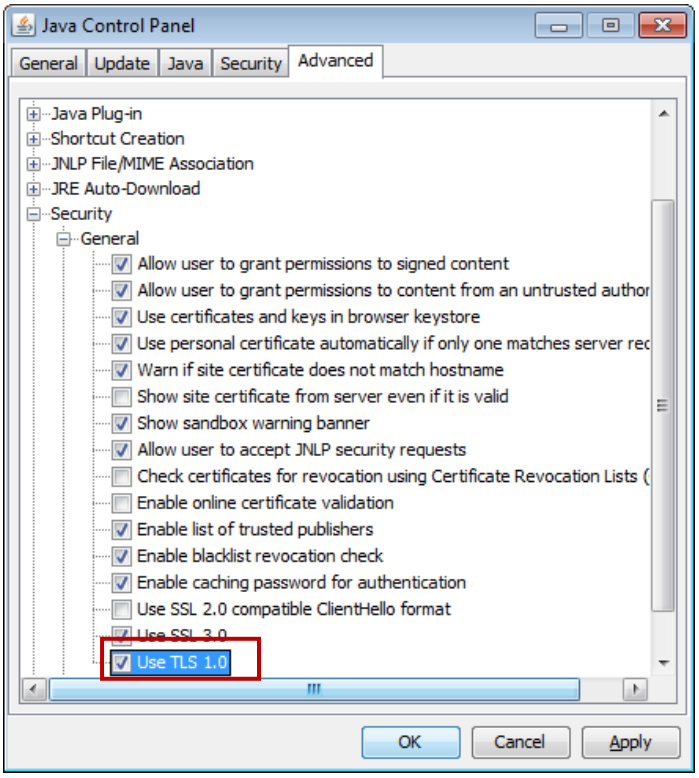
Java 1.7.0_10 to latest Java version 1.8

1. Navigate to Java Control Panel
2. Click on the “Advanced” tab
3. Enable “TLS 1.0” checkbox under Advanced Security Settings and click “Apply” & “OK”.



Java 1.7.0_0 to 1.7.0_9

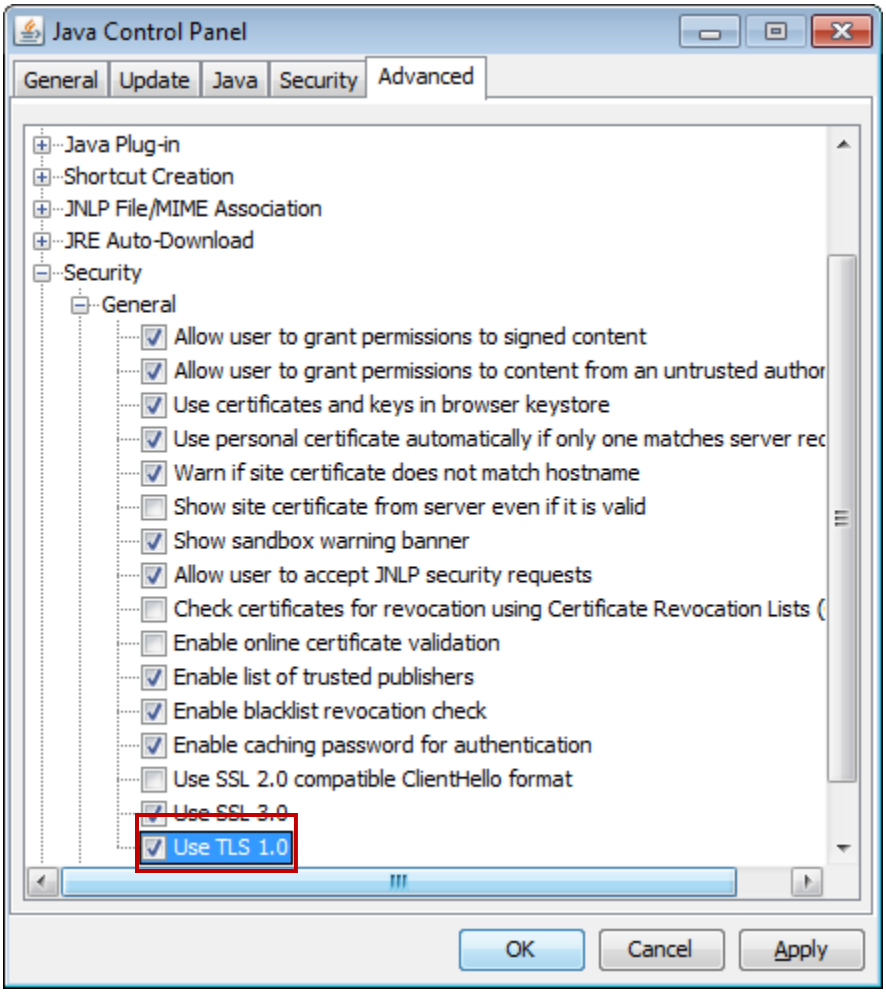
1. Navigate to Java Control Panel
2. Click on the “Advanced” tab
3. Navigate to Security → General → Enable “TLS 1.0” checkbox and click “Apply” & “OK”.



Java 6 Versions (1.6 Update xx)

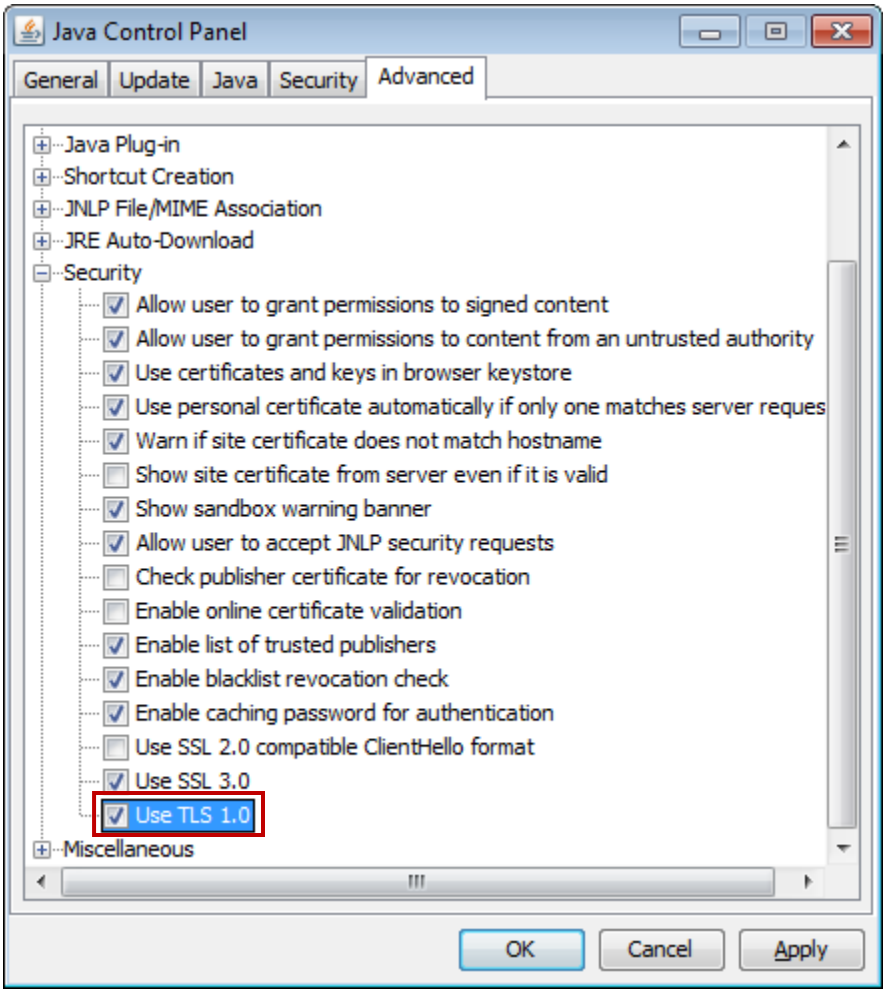
Java 1.6.0_19 to 1.6.0_45

1. Navigate to Java Control Panel
2. Click on the “Advanced” tab
3. Navigate to Security → General → Select “TLS 1.0” checkbox and click “Apply” & “OK”.



Java 1.6.0 to 1.6.0_18

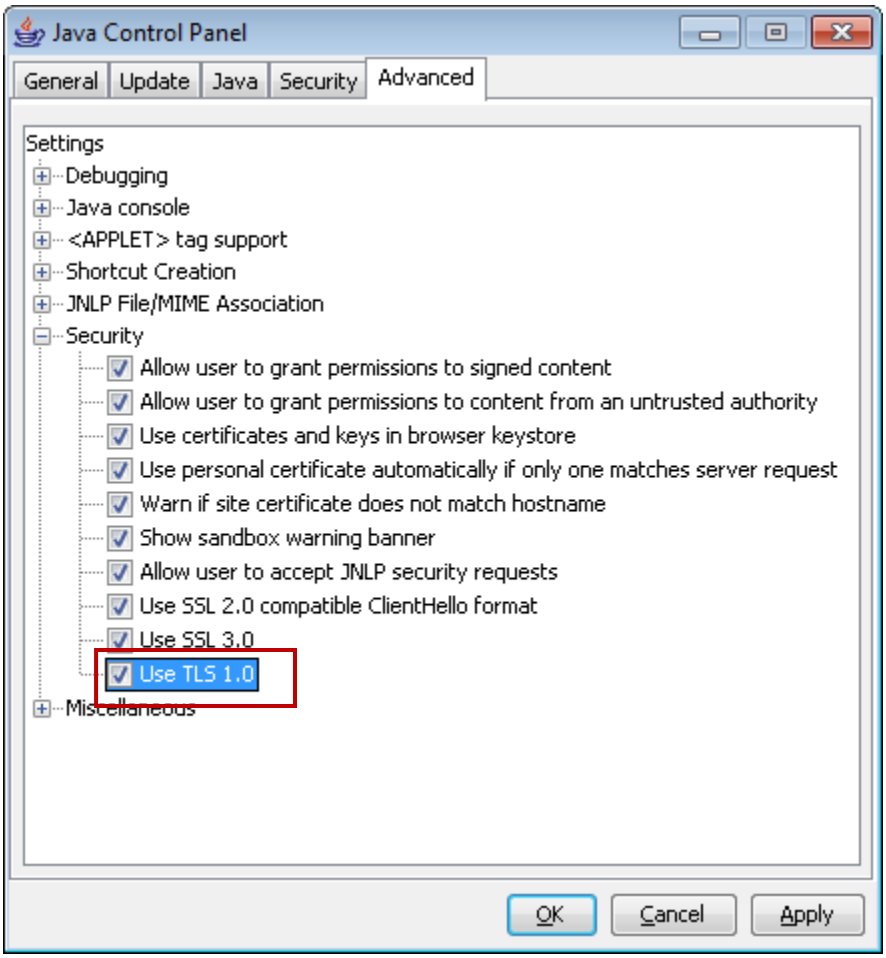
1. Navigate to Java Control Panel
2. Click on the “Advanced” tab
3. Navigate to Security → Select “TLS 1.0” checkbox and click “Apply” & “OK”.



Java 5 Versions (1.5 Update xx)

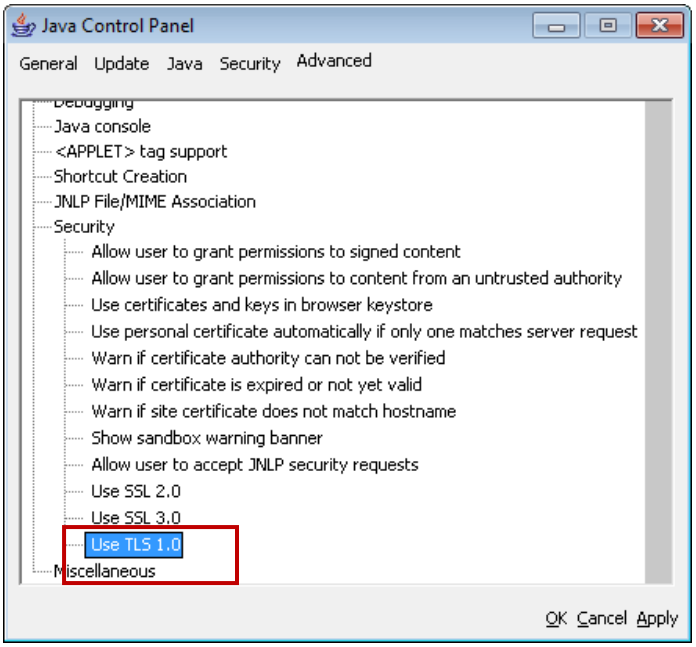
Java 1.5.0_22 to 1.5.0_28

1. Navigate to Java Control Panel
2. Click on the “Advanced” tab
3. Navigate to Security → Select “TLS 1.0” checkbox and click “Apply” & “OK”.



Java 1.5.0_6 to 1.5.0_21

1. Navigate to Java Control Panel
2. Click on the “Advanced” tab
3. Navigate to Security → Select “TLS 1.0” checkbox and click “Apply” & “OK”.



Java 1.5.0 to 1.5.0_04

There is no option to enable “TLS 1.0” for this Java version. Therefore, we **strongly recommend** upgrading to the latest version of Java.

In addition, all Java 1.5.x versions were removed from our list of CitiDirect-supported Java versions long ago.

Java 1.4

There is no option to enable "TLS 1.0" for this Java version. Therefore, we **strongly recommend** upgrading to the latest version of Java.

In addition, Java 1.4.x versions were removed from our list of CitiDirect-supported Java versions long ago.

Also, please note that public updates for these Java versions ended several years ago. See below from Oracle:

Major Release	General Availability Date	End of Public Updates
Java 4 (1.4.x)	February 2002	October 2008
Java 5 (1.5.x)	May 2004	October 2009

CitiDirect BE Mobile

For clients accessing CitiDirect BE℠ Mobile on their mobile device, please read below:

The Safari, Blackberry, and Internet Explorer mobile browsers all support TLS 1.0 by default, and should not require any additional changes. However, some older mobile phones may require an upgrade to a more recent mobile browser. When in doubt, please contact your IT Department or mobile phone providers for additional guidance and detailed instructions.