CitiDirect® Portal
Bezpieczeństwo, wymagania techniczne i konfiguracja

CitiService
Pomoc Techniczna CitiDirect
tel. 801 343 978, +48 22 690 15 21
poniedziałek – piątek; 8:00 – 17:00
helpdesk.ebs@citi.com

www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

citi handlowy®

Spis treści

1. Bezpieczeństwo

Oferujemy bardzo wysokie standardy zabezpieczeń, aby zapewnić naszym Klientom bezpieczeństwo podczas korzystania z CitiDirect, CitiDirect Mobile oraz CitiDirect Tablet. Prosimy jednak pamiętać, że bezpieczeństwo Państwa środków zależy również od Państwa.

1.1 Identyfikacja i weryfikacja Użytkownika

Dostęp do CitiDirect jest przypisany do Użytkowników, którzy logują się do systemu za pomocą swojej karty SafeWord (tzw. tokena) lub tokena mobilnego MobilePASS.

Karta przypisana jest do konkretnego Użytkownika. Karta generuje dynamiczne, jednorazowe hasła, które w znacznym stopniu ograniczają ryzyko uzyskania dostępu do CitiDirect przez osoby nieuprawnione, np. poprzez kradzież lub złamanie hasła. Dodatkowo sama karta zabezpieczona jest 4-cyfrowym numerem PIN, znanym tylko jej Posiadaczowi. Numer PIN może być w dowolnym momencie zmieniony przez Posiadacza karty.

1.2 Poziomy uprawnień Użytkowników

Uprawnienia Użytkowników kontrolowane są za pomocą ich profili dostępowych, które określają konkretny poziom dostępu do funkcji w systemie CitiDirect. Profile dostępowe nadane Użytkownikom definiują:

- dostęp do określonych rachunków i typów transakcji
- możliwość wykonywania działań w ramach transakcji o ustalonym limicie kwotowym
- schematy i limity autoryzacji itd.

1.3 Wielostopniowa autoryzacja transakcji

Nawet najlepiej zaprojektowane wewnętrzne procesy mogą okazać się niewystarczające, gdy tylko jedna osoba ma pełną kontrolę nad transakcjami w systemie. Dlatego rekomendujemy schematy autoryzacyjne wymagające akceptacji dodatkowego Użytkownika lub Użytkowników. Bank oferuje aż do 9 poziomów autoryzacji. Wybierając wyższy poziom autoryzacji wymaganej podczas zlecania płatności w CitiDirect, można w znacznym stopniu wzmocnić poziom bezpieczeństwa.

Zalecamy zdefiniowanie w firmie przynajmniej jednego poziomu autoryzacji transakcji.

Bank oferuje również inne funkcjonalności ograniczające ryzyko, takie jak blokada ręcznego tworzenia płatności przez Użytkowników, wprowadzenie konieczności autoryzacji tworzonych szablonów płatności oraz ustawienie limitów płatności. W celu ustanowienia takich dodatkowych zabezpieczeń prosimy o kontakt z Państwa Doradcą Bankowym.

1.4 Sesja szyfrowania i cyfrowy certyfikat bezpieczeństwa

Wszystkie informacje, począwszy od identyfikacji Klienta aż do momentu zakończenia sesji CitiDirect, są zabezpieczone protokołem TLS (Transport Layer Security), gwarantującym poufność przesyłanych danych za pomocą zaawansowanych metod szyfrowania.

Protokół TLS chroni także spójność danych. Jego elementem jest Kod Weryfikacji Autentyczności (Message Authentication Code – MAC) wykrywający, czy w trakcie transmisji dane nie zostały zmienione w sposób nieautoryzowany.

Nasz serwis https://portal.citidirect.com jest zabezpieczony cyfrowym certyfikatem Symantec Class 3 EV SSL CA – G3. Jest to cyfrowy podpis strony potwierdzający, że Użytkownik znajduje się w serwisie, którego właścicielem jest Citi Handlowy. Certyfikat gwarantuje, że wszystkie poufne transakcje dokonywane za pośrednictwem CitiDirect są zaszyfrowane.

Przed logowaniem do serwisu sprawdź aktualność oraz wystawcę certyfikatu.

1.5 Automatyczne przerywanie sesji

Każda sesja jest automatycznie przerywana po 20 minutach od ostatniej wykonanej czynności w celu uniemożliwienia dostępu do rachunków osobom trzecim, jeśli Użytkownik zapomni wylogować się z serwisu.

1.6 Blokowanie Użytkowników

W celu zapewnienia bezpieczeństwa Państwa środkom karta SafeWord oraz Użytkownik są automatycznie blokowane w przypadku 7 błędnych prób zalogowania i/lub po 12 miesiącach od:

- daty ostatniego logowania – w przypadku Użytkowników, którzy logowali się do systemu lub
- daty utworzenia Użytkownika w systemie – w przypadku osób nigdy nielogujących się do systemu.

W celu utrzymania dostępu do systemu CitiDirect na danej karcie SafeWord zalecamy zalogować się do systemu co najmniej raz na 3 miesiące. Zablokowaną kartę SafeWord należy wymienić, jeżeli Użytkownik zamierza korzystać w przyszłości z systemu CitiDirect, co należy zgłosić osobnym wnioskiem.

W przypadku utraty lub uszkodzenia karty SafeWord należy niezwłocznie skontaktować się z CitiService pod numerem **(22) 690 19 81** lub **801 24 84 24** w celu zablokowania dostępu do CitiDirect.

Zwracamy szczególną uwagę na kwestie związane z bezpieczeństwem w Internecie – odzwiedź serwis:
www.citidirect.pl/bezpieczenstwo.

Tematy w serwisie prezentowane są w uporządkowanych sekcjach, stanowiąc cenne źródło informacji nt. zabezpieczeń płatności elektronicznych oraz cyberzagrożeń związanych m.in. z codziennym korzystaniem z bankowości internetowej.

Niezależnie od wielopoziomowych zabezpieczeń zastosowanych przez Citi Handlowy:

- chroń dane osobowe – rozważnie korzystaj z Internetu
- chroń narzędzia i dane służące do logowania i autoryzacji transakcji
- korzystaj z najnowszej wersji systemu operacyjnego oraz przeglądarek internetowych
- używaj aktualnego oprogramowania antywirusowego oraz zapory sieciowej (firewall)
- nie instaluj nielegalnego oprogramowania pochodzącego z niezaufanych źródeł
- nie odpowiadaj na wiadomości e-mail, w których umieszczona jest prośba o podanie danych osobowych lub kodów dostępu
- nie otwieraj załączników i nie uruchamiaj żadnych linków w podejrzanych wiadomościach mailowych oraz SMS
- loguj się do serwisu bankowości elektronicznej z zaufanego komputera i sieci (unikaj tzw. hot-spotów), wprowadzając konkretny adres URL – nie wyszukuj go, korzystając z wyszukiwarek
- sprawdzaj, czy połączenie podczas logowania jest bezpieczne (https, SSL, TLS).

2. Wymagania systemowe

2.1 Systemy operacyjne

System posiada certyfikat zgodności z poniższymi systemami operacyjnymi.

Systemy Windows®:

- Windows® 7, z wyjątkiem wersji arabskiej
- Windows® 10, z wyjątkiem wersji arabskiej.

Systemy Apple® macOS:

- wersje od 10.12 i nowsze.

2.2 Przeglądarki internetowe

- Internet Explorer 11.0 (Windows 7)
- Internet Explorer 11.0 (Windows 10)
- Safari: wersja 10 i nowsze.

2.3 Oprogramowanie Java (opcjonalnie)

System CitiDirect wspiera oprogramowanie Java w wersji:

- Java 8.

2.4 Adobe Reader

Program Adobe Reader jest wykorzystywany do podglądu wygenerowanych w CitiDirect raportów w formacie PDF. Wspierane wersje programu Adobe Reader:

- Wersja 9.0 lub nowsza.

2.5 Sieć / dostęp do Internetu

- transfer do/z sieci zewnętrznej (dla pojedynczej stacji) min. 128 kbs, zalecany 512 kbs
- otwarte porty http (80) i https (443)
- brak skanowania, blokowania oraz cache'owania apletów Javy i Active X z adresu: https://portal.citidirect.com
- włączona obsługa protokołu TLS 1.2 w ustawieniach przeglądarki oraz (opcjonalnie) Java.

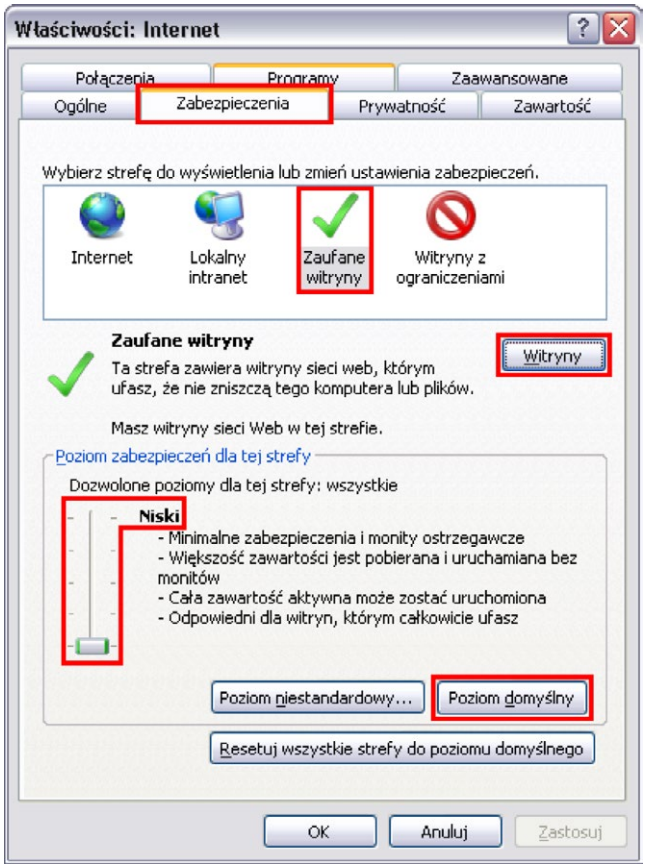
Szczegółowe informacje na temat wymagań technicznych systemu CitiDirect znajdują się na stronie logowania.

3. Konfiguracja

3.1 Internet Explorer

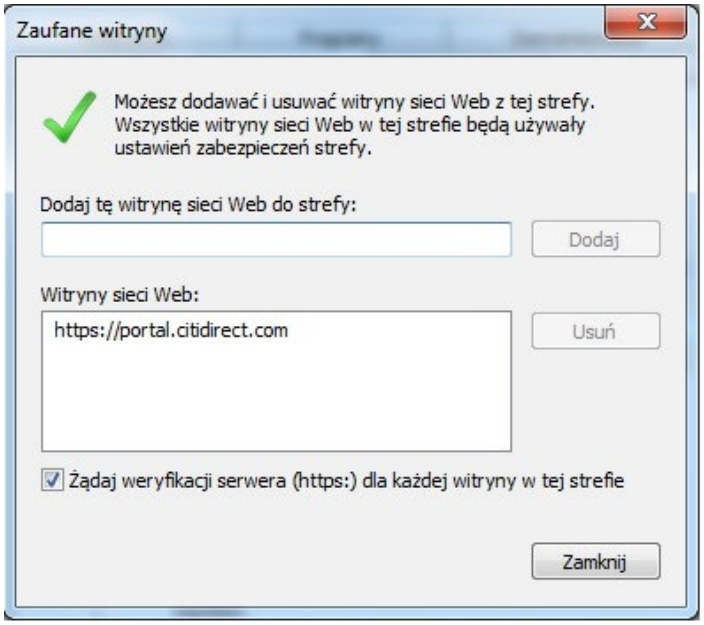
CitiDirect działa prawidłowo przy domyślnych ustawieniach opcji internetowych. W celu optymalizacji wydajności zalecamy zastosowanie poniższych ustawień.

Uruchom przeglądarkę i wejdź w **Narzędzia → Opcje internetowe**

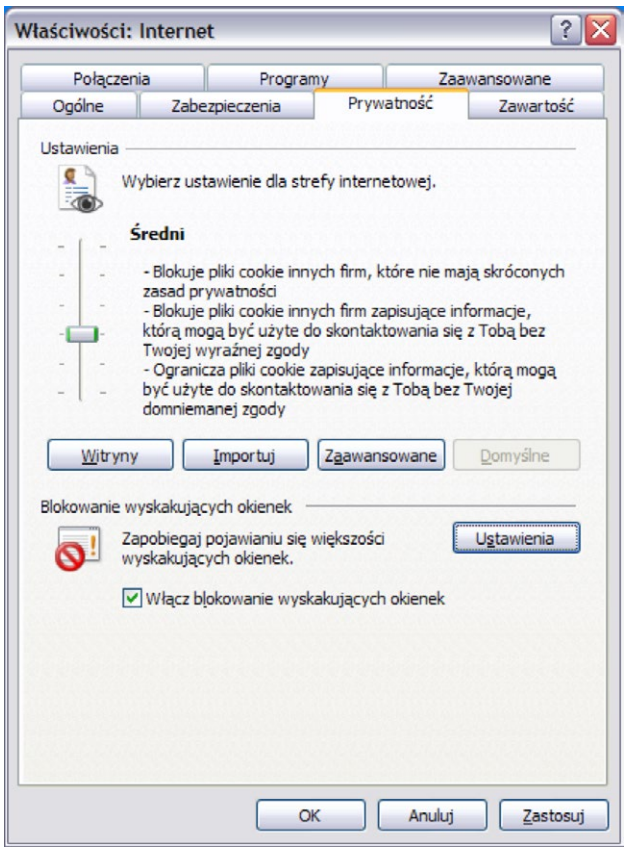


Zakładka **Zabezpieczenia**

W oknie wyboru stref kliknij **Zaufane witryny**. Najprawdopodobniej poziom zabezpieczeń dla tej strefy będzie ustawiony na Niestandardowy. Zresetuj ustawienia, klikając przycisk **Poziom domyślny,** a następnie przesuwając suwak na sam dół, ustaw najniższy możliwy poziom zabezpieczeń – Niski.

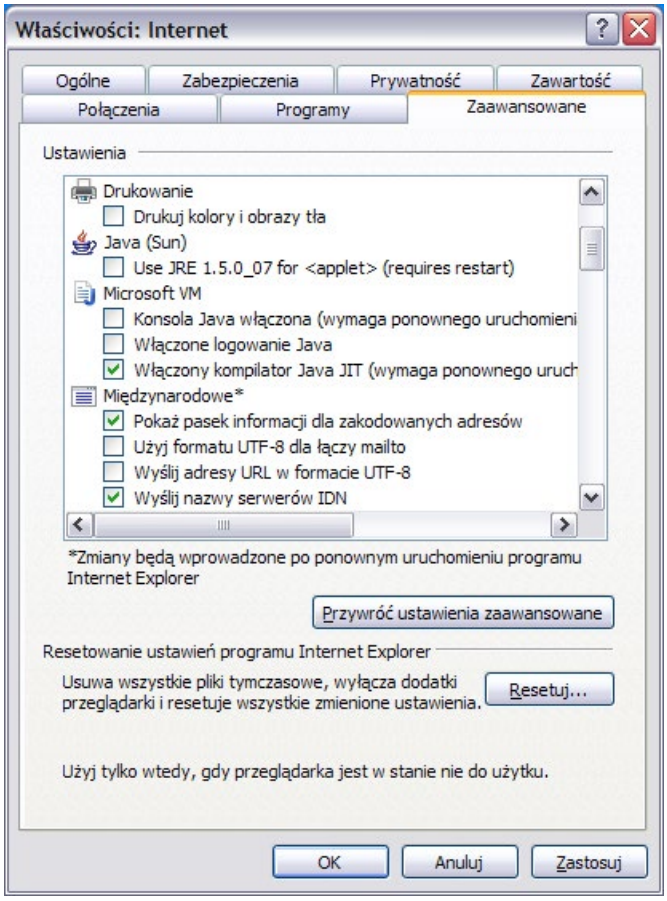


Otwórz listę witryn zaufanych, klikając przycisk **Witryny** i dodaj do niej adres systemu CitiDirect: https://portal.citidirect.com.



Zakładka **Prywatność**

Sekcja **Ustawienia** ma wpływ na to, czy przeglądarka będzie pamiętała założonego Użytkownika na stronie logowania. Powinien być tu wybrany domyślny poziom – Średni – lub niższy.

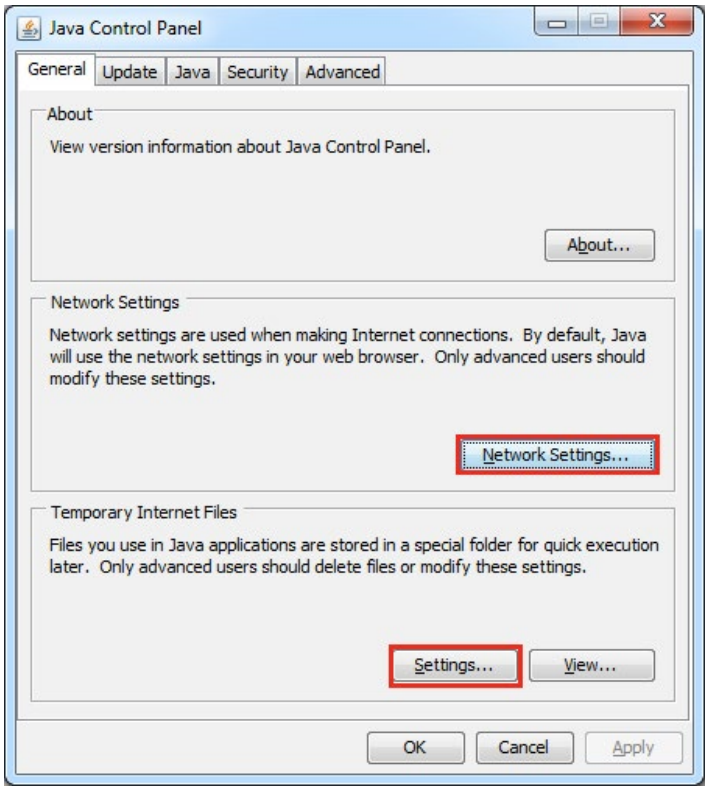


Zakładka **Zaawansowane**

Zalecamy zastosowanie ustawień domyślnych. Gdy nie masz pewności, czy ustawienia są domyślne, kliknij przycisk **Przywróć ustawienia zaawansowane**, następnie **Zastosuj**.

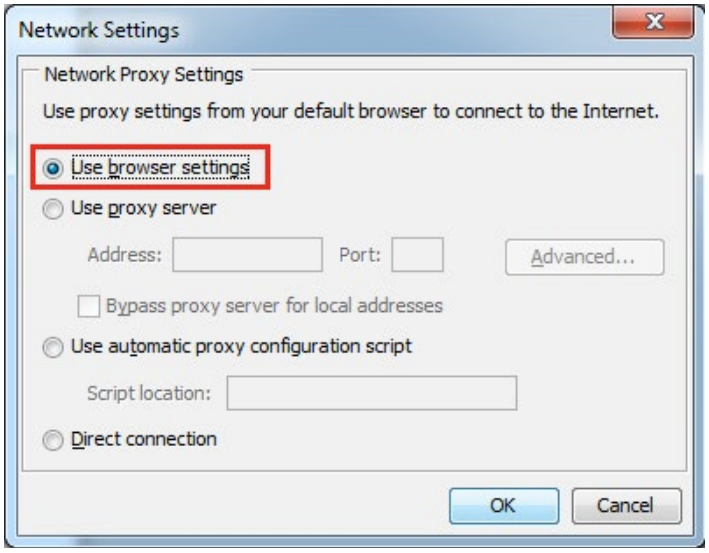
3.2. Java Sun

Z menu **START** systemu Windows wybierz **JAVA CONFIGURATION**.



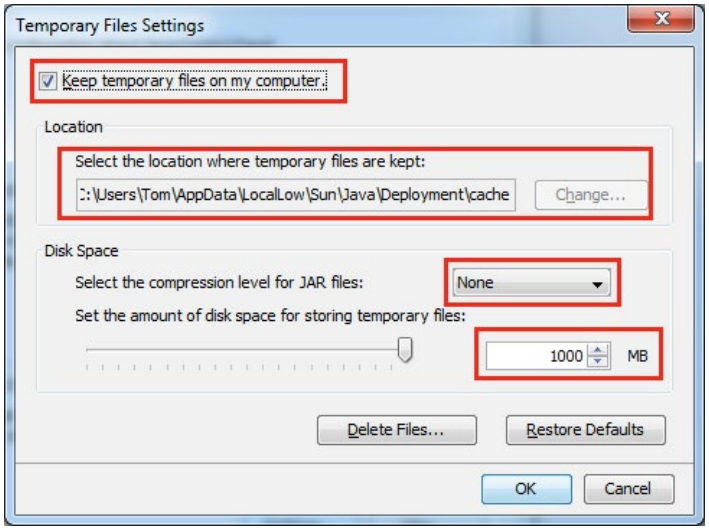
Zakładka **General**

Ustawienia mające wpływ na CitiDirect znajdują się w sekcjach **Network Settings Temporary Internet Files**.



Network Setting

Wybierz opcję **Use browser settings**.



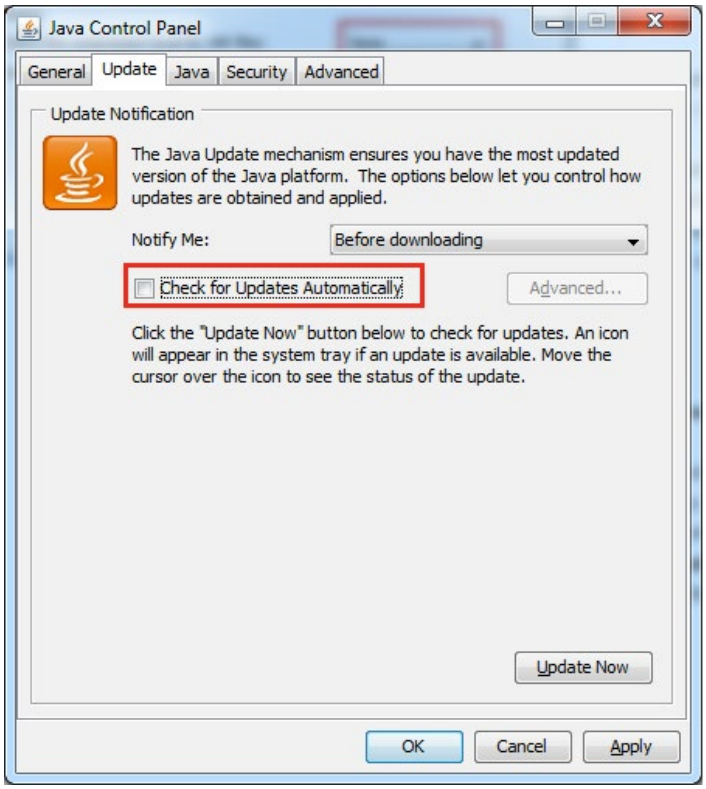
Temporary Internet Files

Keep temporary files on my computer – ta opcja musi być zaznaczona.

Location – Użytkownik Windows musi mieć pełny dostęp do podanego tu katalogu.

Poziom kompresji musi być ustawiony na **None**.

Ilość miejsca na dysku twardym powinna być nie mniejsza niż 250 MB. Domyślne ustawienie – **1000 MB**.



Zakładka **Update**

Zalecamy wyłączenie aktualizacji automatycznych.
W tym celu odznacz opcję **Check for updates Automatically**.

www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

citi handlowy®