

## Wymagane uprawnienia

Aplet Java zażąda uprawnień wyświetlonych w oknie dialogowym **Ostrzeżenie o zabezpieczeniach**. Aplet Java może wymagać do swojego działania dostępu do pliku i innych zasobów komputera. Każda z czynności wymaga konkretnych uprawnień. Administrator sieci mógł już zdecydować, które uprawnienie są dozwolone. Dla dozwolonych uprawnień mógł on też określić, czy użytkownik powinien być powiadamiany, gdy pojawia się ich żądanie. W przeciwnym przypadku powiadomienia pojawiają się jedynie wtedy, gdy aplet Java wymaga większych uprawnień niż te, które są dozwolone automatycznie.

Mając informacje o wydawcy oprogramowania oraz uprawnieniach wymaganych przez program, musisz zdecydować, czy zainstalować i uruchomić ten aplet Java. Jeżeli nie masz pewności, kliknij przycisk **OK** w oknie dialogowym **Alarm zabezpieczeń**, a następnie kliknij przycisk **Nie** w oknie dialogowym **Ostrzeżenie o zabezpieczeniach**.

Więcej informacji na temat następujących uprawnień możesz znaleźć klikając je:

[Drukowanie](#)

[Interfejs użytkownika](#)

[Multimedia](#)

[Niestandardowe](#)

[Operacje I/O na plikach](#)

[Operacje I/O sieci](#)

[Operacje I/O użytkownika na plikach](#)

[Refleksja](#)

[Rejestr](#)

[Schowek klienta](#)

[Wtyki](#)

[Właściwości systemu](#)

[Właściwości](#)

[Wykonywanie](#)

[Zabezpieczenia](#)

Informacje na temat wyświetlania uprawnień na swoim komputerze możesz znaleźć w Tematach pokrewnych.

---

{button ,AL("A\_IDH\_SEC\_ALERT\_VIEW\_JAVA\_CUSTOM\_SETTINGS")}[Tematy pokrewne](#)

Wyświetla typ dostępu, który oglądasz lub modyfikujesz. Możesz kliknąć typ dostępu, a następnie określić ustawienia dla tego typu dostępu.

Miejsce na wpisanie nazwy pliku, który chcesz dodać do listy plików o dozwolonym konkretnym typie dostępu. Możesz wpisać nazwy plików lub użyć symboli wieloznacznych, takich jak \*.exe.

Przedstawia listę plików, którym jest przyznany określony typ dostępu do nich.

Dodaje element do listy w celu uwzględnienia uprawnień.

Usuwa zaznaczony element z listy.

Miejsce na wpisanie nazwy pliku do wykluczenia z listy plików, którym przyznany jest określony typ dostępu do nich.

Przedstawia listę nazw plików, którym nie jest przyznany określony typ dostępu do nich.



Określa, czy będzie przyznany dostęp do bazy URL plików kodu.

Wyczwietla typ wyczwietlanego lub modyfikowanego dostêpu.

Miejsce na podanie wpisu rejestru do dodania do listy wpisów rejestru, którym jest przyznany określony dostęp do nich.

Przedstawia listę wpisów rejestru, którym przydzielono określony dostęp do nich.

Miejsce na podanie wpisu rejestru do wykluczenia z listy wpisów rejestru, którym przyznany jest określony typ dostępu do nich.

Przedstawia listę wpisów rejestru, którym nie chcesz przyznawać określonego dostępu do nich.

Określa, czy pozwalać apletom Java tworzyć okna dialogowe.

Określa, czy pozwalać apletom Java tworzyć okna najwyższego poziomu.



Określa, czy wyświetlać ostrzeżenie, gdy aplet Java żąda utworzenia okna najwyższego poziomu.

Określa, czy pozwalać apletom Java używać schowka do wycinania, kopiowania i wklejania informacji.

Określa pozwolenie dla apletów Java na uzyskanie nieograniczonego dostępu do właściwości systemu.

Zezwala na dostęp do określonych przez użytkownika właściwości systemu i sufiksów oraz zabrania dostępu do wykluczonych właściwości systemu.

Miejsce na wpisanie sufiksów, do których mają dostęp aplety Java.

Miejsce na wpisanie właściwości systemu, do których mają dostęp aplety Java.

Miejsce na wpisanie właściwości systemu, do których aplety Java nie powinny mieć dostępu.

Określa, czy zezwalać na typ 3adowania skojarzony z tym obiektem publicznego uprawnienia.



Określa, czy zezwalać na typ ³adowania odwo³uj¹cy siê do dowolnego innego typu ³adowania innego od tego skojarzonego z tym obiektem publicznego uprawnienia.

Określa, czy zezwalać na typowanie odwołujący się do klas systemu publicznego.

Określa, czy zezwalać na typ ³adowania skojarzony z tym obiektem uprawnienia.

Określa, czy zezwala na typ 3adowania odwołujący się do dowolnego innego typu 3adowania innego od tego skojarzonego z tym obiektem uprawnienia.

Określa, czy zezwalać na typowanie odwodzący się do zadeklarowanych klas systemowych.

Określa, czy zezwalać apletom Java na czytanie plików, jeżeli użytkownik na to pozwala.

Określa, czy zezwalać apletom Java na zapisywanie w plikach, jeżeli użytkownik na to pozwala.

Określa, ile miejsca na komputerze użytkownika mogą używać aplety Java.



Określa, czy zezwalać apletom Java na ignorowanie podanych przez użytkownika ograniczeń ilości miejsca na wszystkie pliki internetowe.

Określa, czy można tworzyć pliki wędrujące. Pliki wędrujące są tworzone w profilu użytkownika i są obecne na każdym komputerze, do którego użytkownik jest zalogowany.

Określa, czy można uruchamiać aplikacje podane w polu **Pozwalaj na wykonywanie**.

Określ, które programy można uruchamiać.

Określ, których programów nie można uruchamiać.

Określa, czy zezwalać na nieograniczony dostęp do w1tku.

Określa, czy zezwalać na nieograniczony dostęp do grupy wątków.

Określa, czy obiekt uprawnień pozwala na wys³anie strumienia System.in.



Określa, czy obiekt uprawnień pozwala na ustawienie strumienia System.out.

Określa, czy obiekt uprawnień pozwala na ustawienie strumienia System.err.

Okreœla, czy klasy, które maj¹ uprawnienie `PrintingPermission` bêd¹ mog³y korzystaæ z us³ug drukowania.

Określa, czy zezwalać na dostęp do rozszerzonych aspektów interfejsu API Microsoft DirectX.

Określa, czy zezwalać na dostęp do klas zabezpieczeń JDK, `java.lang.security`.

Wyświetla typ wyświetlanej lub modyfikowanej komunikacji. Następująca tabela pokazuje typy komunikacji i ustawienia dostępne dla nich.

***Aby określić ustawienia dla typu komunikacji***

Ogólna komunikacja z określonymi hostami

Połączenie za pomocą podanych interfejsów i portów

Łączenie podanych grup multiemisji

Ustawienia zastępujące indywidualne reguły portów

***Kliknij***

Adresy połączenia

Adresy wiązania

Adresy multiemisji

Porty globalne

Miejsce na wpisanie hosta i portu dodawanego do listy hostów i portów, które mają<sup>1</sup> zezwolenie na określone<sup>1</sup> komunikacje z nimi.

Przedstawia listę hostów i portów, które mają zezwolenie na określonej komunikacji z nimi.



Miejsce na wpisanie hosta i portu wykluczanego z listy hostów i portów, które mają<sup>1</sup> zezwolenie na określone<sup>1</sup> komunikacje z nimi.

Przedstawia listę hostów i portów, które nie mają<sup>1</sup> zezwolenia na określonej<sup>1</sup> komunikacji z nimi.

Określa, czy chcesz po<sup>31</sup>czyć się z plikowym adresem URL.

Określa, czy chcesz po<sup>31</sup>czyć się z nieplikowym adresem URL.

Miejsce na wpisanie nazwy i danych uprawnień, które chcesz dodać do listy niestandardowych ustawień uprawnień.

Przedstawia listę nazw i danych dodawanych niestandardowych ustawień uprawnień.

Kliknij, aby ustawić poziom zabezpieczeń na Wysokie (najbezpieczniejsze).

Kliknij, aby ustawić poziom zabezpieczeń na Średnie.



## Wyświetlanie niestandardowych ustawień Java

Uprawnienia są ustawiane przez administratora sieci za pomocą pakietu Internet Explorer Administration Kit. Zazwyczaj nie można edytować tych ustawień, ale można je wyświetlić. Można to zrobić, wykonując następującą procedurę.

- 1 Kliknij prawym przyciskiem myszy ikonę **Internet** na pulpicie, a następnie kliknij przycisk **Właściwości**.
- 2 Kliknij kartę **Zabezpieczenia**, a następnie kliknij przycisk **Niestandardowe**.
- 3 Na liście **Ustawienia** w obszarze **Java** kliknij pozycję **Niestandardowe**.
- 4 Kliknij przycisk **Niestandardowe ustawienia języka Java** u dołu okna dialogowego.

### Uwagi

- Jeżeli u dołu okna dialogowego ustawień języka Java pojawia się przycisk **Edytuj**, możesz zmieniać te ustawienia.
- Jeżeli u dołu okna dialogowego ustawień języka Java nie pojawia się przycisk **Edytuj**, skontaktuj się z administratorem sieci.

---

{button ,AL("A\_IDH\_SEC\_ALERT\_MORE\_INFO")} [Tematy pokrewne](#)

Zamyka okno dialogowe i zapisuje wprowadzone zmiany.

Zamyka okno dialogowe bez zapisywania wprowadzonych zmian.

### Edytor stref - okno dialogowe

W tej strefie można przypisywać uprawnienia Nie podpisany, Dozwolony, Kwestionowany/Odmowa. Uprawnienie, które nie ma przypisanej wartości Nie podpisany lub Dozwolony ma przypisaną wartość Kwestionowany/Odmowa,

Przy uprawnieniach Kwestionowany/Odmowa można przypisać konkretne uprawnienia jako Kwestionowany. Wszystkie pozostałe uprawnienia będą przypisane jako Odmowa. Alternatywnie, można przypisać konkretne uprawnienia jako Odmowa, a wszystkie pozostałe uprawnienia będą przypisane jako Kwestionowany.

Jeżeli chcesz automatycznie nadawać wszystkie uprawnienia bez otwierania odpowiedniego okna dialogowego i włączania wszystkich uprawnień, możesz wybrać opcję **Zezwalaj na pełny zestaw uprawnień**.

## Ustawienia niestandardowe - okno dialogowe

W tym oknie dialogowym wyświetlane są uprawnienia Java nadane przez administratora sieci.

Aplet Java może wymagać do swojego działania dostępu do pliku i innych zasobów komputera. Każda z czynności wymaga konkretnych uprawnień, aby mogła być wykonana. Administrator sieci mógł już zdecydować, które uprawnienie są dozwolone. Dla dozwolonych uprawnień mógł też określać, czy użytkownik powinien być powiadamiany, gdy pojawia się ich użycie. W przeciwnym przypadku powiadomienia pojawiają się jedynie wtedy, gdy aplet Java wymaga większych uprawnień od dozwolonych automatycznie.

Każda z następujących kart reprezentuje typ zestawu uprawnień:

### **Karta**

### **Uprawnienia**

#### **Niepodpisany**

Są nadawane nie podpisanej pobranej zawartości.

#### **Dozwolony**

Nie wymaga potwierdzenia przez użytkownika.

**Kwestionowany/Odmowa** Wymaga potwierdzenia przez użytkownika lub są absolutnie zakazane.

Następujące uprawnienia mogą być przypisane tym kartom:

Drukowanie

Interfejs użytkownika

Multimedia

Niestandardowe

Operacje I/O na plikach

Operacje I/O sieci

Operacje I/O użytkownika na plikach

Refleksja

Rejestr

Schowek użytkownika

Wzrostki

Właściwości systemu

Właściwości

Wykonywanie

Zabezpieczenia

### **Operacje I/O na plikach**

Ta karta s³u¿y do okreœlania plików i typów plików, którym zezwalasz na zestaw uprawnień tej strefy. Domyœlnie wszystkie pliki s¹ wykluczone, wiêc nie trzeba okreœlaæ plików do wykluczenia, o ile nie stanowi¹ one podzbioru uwzglêdnionych plików. Na przyk³ad, jeœli uwzglêdniasz typ pliku (\*.avi), mo¿esz wykluczyæ konkretny plik tego typu (MojPlik.avi). Mo¿esz okreœlaæ ró¿ne uprawnienia dla ró¿nych typów dostêpu: Odczyt, Zapis i Usuwanie.

### **Uwaga**

Dla ka¿dego ustawienia w tym oknie dialogowym jest dostêpna Pomoc. Wybierz lub kliknij przycisk, o którym chcesz uzyskaæ informacje, a nastêpnie naciœnij klawisz F1.

## **Rejestr - karta**

Ta karta s³u¿y do okreœlania wpisów rejestru, którym zezwalasz na zestaw uprawnieñ tej strefy. Domyœlnie wszystkie wpisy rejestru s¹ wykluczone, wiêc nie trzeba okreœlaæ wpisów do wykluczenia, o ile nie stanowi¹ one podzbioru uwzglêdnionych wpisów. Na przyk³ad, jeœli uwzglêdniasz wpis HKEY\_CURRENT\_USER, mo¿esz wykluczyæ konkretn¹ kategoriê tego wpisu (HKEY\_CURRENT\_USER\NETWORK). Mo¿esz okreœlaæ ró¿ne uprawnienia dla ró¿nych typów dostêpu: Odczyt, Zapis i Usuwanie.

## **Uwaga**

Dla ka¿dego ustawienia w tym oknie dialogowym jest dostêpna Pomoc. Wybierz lub kliknij przycisk, o którym chcesz uzyskaæ informacje, a nastêpnie naciœnij klawisz F1.

### Interfejs użytkownika - karta

Karta ta s³u¿y do okreœlania uprawnieñ dla niektórych bardziej widocznych czynnoœci, których mo¿e za¿¹daæ aplet Java na komputerze u¿ytkownika, takich jak tworzenie okna lub okna dialogowego, dostêp do w³œciwoœci systemu (na przyk³ad plików .ini) lub sprawdzania informacji w celu okreœlenia ich struktury, aby aplet móg³ pobraæ informacje. Uprawnienia te mog¹ byæ umieszczone na liœcie Ustawieñ niestandardowych Java lub w oknie dialogowym **Ostrze¿enie o zabezpieczeniach**, gdy aplet Java ¿¹da uprawnieñ, które wykraczaj¹ poza uprawnienia nadawane automatycznie.

### Uwaga

Dla ka¿dego ustawienia w tym oknie dialogowym jest dostêpna Pomoc. Wybierz lub kliknij przycisk, o którym chcesz uzyskaæ informacje, a nastêpnie naciœnij klawisz F1.



### Różne - karta

Karta ta s³u¿y do okreœlania uprawnieŃ do odczytu, zapisu i przechowywania plików, uruchamiania programów, prowadzenia w³tków oraz innych. Uprawnienia te mog¹ byæ umieszczone na liœcie UstawieŃ niestandardowych Java lub w oknie dialogowym **Ostrze¿enie o zabezpieczeniach**, gdy aplet Java ¿¹da uprawnieŃ, które wykraczaj¹ poza uprawnienia nadawane automatycznie.

### Uwaga

Dla ka¿dego ustawienia w tym oknie dialogowym jest dostêpna Pomoc. Wybierz lub kliknij przycisk, o którym chcesz uzyskaæ informacje, a nastêpnie naciœnij klawisz F1.

### **Operacje I/O w sieci - karta**

Karta ta s³u¿y do okreœlania typów dozwolonych po³¹czeñ oraz hostów i portów. Domyœlnie wszystkie hosty i porty s¹ wykluczone, wiêc nie ma potrzeby okreœlania hostów ani portów do wykluczenia, o ile nie s¹ one podzbiorem uwzglêdnionych hostów i portów. Mo¿esz okreœlaæ ró¿ne uprawnienia dla ró¿nych typów po³¹czeñ: Adresy po³¹czenia, Adresy wi¹zania, Adresy multiemisji i Porty globalne.

### **Uwaga**

Dla ka¿dego ustawienia w tym oknie dialogowym jest dostêpna Pomoc. Wybierz lub kliknij przycisk, o którym chcesz uzyskaæ informacje, a nastêpnie naciœnij klawisz F1.

### **Niestandardowe - karta**

Karta ta s³u¿y do okreœlania ustawieñ W³œciwoœci niestandardowych wed³ug nazw lub typów danych.

### **Uwaga**

Dla ka¿dego ustawienia w tym oknie dialogowym jest dostêpna Pomoc. Wybierz lub kliknij przycisk, o którym chcesz uzyskaæ informacje, a nastêpnie naciœnij klawisz F1.

<sup>-1</sup> danie lub uprawnienie dostępu lub kontrolowania dostępu do plików.

<sup>1</sup> dany lub uprawnienie do wykonywania operacji sieciowych lub czynności związanych z siecią.

Uprawnienie kontrolujące możliwość tworzenia wątków i grup wątków oraz operowania nimi.

<sup>-1</sup> danie lub uprawnienie dostępu do w³acziwoœci systemu lub operowania nimi.

—<sup>1</sup> danie lub uprawnienie do sterowania innym programem lub uruchamianie go.



<sup>1</sup>danie lub uprawnienie do wykonywania operacji odbicia lub używania interfejsu API do uzyskiwania dostępu do elementów podanej klasy.

Uprawnienie kontrolujące dostęp do interfejsu API drukowania.

Uprawnienie kontrolujące możliwość uzyskiwania dostępu do rejestru lub udzielenia dostępu do klucza rejestru.

Uprawnienie kontrolujące dostęp do klas zabezpieczeń JDK, `java.lang.security`.

Uprawnienie kontrolujące możliwość tworzenia miejsca pomocniczego do 1 MB przez kod podpisany, które może być wykorzystywane do przechowywania tymczasowych informacji. Aplet Java nie będzie mógł czytać ani zapisywać żadnych innych plików na dysku twardym użytkownika. Podpisany aplet może mieć dostęp jedynie do własnego miejsca pomocniczego. Poziom tego uprawnienia jest określany jako średni.

<sup>1</sup> dające użytkownikowi rozszerzony aspekt interfejsu API użytkownika lub uprawnienie kontrolujące możliwość używania niektórych rozszerzonych funkcji AWT (Application Windowing Toolkit).

Uprawnienie kontrolujące możliwość zmiany wartości strumieni systemowych: `java.lang.System.in`, `java.lang.System.out` oraz `java.lang.System.err`.

Uprawnienie, które kontroluje zdolność do wyświetlania okien dialogowych, potrzebnych do wykonywania operacji. Na przykład, jeżeli aplet wymaga otwarcia pliku, musi wywołać standardowe okno dialogowe **Otwórz plik**, aby następnie pozwolić użytkownikowi na wybór pliku. Dlatego sam aplet nie może wykonać w pełni operacji. W wyniku tego operacja taka jest uważana za bezpieczniejszą od użycia kodu realizującego bezpośredni dostęp do pliku, ponieważ mamy tu do czynienia z bezpośrednim zaangażowaniem użytkownika. Poziom tego uprawnienia jest określany jako średni.



Uprawnienie zezwalające na użycie rozszerzonej funkcjonalności multimedialnej.

Uprawnienie zapewniające specjalne możliwości kontroli rodzaju uprawnień udzielanych podpisanej zawartości.

