



Instrukcja dla Użytkowników CitiDirect:

Włączanie obsługi protokołu TLS w ustawieniach przeglądarki oraz panelu Java

Zastrzeżenie:

Ewentualne zmiany w związku z niniejszą instrukcją Posiadacz Rachunku wprowadza na własną odpowiedzialność. Jednocześnie przypominamy, że Bank Handlowy w Warszawie S.A. nie odpowiada za jakiegokolwiek szkody spowodowane użytkowaniem produktów innych dostawców.

Spis treści

Wstęp	3
Uzasadnienie – dlaczego konieczna jest zmiana ustawień?	3
Jak sprawdzić wersję przeglądarki internetowej?	5
Jak sprawdzić wersję oprogramowania Java?	6
Internet Explorer (IE) – wersja 7	7
Internet Explorer (IE) 8, 9 version	8
Internet Explorer (IE) – wersja 10, 11	9
MAC Safari	9
Java – wersje 7 i 8 (1.7 Aktualizacja xx oraz 1.8 Aktualizacja xx)	10
Java 1.7.0_10 do najnowszej Java 1.8	10
Java – wersja 1.7.0_0 do 1.7.0_9	11
Java – wersja 6 (1.6 Aktualizacja xx)	12
Java - wersja 1.6.0_19 do 1.6.0_45	12
Java - wersja 1.6.0 do 1.6.0_18	13
Java – wersja 5 (1.5 Aktualizacja xx)	14
Java – wersja 1.5.0_22 do 1.5.0_28	14
Java – wersja 1.5.0_6 do 1.5.0_21	15
Java – wersja 1.5.0 do 1.5.0_04	15
Java – wersja 1.4	16
CitiDirect EB Mobile	17

Wstęp

Niniejszy dokument jest instrukcją włączania obsługi protokołu TLS 1.0 dla Użytkowników CitiDirect.

Od dnia 14 lutego 2015 r. w celu zwiększenia bezpieczeństwa logowania przez portal CitiDirect EB (<https://portal.citidirect.com>) oraz korzystania z systemu CitiDirect zostanie zablokowana obsługa protokołu SSL 3.0 (Secure Sockets Layer), a w jego miejsce włączona zostanie obsługa protokołu TLS 1.0 (Transport Layer Security 1.0), który zapewnia wyższą ochronę przed atakami typu [POODLE](#).

Poniższa instrukcja ma za zadanie pomóc Użytkownikom CitiDirect skonfigurować ustawienia w odpowiedni sposób do dnia 14 lutego 2015 r., aby przygotować się na moment wyłączenia protokołu SSL 3.0 w CitiDirect, a tym samym zapewnić ciągłość Państwa pracy w systemie.

Od 14 lutego 2015 r. Użytkownicy, którzy nie włączą w ustawieniach przeglądarki oraz Panelu Java obsługi protokołu TLS nie będą mogli korzystać z systemu CitiDirect.

W związku z tym na komputerze każdego Użytkownika **należy już teraz sprawdzić, a w razie potrzeby zmienić, ustawienia protokołów bezpieczeństwa w przeglądarce internetowej oraz w ustawieniach Java**. Niniejsza instrukcja opisuje sposób zmiany niezbędnych ustawień w zależności od posiadanej wersji przeglądarki oraz oprogramowania Java.

Uzasadnienie – dlaczego konieczna jest zmiana ustawień?

W zabezpieczeniach wykorzystywanego dotychczas protokołu SSL 3.0 odkryto niedawno lukę. Do wykrycia słabości protokołu przyczynił się nowy atak sieciowy typu POODLE (czyli “Padding Oracle On Downgraded Legacy Encryption”). Wszystkie strony internetowe, które obsługują protokół SSL 3.0 są obecnie narażone na ataki tego typu. Najefektywniejszym sposobem zabezpieczenia się przed atakami POODLE jest jak najszybsze zablokowanie obsługi protokołu SSL 3.0 i uruchomienie zamiast niego obsługi protokołu TLS 1.0 w ustawieniach przeglądarki internetowej oraz ustawieniach Java. **Protokół TLS (Transport Layer Security) nie jest bowiem podatny na ataki POODLE.**

W związku z tym, w celu zwiększenia Państwa bezpieczeństwa, prosimy o włączenie obsługi protokołu TLS 1.0 w ustawieniach przeglądarki oraz w panelu ustawień Java. Wszystkie aktualne wersje przeglądarek oraz oprogramowania Java posiadają domyślnie włączoną obsługę protokołu TLS, jednak mógł on kiedyś zostać ręcznie zablokowany przez Użytkowników lub – w przypadku posiadania starej przeglądarki lub wersji Java, może nie być on obsługiwany.

W związku z powyższym, kluczowym jest **upewnienie się, że protokół TLS 1.0 na pewno jest u Państwa włączony, a w razie konieczności dokonanie odpowiedniej aktualizacji przeglądarki i oprogramowania Java do wersji, która obsługuje ten protokół.**

Ataki POODLE zostały zaklasyfikowane jako oficjalne zagrożenie sieciowe w różnych ogólnościowych indeksach dotyczących bezpieczeństwa w Internecie (poniższe strony są dostępne jedynie w języku angielskim):

United States Computer Emergency Readiness Team:

<https://www.us-cert.gov/ncas/alerts/TA14-290A>

Common Vulnerabilities and Exposures (CVE®) (jako pozycja CVE-2014-3566):

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

Ataki zostały również opisane przez **firmę Oracle** (dostawcę oprogramowania Java):

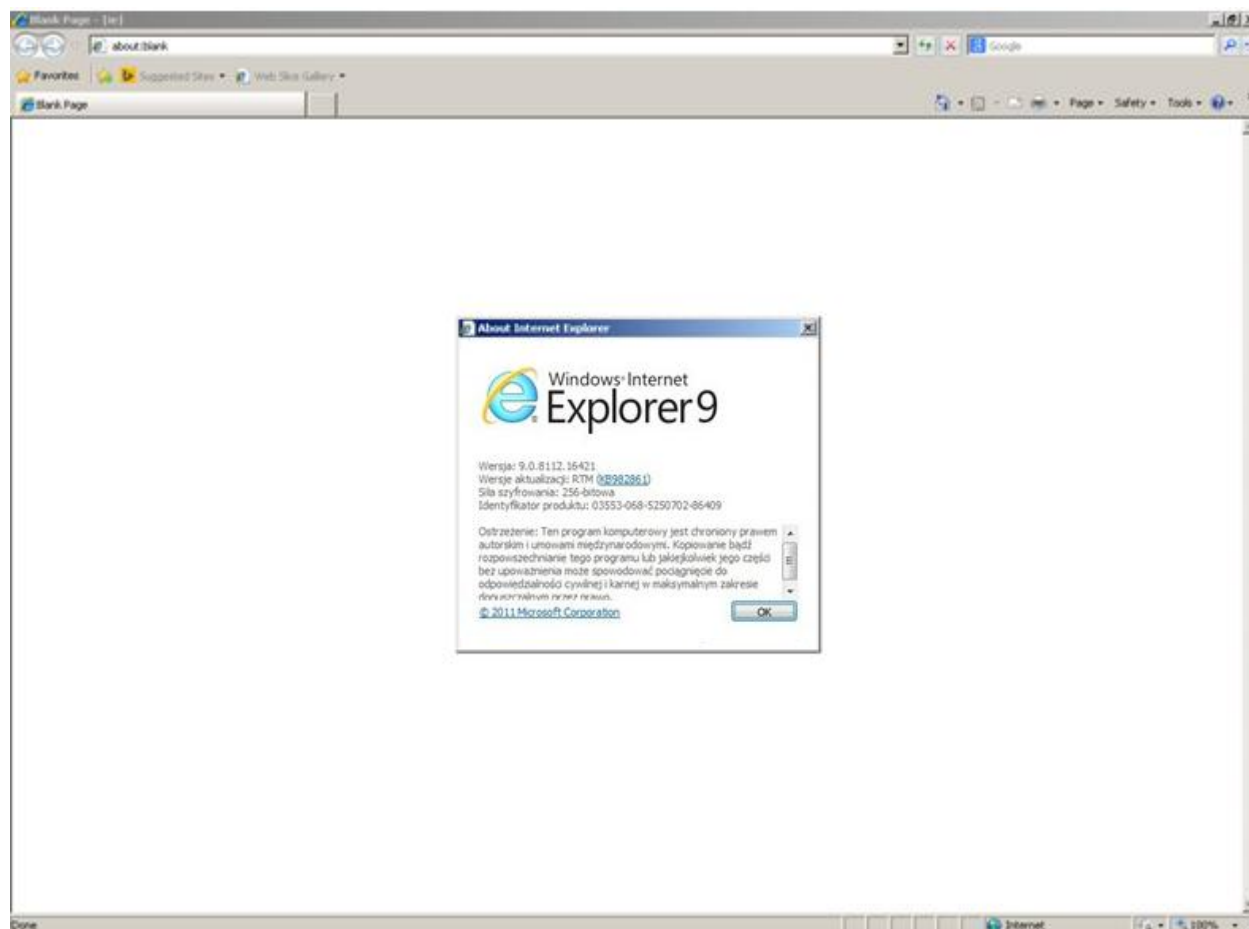
<http://www.oracle.com/technetwork/topics/security/poodlecve-2014-3566-2339408.html>

Jak sprawdzić wersję przeglądarki internetowej?

W celu sprawdzenia, jaka wersja przeglądarki internetowej Internet Explorer zainstalowana jest na komputerze, należy wykonać poniższe kroki.

Internet Explorer

- Uruchom przeglądarkę Internet Explorer i przejdź do menu Pomoc (ikona  w prawym górnym rogu) a następnie do pozycji → Internet Explorer – Informacje. W oknie wyświetli się informacja o wersji przeglądarki.



Zależnie posiadanej wersji przeglądarki, proszę kliknąć na odpowiedni link poniżej – przeniesie on Państwa do stosownej sekcji w niniejszej instrukcji.

- [Internet Explorer \(IE\) – wersja 7](#)
- [Internet Explorer \(IE\) 8, 9](#)
- [Internet Explorer \(IE\) – wersje 10, 11](#)
- [Przeglądarka MAC Safari](#)

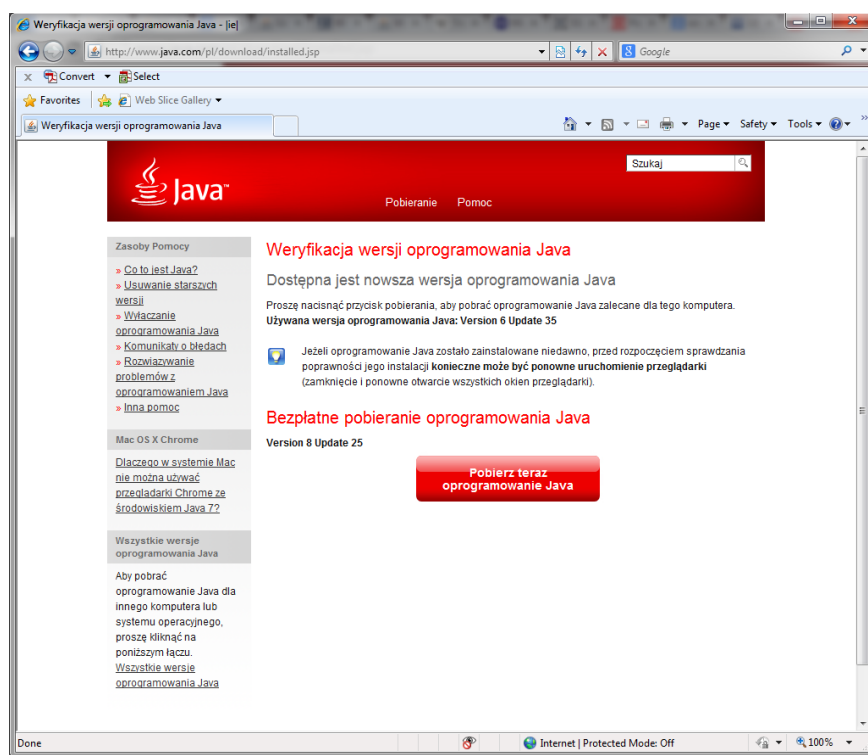
Jak sprawdzić wersję oprogramowania Java?

W celu sprawdzenia, jaka wersja oprogramowania Java zainstalowana jest na komputerze, należy wykonać poniższe kroki:

- Uruchom przeglądarkę Internet Explorer i przejdź na poniższą stronę:

www.java.com/pl/download/installed.jsp?detect=jre

Jeżeli Java została poprawnie zainstalowana na ekranie wyświetli się obecnie używana wersja Java – strona będzie wyglądać podobnie do tej poniżej:



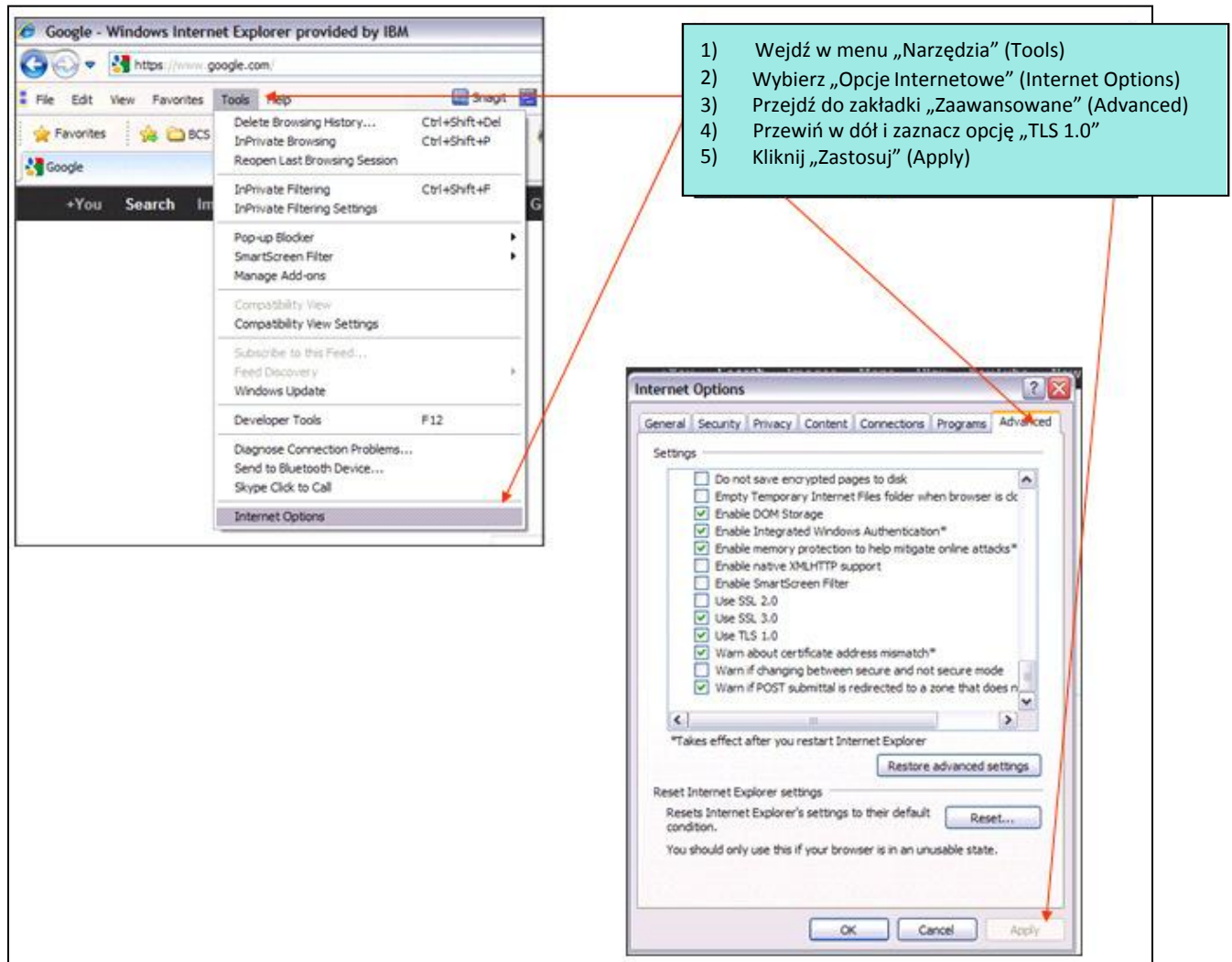
W zależności od posiadanej wersji Java proszę wybrać odpowiedni link z listy – przeniesie on Państwa do stosownej sekcji w niniejszej instrukcji.

- [Java 1.5.0 do 1.5.0 04](#)
- [Java 1.5.0 6 do 1.5.0 21](#)
- [Java 1.5.0 22 do 1.5.0 28](#)
- [Java 1.6.0 do 1.6.0 18](#)
- [Java 1.6.0 19 do 1.6.0 45](#)
- [Java 1.7.0 0 do 1.7.0 9](#)
- [Java 1.7.0 10 do 1.8 \(najnowsza\)](#)

Uwaga: Najnowsze wersje Java oraz przeglądarek internetowych mają domyślnie włączoną obsługę protokołu TLS 1.0. Jednak mimo to zalecamy sprawdzenie, czy protokół jest na pewno włączony w wersji Java oraz przeglądarki posiadanej przez Państwa.

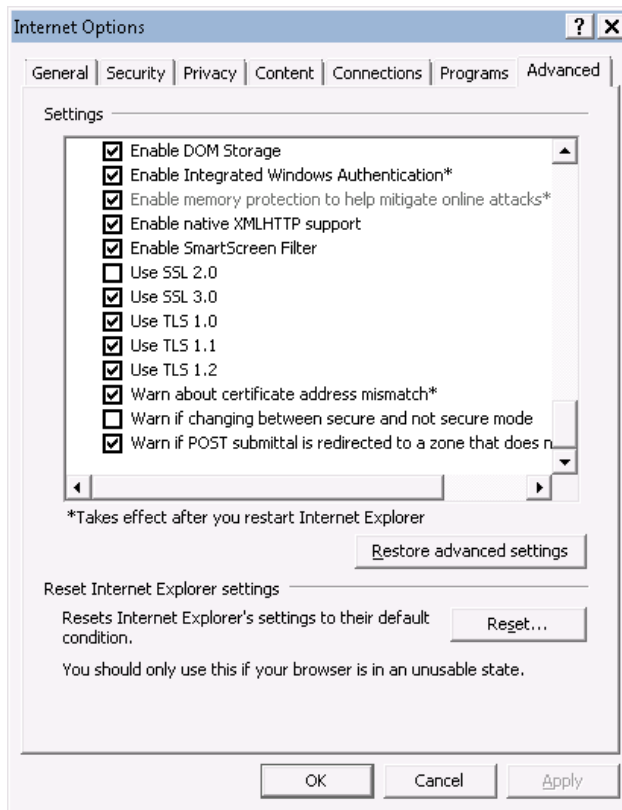
Internet Explorer (IE) – wersja 7

1. Uruchom przeglądarkę Internet Explorer i przejdź do menu “Narzędzia” (Tools) w górnej części ekranu.
2. Wybierz “Opcje Internetowe” (Internet Options)
3. W oknie Opcji Internetowych przejdź do zakładki “Zaawansowane” (Advanced)
4. Przewiń w dół w zakładce Zaawansowane i zaznacz opcję “TLS 1.0”
5. Kliknij “Zastosuj” (Apply).



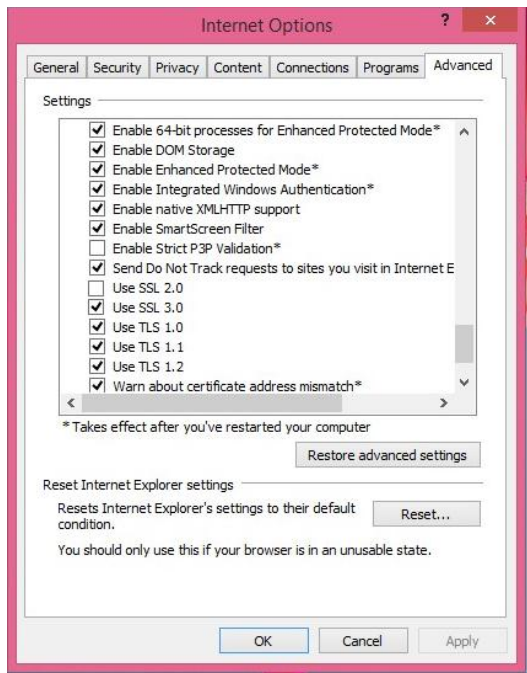
Internet Explorer (IE) 8, 9 version

1. Uruchom przeglądarkę Internet Explorer i przejdź do menu “Narzędzia” (Tools) w górnej części ekranu.
2. Wybierz “Opcje Internetowe” (Internet Options)
3. W oknie Opcji Internetowych przejdź do zakładki “Zaawansowane” (Advanced)
4. Przewiń w dół w zakładce Zaawansowane i zaznacz opcję “**TLS 1.0**”
5. Kliknij “Zastosuj” (Apply).



Internet Explorer (IE) – wersja 10, 11

1. Uruchom przeglądarkę Internet Explorer i przejdź do menu “Narzędzia” (Tools) w górnej części ekranu.
2. Wybierz “Opcje Internetowe” (Internet Options)
3. W oknie Opcji Internetowych przejdź do zakładki “Zaawansowane” (Advanced)
4. Przewiń w dół w zakładce Zaawansowane i zaznacz opcję “**TLS 1.0**”
5. Kliknij “Zastosuj” (Apply).



MAC Safari

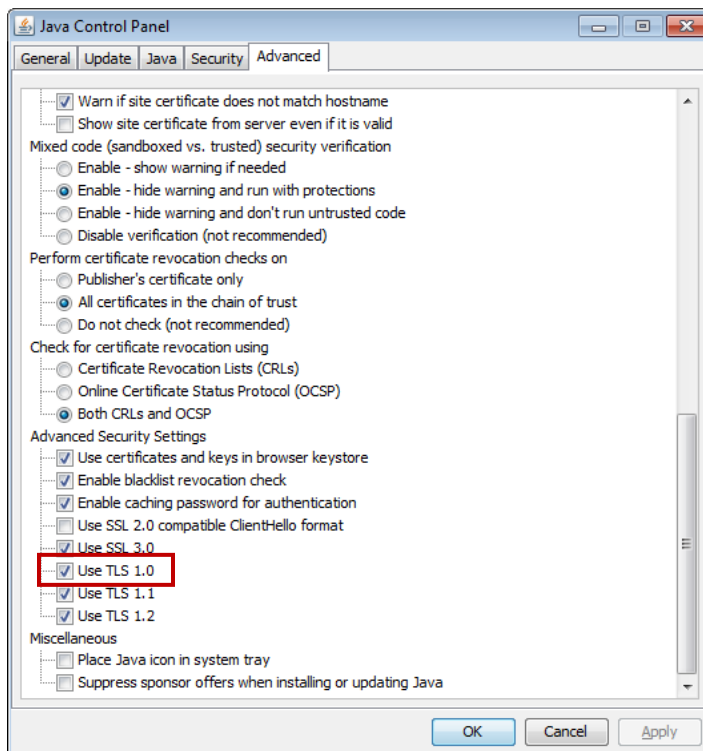
W przeglądarce Safari nie jest wymagana żadna zmiana w ustawieniach.

Java – wersje 7 i 8 (1.7 Aktualizacja xx oraz 1.8 Aktualizacja xx)

W zależności od zainstalowanej aktualizacji danej wersji Java, proszę podjąć następujące kroki:

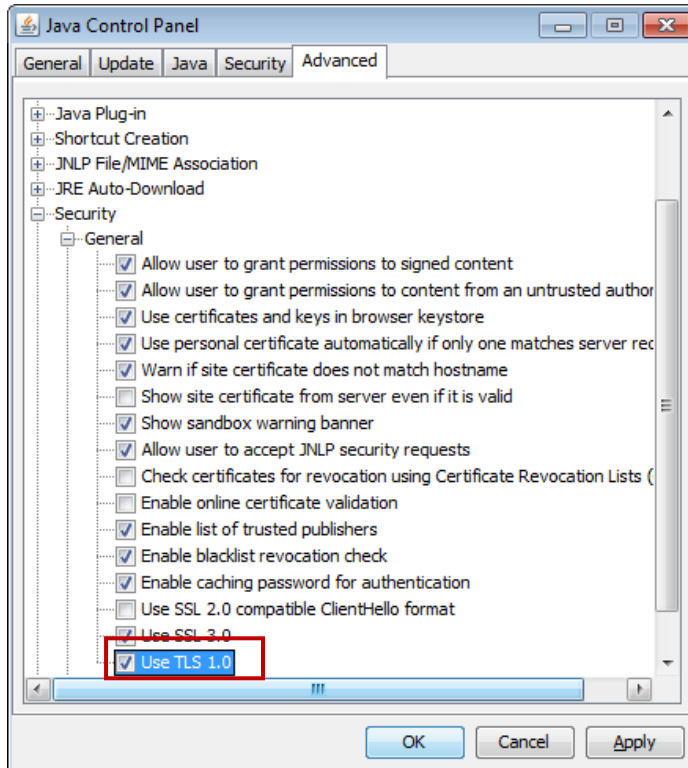
Java 1.7.0_10 do najnowszej Java 1.8

1. Przejdź do panelu “Java Control Panel” (można go odnaleźć klikając, bądź wyszukując Java w Panelu Sterowania)
2. Przejdź do zakładki “Advanced” (Zaawansowane)
3. W sekcji “Advanced Security Settings” zaznacz opcję „Use TLS 1.0”, a następnie kliknij „Apply” (Zastosuj) oraz “OK”.



Java – wersja 1.7.0_0 do 1.7.0_9

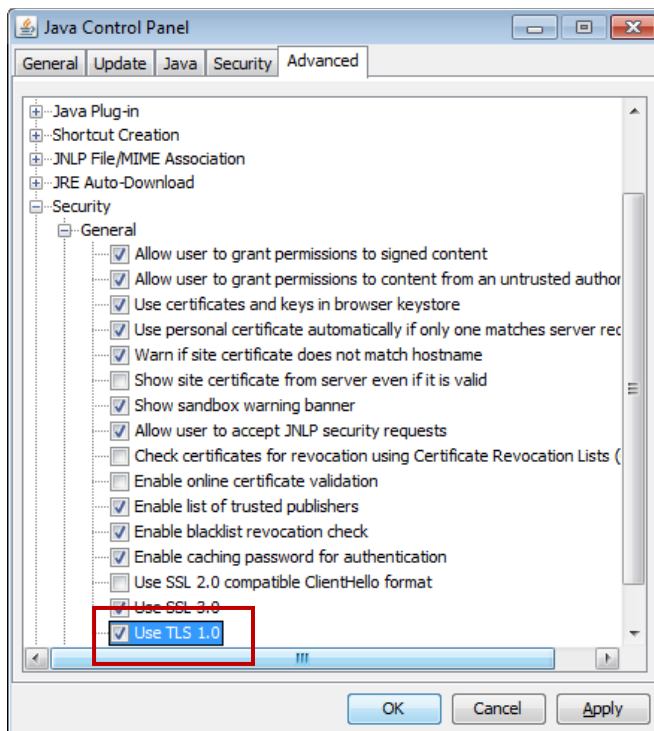
1. Przejdź do panelu “Java Control Panel” (można go odnaleźć klikając bądź wyszukując Java w Panelu Sterowania)
2. Przejdź do zakładki “Advanced” (Zaawansowane)
3. W sekcji “Security” → “General” → zaznacz opcję “Use TLS 1.0”, a następnie kliknij „Apply” (Zastosuj) oraz “OK”.



Java – wersja 6 (1.6 Aktualizacja xx)

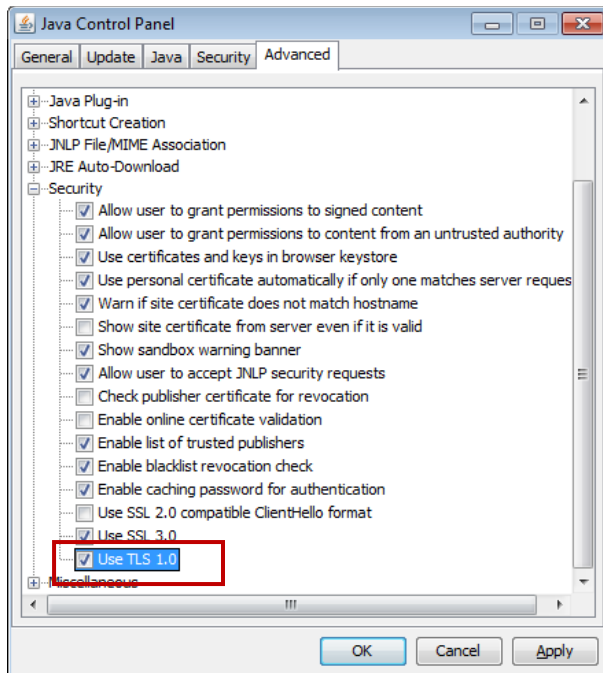
Java - wersja 1.6.0_19 do 1.6.0_45

1. Przejdź do panelu “Java Control Panel” (można go odnaleźć klikając bądź wyszukując Java w Panelu Sterowania)
2. Przejdź do zakładki “Advanced” (Zaawansowane)
3. W sekcji “Security” → “General” → zaznacz opcję “Use TLS 1.0” a następnie kliknij „Apply” (Zastosuj) oraz “OK”.



Java - wersja 1.6.0 do 1.6.0_18

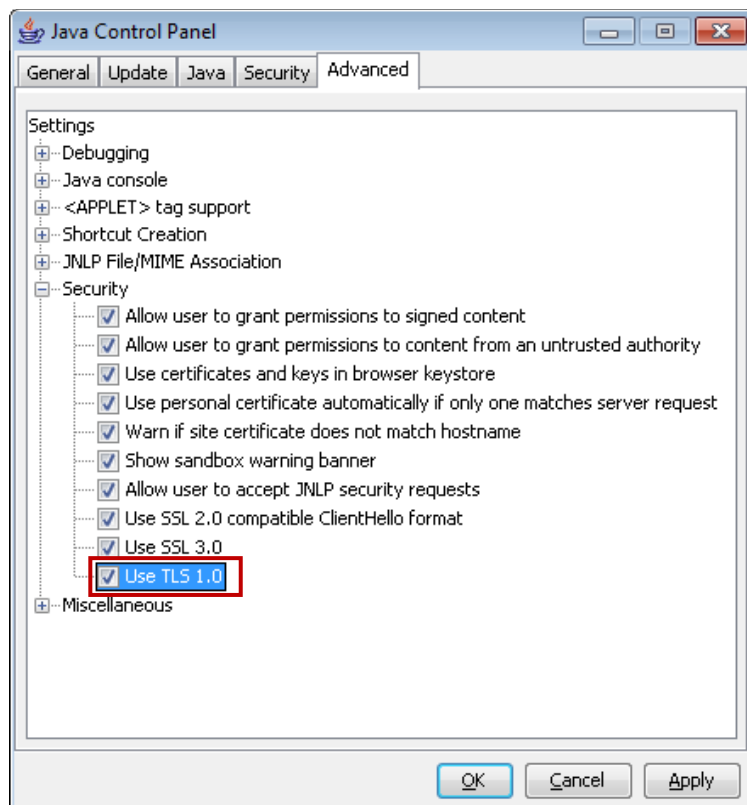
1. Przejdź do panelu "Java Control Panel" (można go odnaleźć klikając bądź wyszukując Java w Panelu Sterowania)
2. Przejdź do zakładki "Advanced" (Zaawansowane)
3. W sekcji "Security" zaznacz opcję "Use TLS 1.0" a następnie kliknij „Apply” (Zastosuj) oraz “OK”.



Java – wersja 5 (1.5 Aktualizacja xx)

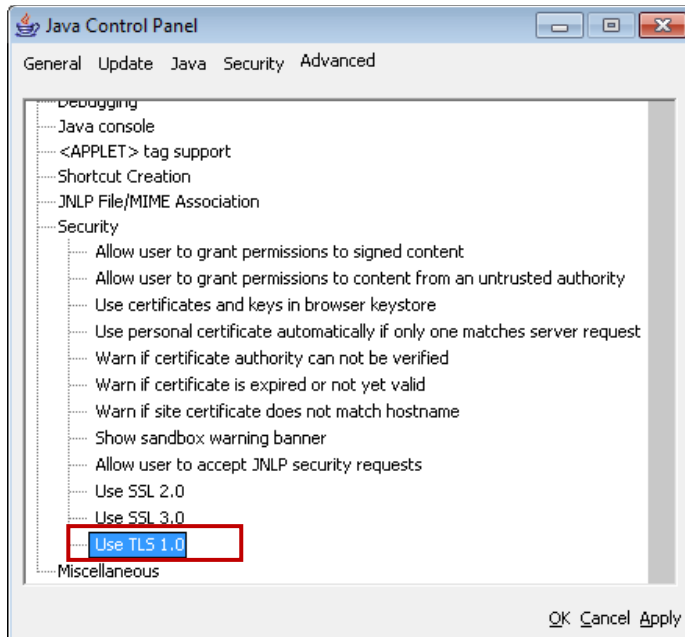
Java – wersja 1.5.0_22 do 1.5.0_28

1. Przejdź do panelu “Java Control Panel” (można go odnaleźć klikając bądź wyszukując Java w Panelu Sterowania)
2. Przejdź do zakładki “Advanced” (Zaawansowane)
3. W sekcji “Security” zaznacz opcję “Use TLS 1.0” a następnie kliknij „Apply” (Zastosuj) oraz “OK”.



Java – wersja 1.5.0_6 do 1.5.0_21

1. Przejdź do panelu “Java Control Panel” (można go odnaleźć klikając bądź wyszukując Java w Panelu Sterowania)
2. Przejdź do zakładki “Advanced” (Zaawansowane)
3. W sekcji “Security” zaznacz opcję “Use TLS 1.0” a następnie kliknij „Apply” (Zastosuj) oraz “OK”.



Java – wersja 1.5.0 do 1.5.0_04

W tej wersji Java nie ma możliwości włączenia obsługi protokołu TLS 1.0. W związku z tym zdecydowanie **zalecamy aktualizację** do najnowszej wersji Java.

Ponadto wszystkie wersje Java 1.5.x zostały usunięte z listy wersji Java certyfikowanych do współpracy z CitiDirect.

Java – wersja 1.4

W tej wersji Java nie ma możliwości włączenia obsługi protokołu TLS 1.0. W związku z tym zdecydowanie **zalecamy aktualizację** do najnowszej wersji Java.

Ponadto wszystkie wersje Java 1.4.x zostały usunięte z listy wersji Java certyfikowanych do współpracy z CitiDirect.

Prosimy wziąć pod uwagę, że wersje 4 i 5 Java są nieaktualne od ponad 5 lat – firma Oracle zaprzestała świadczenia związanej z tymi wersjami pomocy technicznej w latach wymienionych w tabeli poniżej.

Wersja Java	Data wydania wersji	Data zakończenia wsparcia wersji przez firmę Oracle
Java 4 (1.4.x)	Luty 2002	Październik 2008
Java 5 (1.5.x)	Maj 2004	Październik 2009

CitiDirect EB Mobile

Informacja dla Klientów logujących się do mobilnej wersji CitiDirect EBSM:

Przeglądarki mobilne Safari, Blackberry oraz Internet Explorer mają domyślnie włączoną obsługę protokołu TLS 1.0 i nie wymagają żadnych dodatkowych zmian. Jednak niektóre starsze modele telefonów mogą wymagać aktualizacji przeglądarki mobilnej do nowszej wersji. W razie wątpliwości prosimy o kontakt z departamentem IT w Państwa firmie lub z dostawcą telefonu komórkowego w celu uzyskania szczegółowych instrukcji.

Niniejszy materiał został wydany jedynie w celach informacyjnych i nie stanowi oferty w rozumieniu art. 66 Kodeksu Cywilnego.

Bank Handlowy w Warszawie S.A. z siedzibą w Warszawie, ul. Senatorska 16, 00-923 Warszawa, zarejestrowany w rejestrze przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod nr. KRS 000 000 1538; NIP 526-030-02-91; wysokość kapitału zakładowego wynosi 522.638.400 złotych, kapitał został w pełni opłacony.

Citi Handlowy oraz CitiDirect są zastrzeżonymi znakami towarowym należącym do podmiotów z grupy Citigroup Inc.