

Konfiguracja przeglądarek internetowych

Poniżej przedstawiona została lista najpopularniejszych przeglądarek ze szczegółową konfiguracją:

- . Mozilla Firefox
- . Internet Explorer 5.0 i późniejsze
- . Internet Explorer 7
- . Netscape 7.1 [eng]
- . Netscape 8
- . Opera 6.05 [eng]
- . Opera 7.2 [pl]
- . Opera 8 i 9 [pl]
- . Sylaba Communicator 4.7

Błędy i komunikaty zwracane przez serwery WWW

Serwer WWW podczas komunikowania się z Twoją przeglądarką wysyła za każdym razem serię komunikatów. Podzielone są one wedle znaczenia, a każda z kategorii ma swój liczbowy przedrostek. Komunikaty zaczynające się od liczby 200 oznaczają udaną transakcję pomiędzy Twoją przeglądarką a serwerem WWW. Komunikaty zaczynające się od liczby 300 informują przeglądarkę, że nastąpi przekierowanie na inną stronę. O ile powyższych komunikatów raczej nie zobaczysz, to z kolejnymi na pewno się spotkałeś. Jeśli komunikat zaczyna się od liczby 400 wina leży po stronie przeglądarki lub Twojej. Komunikaty zaczynające się od 500 oznaczają błąd serwera lub skryptu na serwerze.

Lista błędów:

- . 400 Bad Request - wysłane zapytanie zawiera błąd, dane nie mogą zostać pobrane
- . 401 Unauthorised - strona wymaga autoryzacji, jednakże nie jesteś zalogowany
- . 402 Payment Required - strona wymaga opłaty za oglądanie, jednakże wpłata nie została dokonana
- . 403 Forbidden - dostęp do danych został zabroniony lub nie powiodła się wymagana autoryzacja
- . 404 Not Found - plik nie został odnaleziony
- . 407 Proxy Authentication Required - serwer proxy, z którego korzystasz wymaga autoryzacji
- . 500 Server Error - serwer napotkał na niespodziewany błąd podczas spełniania zapytania (zwykle oznacza to błąd wykonywanego skryptu)
- . 501 Not Implemented - serwer nie obsługuje funkcji, o które wysłała zapytanie Twoja przeglądarka
- . 502 Server overloaded - serwer jest przeciążony i nie jest w stanie obsłużyć kolejnego zapytania

1. Mam problem z dostępem do strony mojego banku i innej strony bezpiecznej. Co robić?

Sprawdź 'siłę szyfrowania' swojej przeglądarki:

- w Internet Explorerze jest to na ogół pod pozycją 'Internet Explorer - Informacje' w menu 'Pomoc'

- w Netscape Navigator należy: wybrać 'Security Info' z menu 'Communicator > Tools'. Kliknij na 'Navigator'. Sprawdź w 'Configure SSL v2' i 'Configure SSL v3' czy występują opcje szyfrowania 128 bitów lub silniejszego

Siła szyfrowania powinna wynosić 128 bitów.

Wyjaśnienie:

Przeglądarki standardowo udostępniane są w dwóch wersjach. O zwykłej sile szyfrowania (zwyczajowo 40 lub 56 bitów) oraz o większej sile szyfrowania (128 bitów).

Ze względu na rosnącą geometrycznie moc komputerów w chwili obecnej używane w przeglądarce szyfry o długości 40 a nawet 56 bitów stają się w chwili obecnej coraz mniej bezpieczne, coraz prostsze do złamania, dlatego większość stron operujących Twoimi zasobami wymaga by Twoja przeglądarka używała silniejszego, a tym samym trudniejszego do złamania szyfrowania 128 bitowego lub udostępni Ci specjalny program z wbudowanymi często wielokrotnie silniejszymi algorytmami szyfrowania.

2. Czemu wszystkie przeglądarki nie mają takiej samej mocy szyfrowania?

Większość najpopularniejszych w internecie i używanych w przeglądarkach Internet Explorer i Netscape Navigator technologii kryptograficznych, powstaje w Stanach Zjednoczonych lub na podstawie licencji lub oprogramowania firm amerykańskich. Rząd amerykański w ramach sankcji gospodarczych prowadzi od wielu lat embargo na przepływ najnowszych technologii, superkomputerów (HPC) oraz oprogramowania ze szczególnym naciskiem na oprogramowanie kryptograficzne. Instytucje działające w innych krajach, nie związane w żaden sposób z amerykańskimi firmami, działają na podstawie prawodawstwa danego kraju. Korzystając z systemów szyfrowania powstających w USA i innych krajach radzimy dokładnie zapoznać się z umową licencyjną, gdyż konkretne algorytmy mogą być objęte restrykcjami eksportowymi danego kraju, a więc korzystanie z nich może być na terenie Polski nielegalne i możesz nieświadomie łamać prawo. Więcej informacji dotyczących eksportu z terenu USA oraz Kanady znajdziesz pod adresem: <http://www.bxa.doc.gov/> (strona w języku angielskim).

3. Jestem na terenie Polski, używam przeglądarki WWW z niskim poziomem szyfrowania. Co mam zrobić aby zwiększyć siłę szyfrowania?

Jeśli używasz przeglądarki Internet Explorer w wersji 4.0 lub późniejszej powinieneś zajrzeć na stronę http://www.microsoft.com/windows/ie_intl/pl/download/128bit/intro.htm. Ze strony tej będziesz mógł uaktualnić przeglądarkę oraz wzmocnić jej siłę szyfrowania. Jeśli używasz przeglądarki Netscape Navigator więcej informacji na temat bezpieczeństwa i błędów w tym programie znajdziesz na stronie <http://home.netscape.com/security/index.html>.

4. Moja przeglądarka ma siłę szyfrowania 128 bitów, a strony nadal nie działają.

Tu będziesz już musiał sięgnąć do swojej pamięci. Czy na pewno nic nie zmieniałeś w ustawieniach sposobów transmisji i szyfrowania? Jeśli tak - zobaczmy co da się naprawić.

Instrukcja dla przeglądarki Internet Explorer:

Wejść w 'Narzędzia' > 'Opcje Internetowe'. W nowym oknie wybierz zakładkę 'Zabezpieczenia'.

Sprawdź jaki poziom zabezpieczeń jest ustawiony dla stref:

- Internet
- Zaufane witryny

Witryny z ograniczeniami

W przypadku ostatniej strefy sprawdź czy nie umieściłeś w spisie tychże witryn strony, do której próbujesz się dostać.

Zalecany poziom bezpieczeństwa dla stron ze strefy 'Internet' to 'Średni'. Dodawanie stron oraz modyfikacje poziomów bezpieczeństwa dla pozostałych stref zalecamy tylko zaawansowanym użytkownikom.

Przechodzimy do zakładki 'Zaawansowane' w okienku ustawień schodzimy na dół do działu 'Zabezpieczenia'.

Pozycje, które nas interesują to:

- Użyj Fortezza
- Użyj PCT 1.0
- Użyj SSL 2.0
- Użyj SSL 3.0
- Użyj TLS 1.0

Przynajmniej dwie z nich - SSL 2.0 i SSL 3.0 jako najpowszechniej używane sposoby bezpiecznej transmisji powinny być zaznaczone. Dodatkowo możemy zaznaczyć pozostałe, uruchomić ponownie przeglądarkę i jeszcze raz sprawdzić stronę WWW.

Instrukcja dla przeglądarki Netscape Navigator.

W menu 'Communicator' > 'Tools' wchodzimy w 'Security Info'
[Skrót klawiszowy CTRL+SHIFT+I].

Wybieramy 'Navigator' i sprawdzamy 'Advanced Security (SSL) Configuration'.

Oba sposoby transmisji powinny być włączone.

W 'Configuration SSL v2' i 'Configuration SSL v3' sprawdzamy czy wszystkie poziomy szyfrowania są włączone. Jeśli nie, zaznaczamy je. Wszelkie manipulacje związane z konfiguracją SSL zalecamy jedynie zaawansowanym użytkownikom.

5. O co chodzi z tymi wszystkimi SSL'ami, poziomami bezpieczeństwa i tak dalej?

Skrót SSL oznacza Secure Socket Layer, jest protokołem bezpiecznej transmisji opracowanym przez firmę Netscape. Za jego pomocą Twoja przeglądarka ustala z serwerem jakim systemem mają być zaszyfrowane dane. Poziomy bezpieczeństwa pozwalają Ci na większą kontrolę nad przeglądarką. Obecnie przeglądarka nie służy tylko do oglądania stron WWW, ale może być pełnoprawnym programem z dostępem do plików oraz innych programów w Twoim systemie. Ustawiając odpowiednio niskie poziomy bezpieczeństwa możesz narazić swój komputer na atak ze strony wirusów lub utracić istotne dane. Bardzo wysoki poziom zabezpieczeń z drugiej strony uniemożliwia Ci korzystanie ze stron, które wymagają od Ciebie podania danych jednoznacznie identyfikujących Twój komputer. Takich jak na przykład strony bankowe.

6. Moja przeglądarka jest dobrze skonfigurowana, ale nadal nie mogę się zalogować. Co dalej?

Sprawdź jaki typ adresu IP posiadasz. Aby to wykonać w systemie Windows kliknij na 'Start', następnie 'Uruchom' i wywołaj program WINIPCFG. Jeśli masz więcej kart sieciowych lub jeśli masz modem telefoniczny wybierz z listy kartę używaną do łączenia się poprzez sieć ASTER. Jeśli w polu adres IP znajduje się numer zaczynający od liczby 10 to znaczy, że masz numer z klasy prywatnej. Jeśli adres IP zaczyna się od liczby 212 to jesteś posiadaczem numeru IP z klasy publicznej.

7. Typu adresów IP- klasa publiczna i prywatna.

Adresy IP z klasy prywatnej zaczynają się od liczb:

- 10.
- 172.16. do 172.31.
- 192.168.

Adresy te określane są często jako prywatne, to znaczy komputery z takimi adresami IP nie są widoczne spoza sieci wewnętrznej. Dostęp do innych sieci a także komunikacja pomiędzy sieciami odbywa się dzięki specjalnym serwerom maskującym. To one przekazują dane z sieci lokalnej do internetu, a otrzymane z internetu dane przekazują do komputerów, które o dane te wysyłały zapytanie. Stosowanie serwerów maskujących znacznie podwyższa poziom bezpieczeństwa komputerów w sieci lokalnej, jednakże dostęp do serwisów wymagających identyfikacji komputera może być znacznie utrudniony lub uniemożliwiony. W sieci ASTER istnieje możliwość wyboru adresu IP z klasy prywatnej lub publicznej. Przy wyborze tym kierować się należy swoim doświadczeniem - mniej zaawansowanym użytkownikom zalecamy bardziej bezpieczny adres z klasy prywatnej. Rodzaj klasy można zmienić w każdej chwili z poziomu systemu samodzielnej administracji [Wilga](#).

Jeśli masz problemy z samodzielną zmianą typu adresu IP skontaktuj się z pomocą techniczną pod numerem 4 114 114, lub wyślij e-mail na adres helpdesk@aster.pl.

8. Posiadam adres IP z klasy adresów prywatnych i chcę go zmienić. Co mam robić?

Istnieją trzy sposoby zmiany:

- zmiana adresu IP z poziomu systemu samodzielnej administracji [Wilga](#)
- zmiana wielkości maksymalnego pakietu [MTU]. Tą opcję polecamy tylko zaawansowanym użytkownikom
- zmiana poprzez skrypt automatycznej konfiguracji przeglądarki WWW

9. Czemu muszę cokolwiek zmieniać? Czemu tak się dzieje, co może być powodem?

Jednym z powodów może być kwestia 'dogadania' się Twojego komputera z serwerem banku lub bezpiecznego serwisu.

Jedną z wartości przekazywanych pomiędzy komputerami jest MTU - Maximum Transmission Unit, czyli maksymalna wartość wielkości pakietu jaką może przekazywać sieć. Twój komputer podłączony poprzez złącze Ethernet z modemem przyjmuje, że wielkość tego pakietu powinna wynosić standardowo 1500 bajtów. Przykładowo korzystanie z modemu telefonicznego, gwarantuje maksymalną wielkość pakietu do 576 bajtów.

Jednakże sieć kablowa działa nieco inaczej niż sieć lokalna i przesyłane pakiety zawierają jedynie 1476 bajtów.

Oznacza to, że każdy Twój pakiet trafiający do modemu o wielkości 1500 lub większej jest dzielony na dwie części - 1476 i reszta. Tak podzielony pakiet trafia do sieci operatora, który obsługuje bank, tam jest przekazywany do serwera który przyjmuje że wartość MTU 1500 jest wielkością, z którą należy wysyłać pakiety do Twojego komputera. Wysyła więc pakiet o wielkości 1500 bajtów, który trafiając na sieć kablową wraca z prośbą o zmniejszenie pakietu do 1476 bajtów. W przypadku komputerów z adresami IP z klasy publicznej serwery ustalają wielkość transmisji i jest ona kontynuowana. Problem zaczyna się przy adresach z klasy prywatnej. Komputer nie jest widziany w sieci internetu, a więc system zewnętrzny uznaje, że skoro komputer, który wysłał zapytanie nie jest tym samym, który wysłał prośbę o zmniejszenie pakietu, transmisje należy przerwać.

10. Co po zmianach adresu IP?

W przypadku zmiany adresu IP na adres z klasy publicznej serwer banku lub bezpiecznego serwisu jest w stanie połączyć się bezpośrednio z Twoim komputerem. Wielkość pakietu jest zmniejszana, a transmisja kontynuowana.

W przypadku zmiany MTU na 1476 lub mniej Twój komputer wysyła pakiety, których wielkości nie trzeba ustalać z innymi systemami.

W przypadku skorzystania ze skryptu automatycznej konfiguracji przeglądarki informacje z Twojego komputera są przekazywane do serwera bankowego poprzez nasz serwer proxy.

11. Bezpieczeństwo przesyłania danych.

Dane, po zmianach ustawień są równie bezpieczne jak przechodząc przez dowolny inny fragment sieci internet.

Ciekawostką może być fakt, że w ramach sieci ASTER cała transmisja odbywająca się od Twojego modemu aż do styku z internetem jest szyfrowana. Jesteśmy jedyną z niewielu sieci oferujących tego rodzaju poziom bezpieczeństwa. Twoje dane przechodzą przez serwer proxy zaszyfrowane i nie są nigdzie zapisywane w żadnym odcinku czasu. Więcej na temat bezpieczeństwa w sieci ASTER.

12. Konfiguracja przeglądarki.

Dla przeglądarki Internet Explorer standardowa konfiguracja powinna wyglądać następująco:

W menu 'Narzędzia' wybierz 'Opcje Internetowe'.

W nowym okienku kliknij w zakładce 'Połączenia' na 'Ustawienia sieci LAN' Zaznacz 'Użyj skryptu automatycznej konfiguracji' i wpisz w okienko **http://www.aster.pl/aster.pac**

Upewnij się że pola 'Automatycznie wykryj ustawienia' oraz 'Użyj serwera proxy' nie są zaznaczone i aktywne.

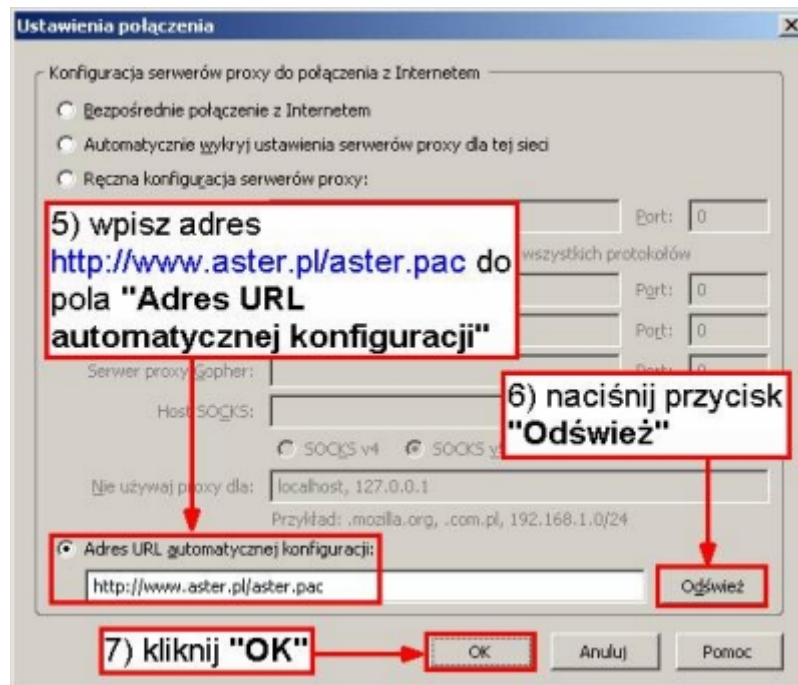
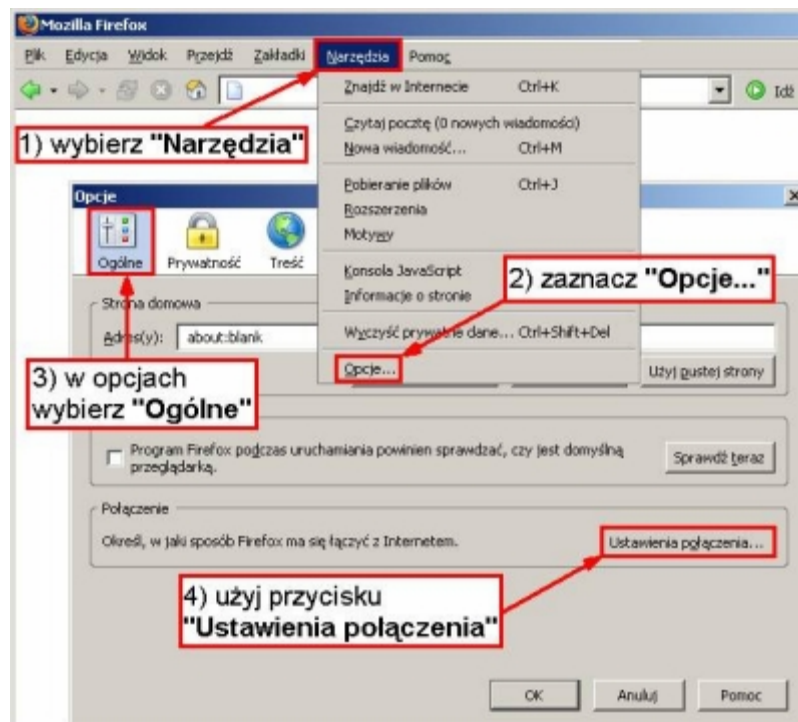
Potwierdzając 'OK.' zamknij wszystkie okna, zamknij wszystkie aktywne okna przeglądarki i uruchom ją ponownie.

W przeglądarce Netscape Navigator standardowa konfiguracja powinna wyglądać następująco:

W menu 'Edit' wybierz 'Preferences'.

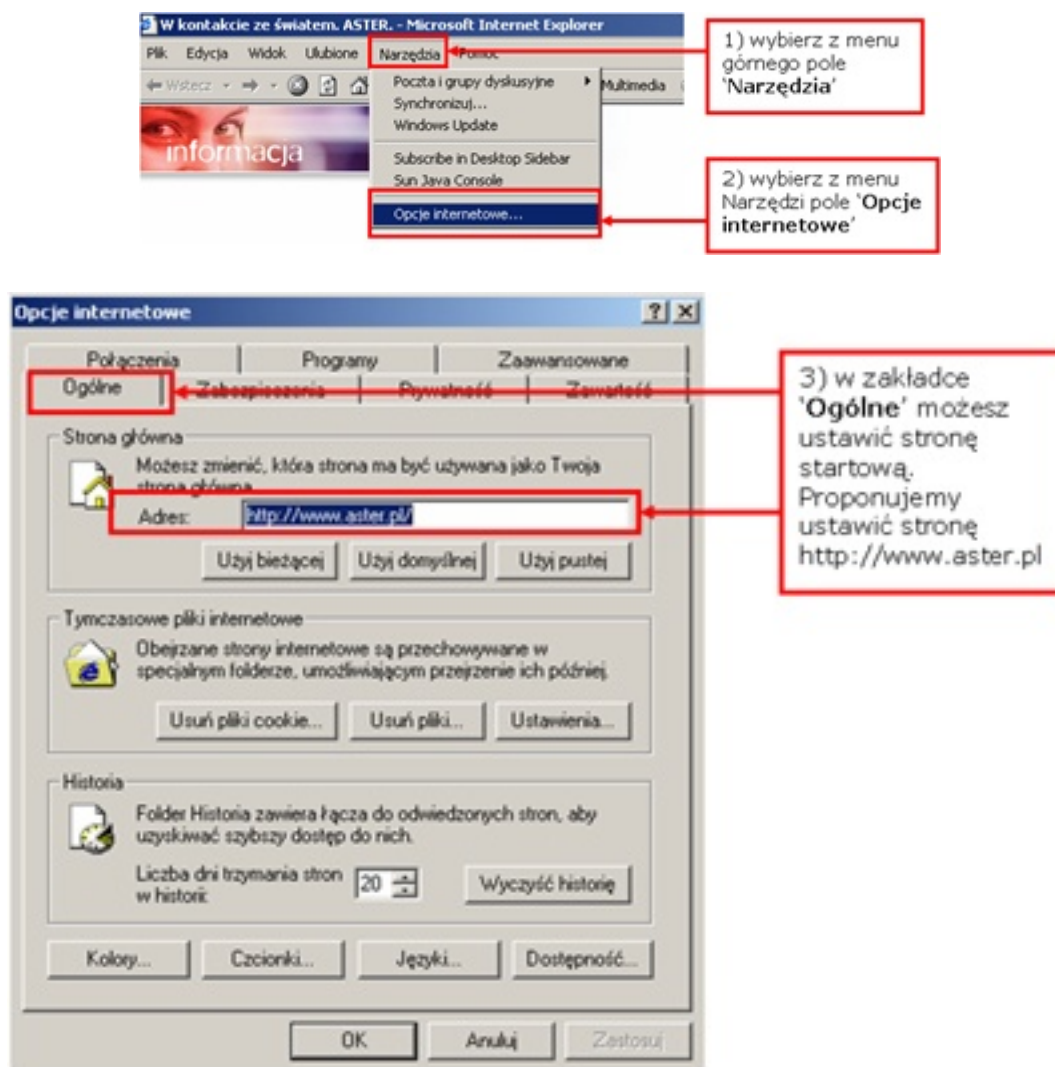
W nowym oknie rozwiń okienko 'Advanced' i wybierz pozycje 'Proxy'. Wybierz 'Automatic proxy configuration/Configuration location (URL)' i w okienku wpisz **http://www.aster.pl/aster.pac**. Kliknij 'Reload' i potwierdź klikając 'OK.'

Mozilla Firefox



Internet Explorer 5.0 i późniejsze

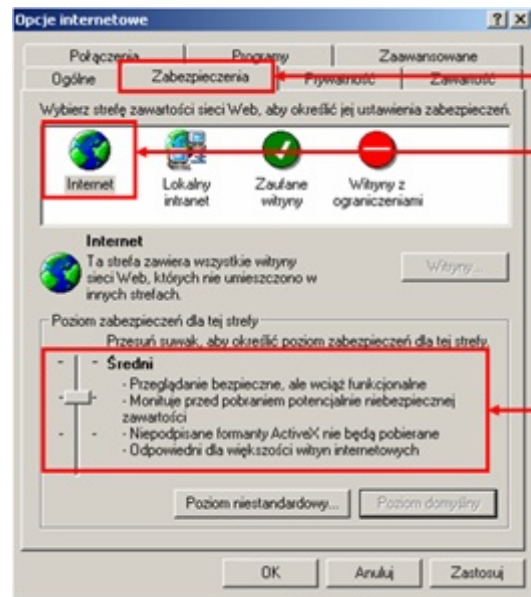
Jeśli chcesz skonfigurować przeglądarkę Internet Explorer 5 lub późniejszą to:



1) wybierz z menu górnego pole 'Narzędzia'

2) wybierz z menu Narzędzi pole 'Opcje internetowe'

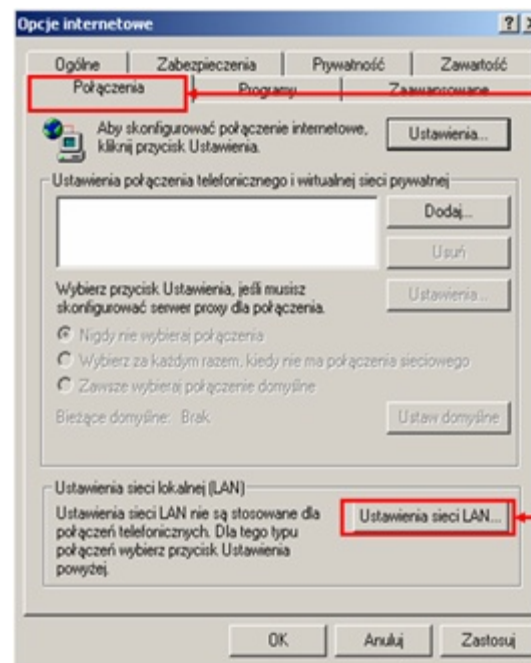
3) w zakładce 'Ogólne' możesz ustawić stronę startową. Proponujemy ustawić stronę <http://www.aster.pl>



4) wybierz zakładkę 'Zabezpieczenia'

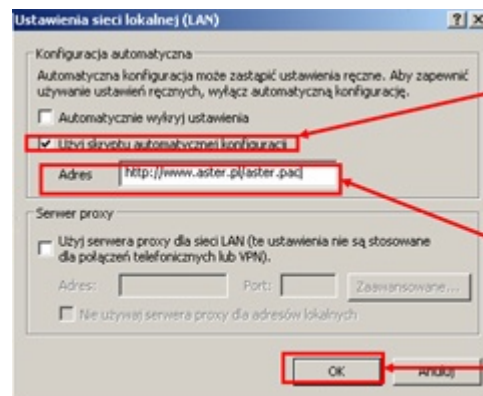
5) wybierz ikonę 'Internet'

6) ustaw poziom bezpieczeństwa na 'Średni'.
Uwaga: ustawienie poziomu bezpieczeństwa na wysoki może być podstawową przyczyną nie działania niektórych serwisów internetowych



7) Wybierz zakładkę 'Połączenia'

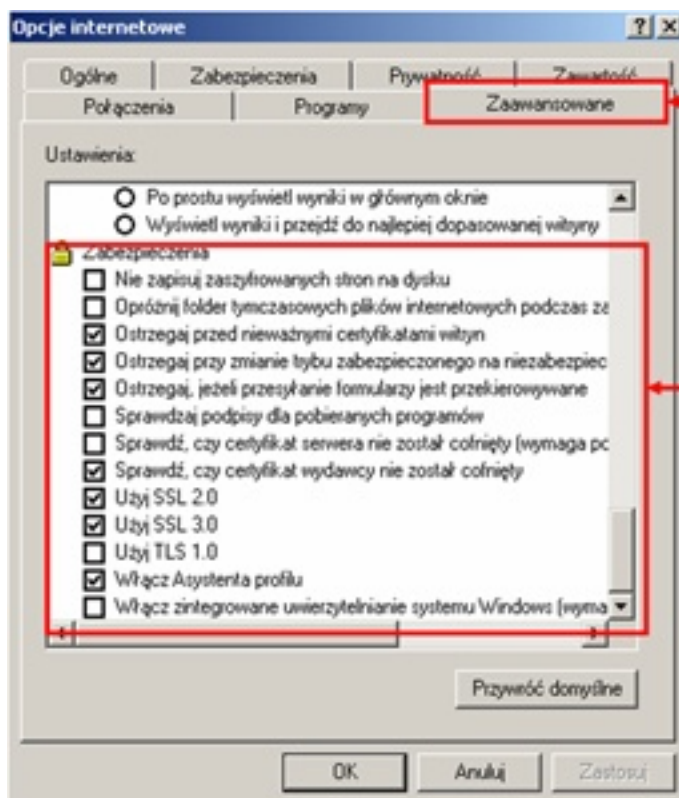
8) Kliknij na pole 'Ustawienia sieci LAN'



9) zaznacz pole 'Użyj skryptu automatycznej konfiguracji'

10) w polu 'Adres' wpisz: 'http://www.aster.pl/aster.pac'

11) potwierdź ustawienia klikając 'OK'

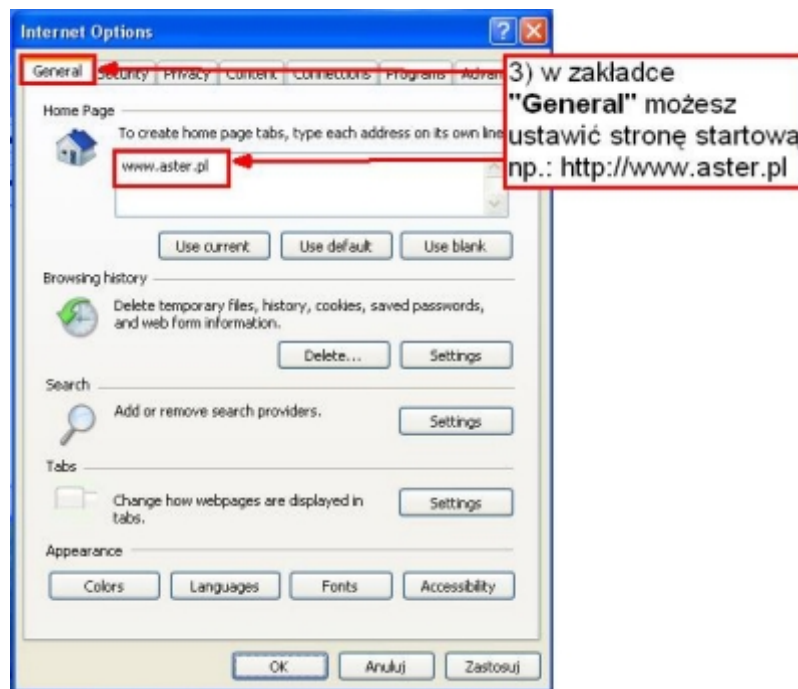
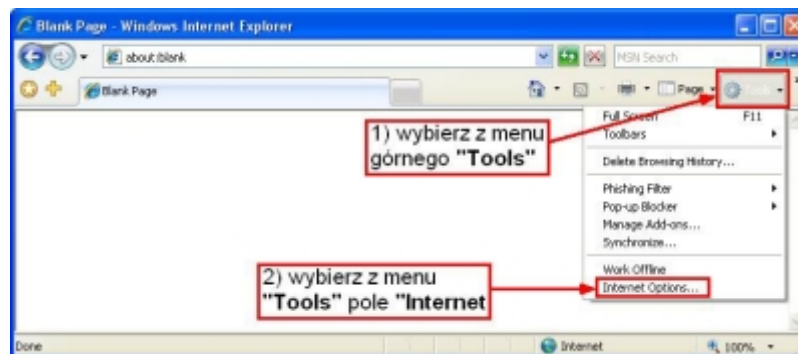


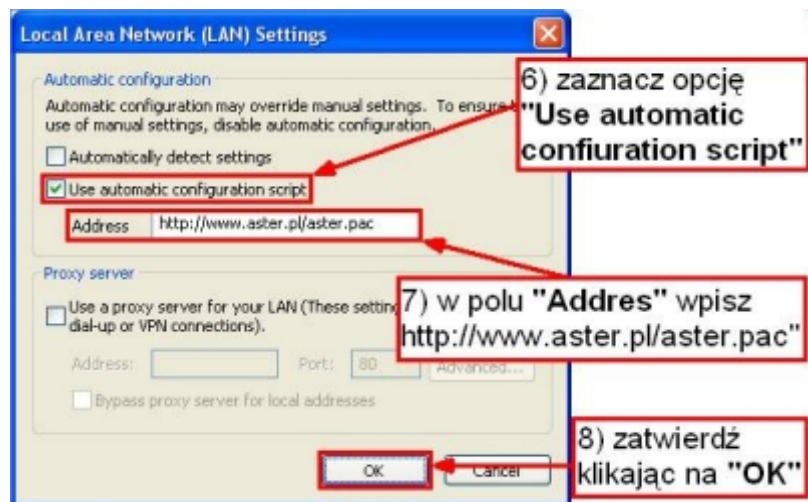
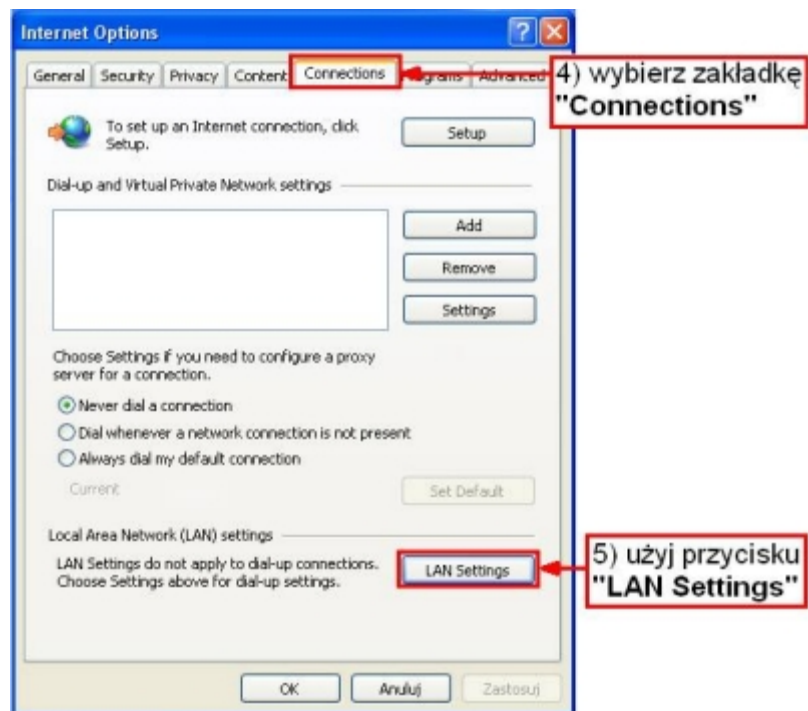
12) wybierz zakładkę 'Zaawansowane'

13) ustaw opcje związane z zabezpieczeniami podobnie jak na rysunku.

Uwaga: wyłączenie zbyt wielu opcji zabezpieczeń może uniemożliwić korzystanie z niektórych serwisów internetowych

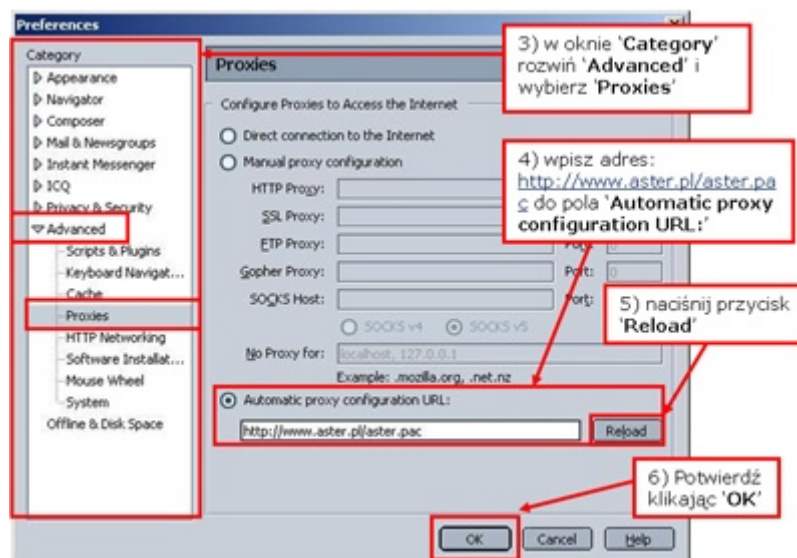
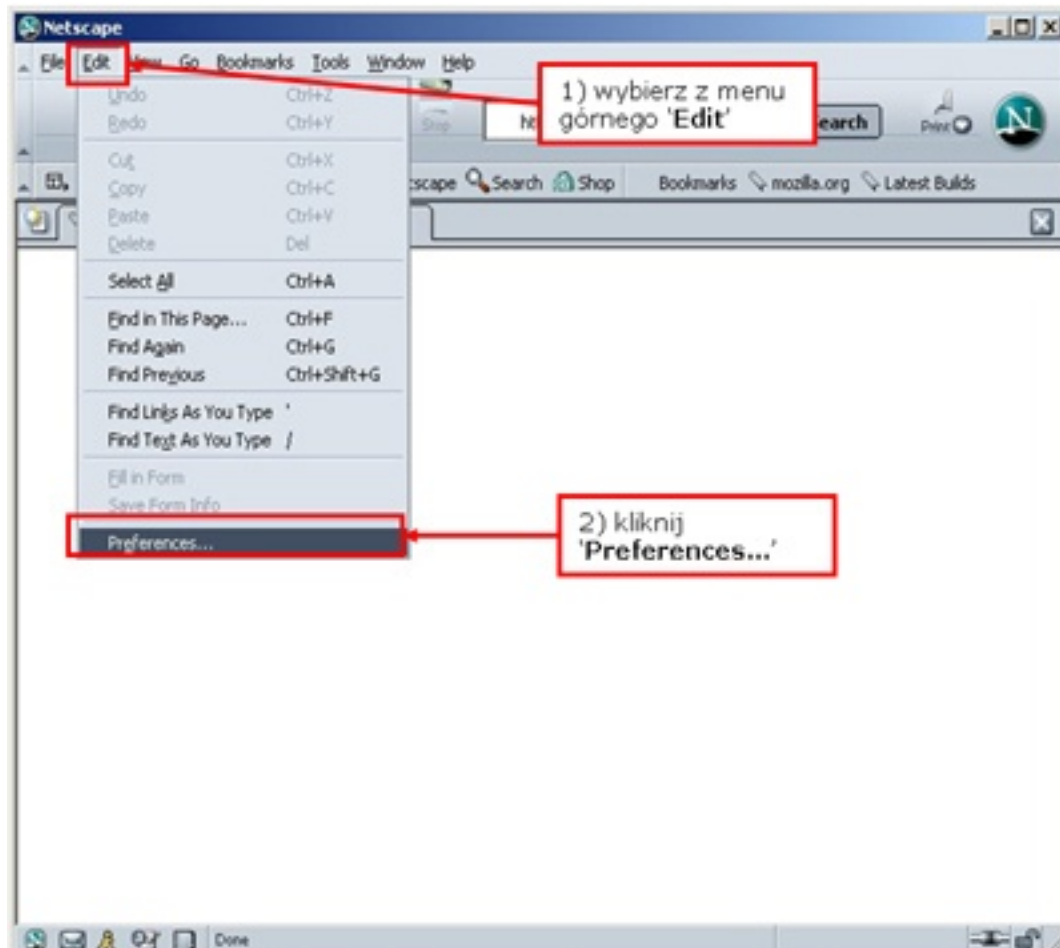
Internet Explorer 7



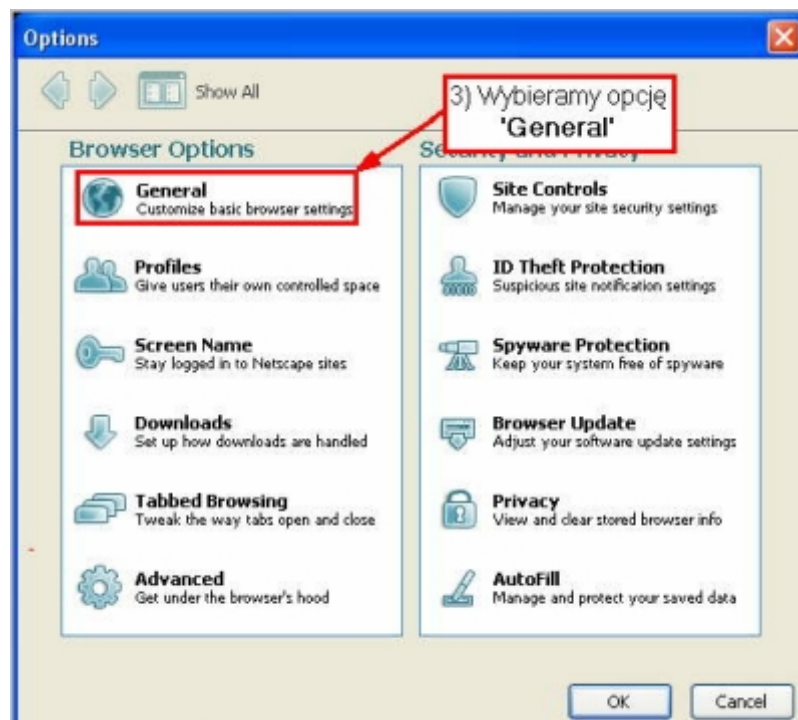
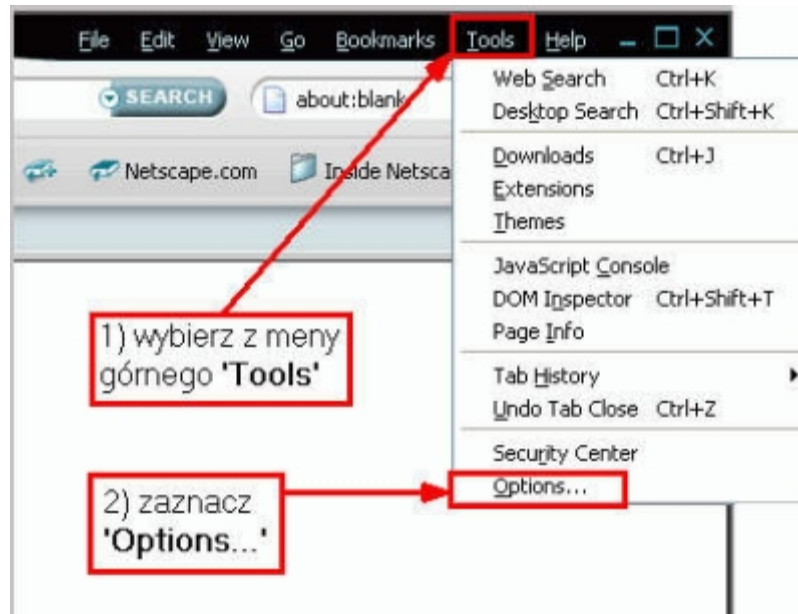


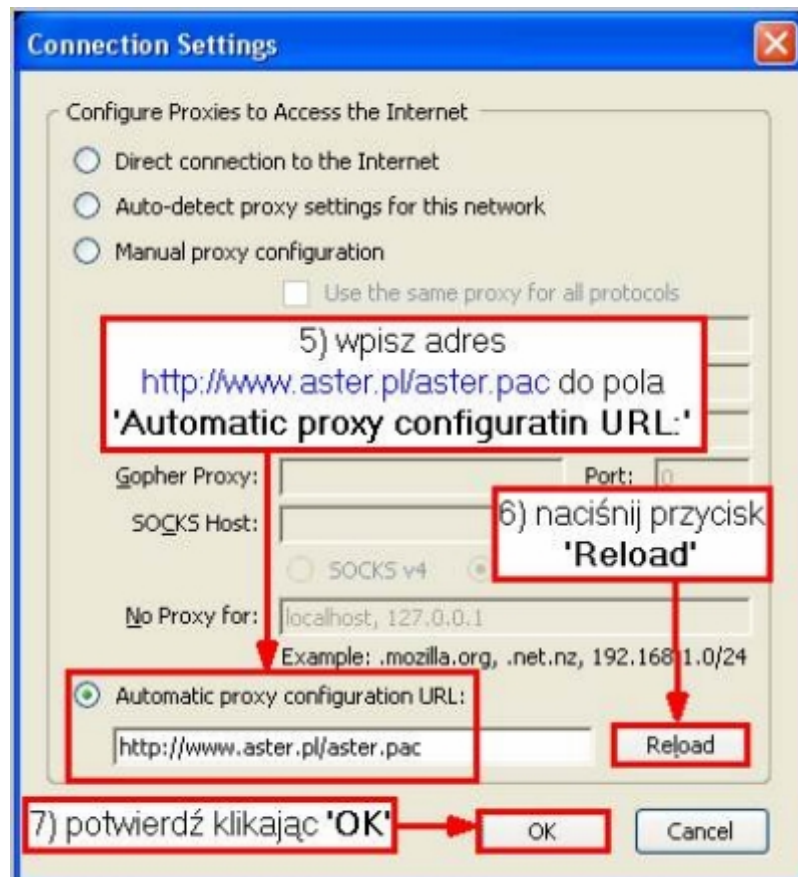
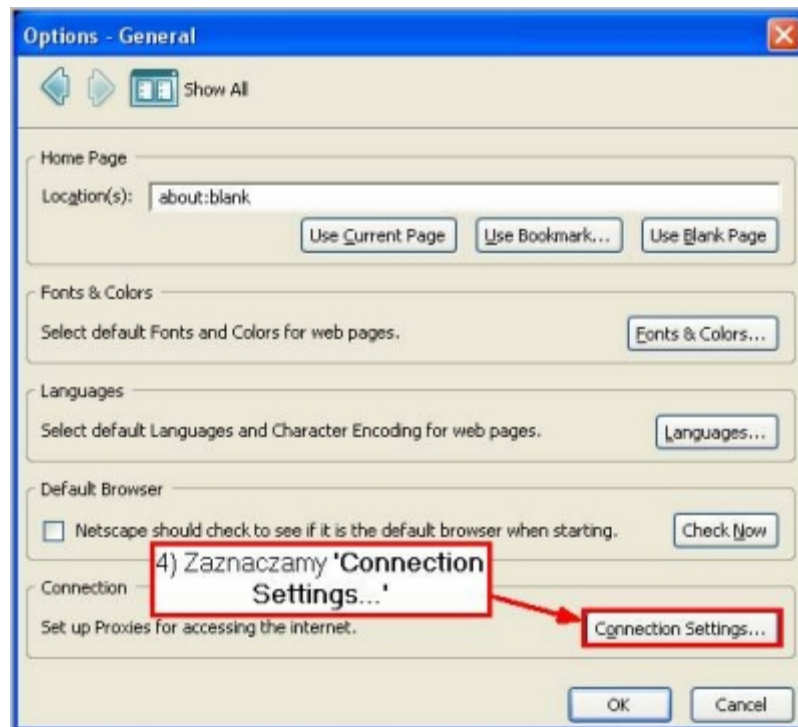
Netscape 7.1 [eng]

Jeśli chcesz skonfigurować Netscape 7.1 [eng] to:



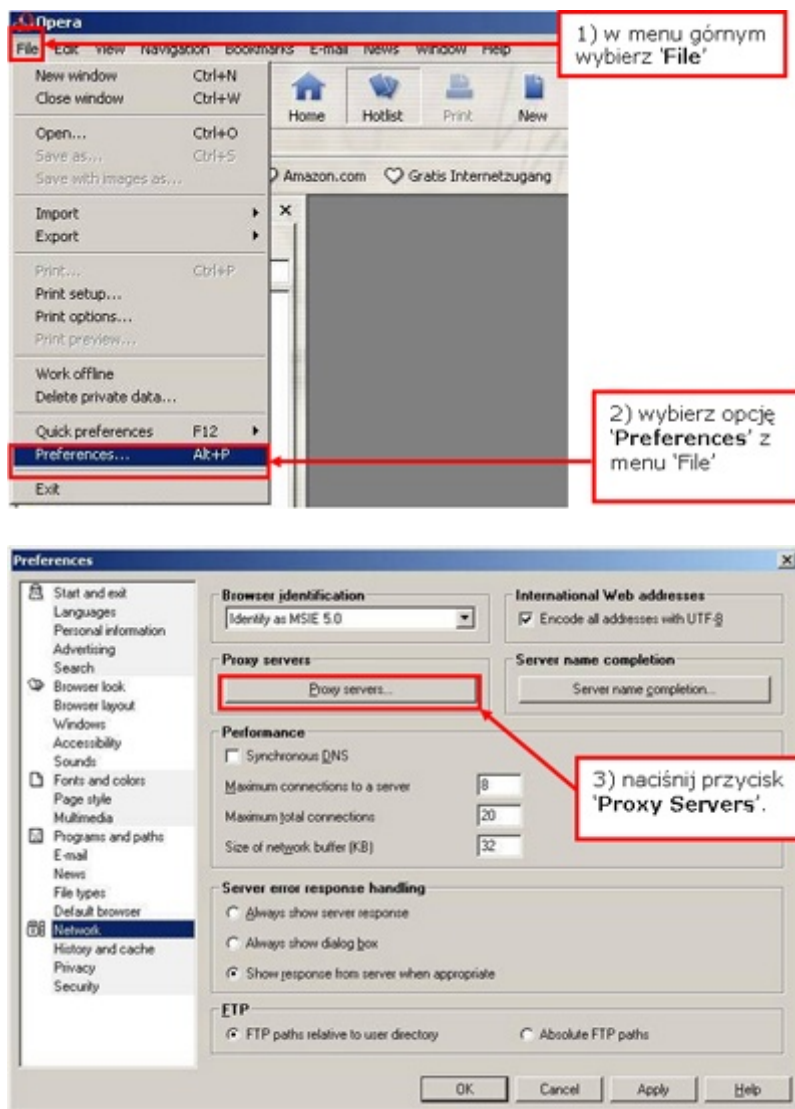
Netscape 8

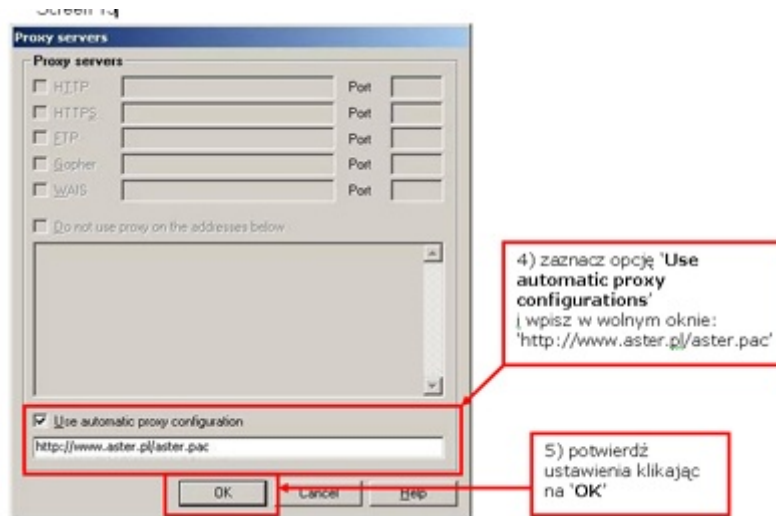




Opera 6.05 [eng]

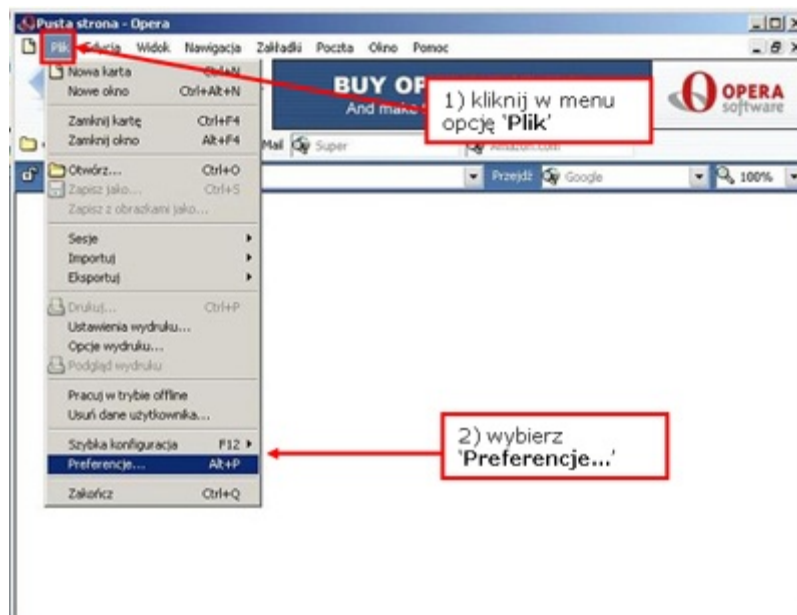
Jeśli chcesz skonfigurować Opera 6.05 to:

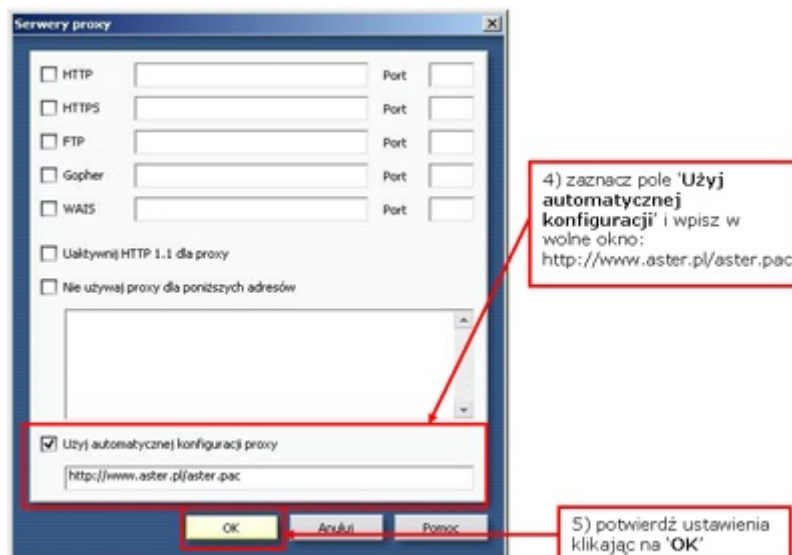
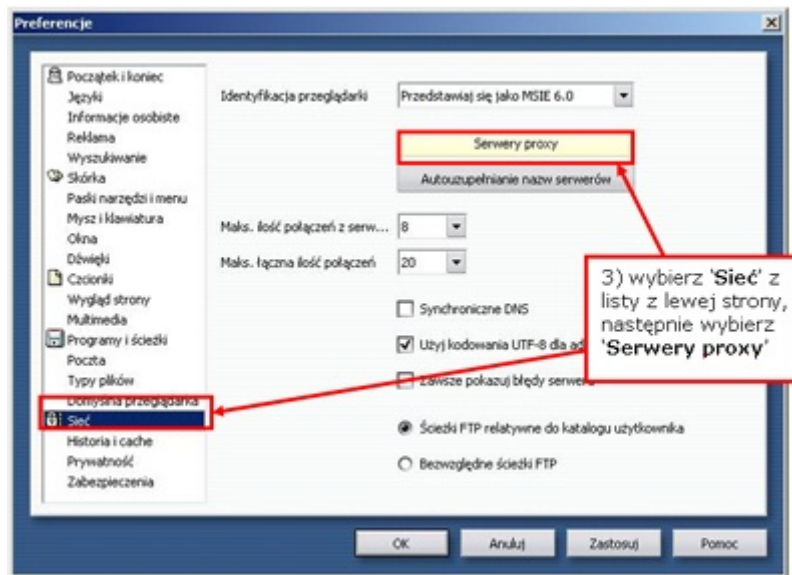




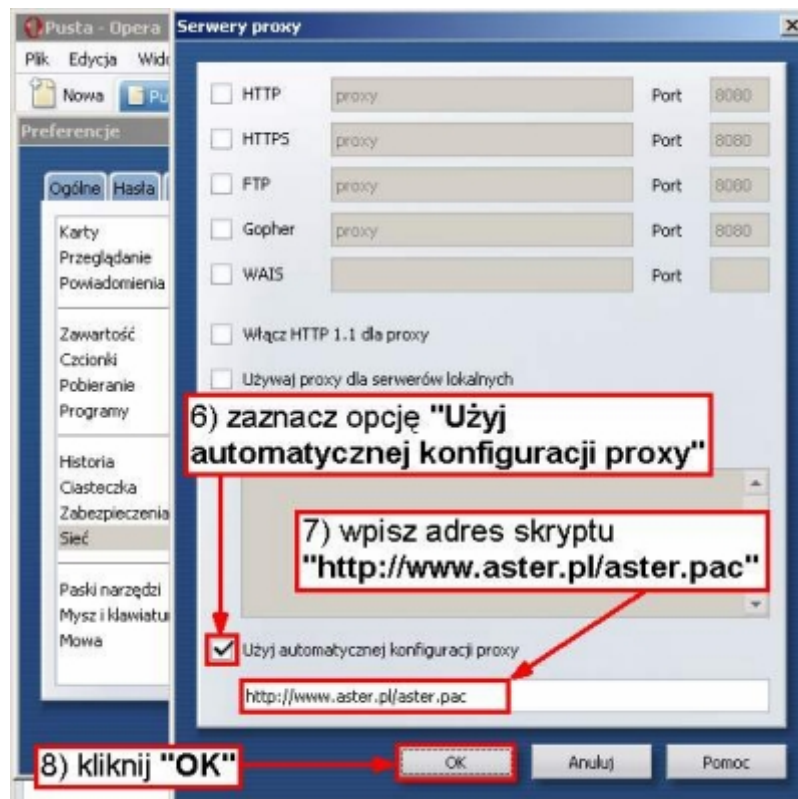
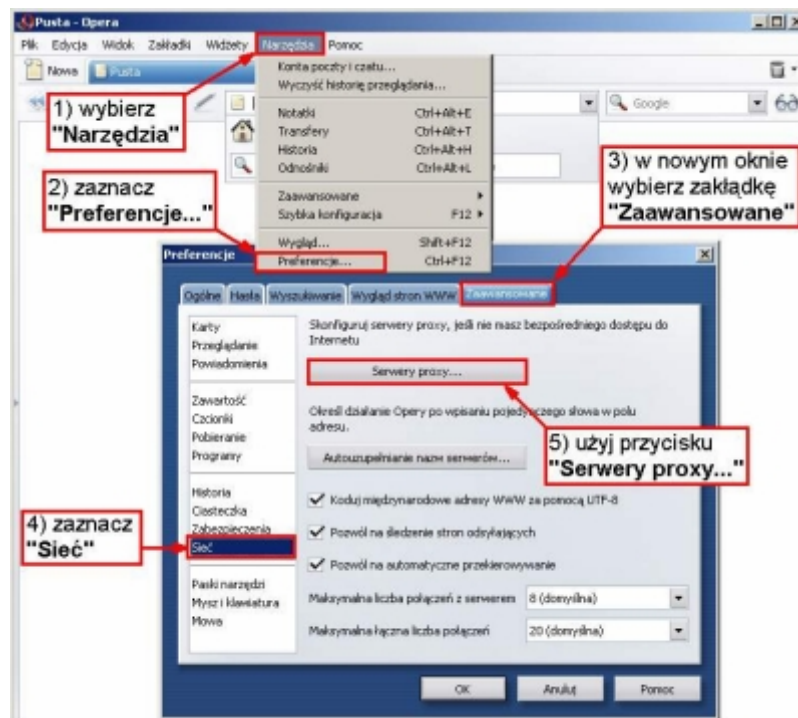
Opera 7.2 [pl]

Jeśli chcesz skonfigurować Opera wersję 7.2 to:





Opera 8 i 9



Sylaba Communicator 4.7

Jeśli chcesz skonfigurować Sylaba Communicator 4.7 to:

