

Edycja uprawnień - karta

Określa, jak Internet Explorer ma obsługiwać ca³¹ zawartość oraz uprawnienia wymagane przez podpisane i nie podpisane aplety Java.

Ustawienia dla uprawnień niepodpisanych i podpisanych wp³ywaj¹ na:

[Dostęp do wszystkich plików](#)

[Dostęp do wszystkich adresów sieciowych](#)

[Wykonywanie](#)

[Dialogi](#)

[Informacje o systemie](#)

[Drukowanie](#)

[Chroniona przestrzeń dostępna](#)

[Dostęp do plików wybrany przez użytkownika](#)

Uprawnienia niepodpisane

Uprawnienia możesz określić indywidualnie, ustawiaj¹c w polu **Uruchamiaj niepodpisane zawartość** wartość **Uruchamiaj w piaskownicy**. Następnie możesz zresetować oddzielnie każde uprawnienie, nadaj¹c mu wartość **Wy³¹cz** lub **W³¹cz** w polu **Uruchamiaj niepodpisane zawartość**. Jeżeli wybierzesz wartość **Wy³¹cz** lub **W³¹cz** w polu **Uruchamiaj niepodpisane zawartość**, ustawienie to będzie stosowane dla wszystkich uprawnień w obszarze **Dodatkowe niepodpisane uprawnienia**.

Wybierz jedn¹ z następujących możliwości:

- Aby uruchomić nie podpisane zawartość jedynie z uprawnieniami dozwolonymi w module sandbox, kliknij opcję **Uruchamiaj w piaskownicy**. Jeżeli wybierzesz tę opcję, możesz zresetować oddzielnie każde uprawnienie, nadaj¹c mu wartość **Wy³¹cz** lub **W³¹cz** w polu **Uruchamiaj niepodpisane zawartość**.
- Aby automatycznie odrzucać nie podpisane zawartość bez monitorowania, kliknij opcję **Wy³¹cz**. Wszystkie uprawnienia w polu **Dodatkowe niepodpisane uprawnienia** mają przypisaną wartość **Wy³¹cz** i nie można indywidualnie zresetować żadnego uprawnienia do wartości **W³¹cz**.
- Aby automatycznie akceptować nie podpisane zawartość bez monitorowania, kliknij opcję **W³¹cz**. Wszystkie uprawnienia w polu **Dodatkowe niepodpisane uprawnienia** mają przypisaną wartość **W³¹cz** i nie można indywidualnie zresetować żadnego uprawnienia do wartości **Wy³¹cz**.

Uprawnienia podpisane

Uprawnienia możesz określić indywidualnie, ustawiaj¹c w polu **Uruchamiaj podpisane zawartość** wartość **Monituj**, która ustawia wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** na wartość **Monituj**. Następnie możesz zresetować oddzielnie każde uprawnienie, nadaj¹c mu wartość **Wy³¹cz** lub **W³¹cz** w polu **Uruchamiaj niepodpisane zawartość**. Jeżeli wybierzesz wartość **Wy³¹cz** lub **W³¹cz** w polu **Uruchamiaj podpisane zawartość**, ustawienie to będzie stosowane dla wszystkich uprawnień w obszarze **Dodatkowe podpisane uprawnienia**.

Wybierz jedn¹ z następujących możliwości:

- Aby uzyskiwać monity przed kontynuowaniem, kliknij opcję **Monituj**. Jeżeli wybierzesz opcję **Monituj** w polu **Uruchamiaj podpisane zawartość**, wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** mają przypisaną wartość **Monituj** i można każde z nich indywidualnie zresetować do wartości **Wy³¹cz** lub **W³¹cz**.
- Aby automatycznie odrzucać podpisane zawartość bez monitorowania, kliknij opcję **Wy³¹cz**. Wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** mają przypisaną wartość **Wy³¹cz** i nie można indywidualnie zresetować żadnego uprawnienia do wartości **Monituj** lub **W³¹cz**.
- Aby automatycznie akceptować nie podpisane zawartość bez monitorowania, kliknij opcję **W³¹cz**. Wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** mają przypisaną wartość **W³¹cz** i nie można indywidualnie zresetować żadnego uprawnienia do wartości **Monituj** lub **Wy³¹cz**.

Zamyka to okno dialogowe i zapisuje wprowadzone zmiany.

Kliknij, aby zresetować wszystkie uprawnienia Java. Wybierz jedną z następujących opcji, a następnie kliknij przycisk **Resetuj**.

- **Zapisane uprawnienia** Resetuje do ostatnich zapisanych uprawnień. Wszystkie zmiany wprowadzone od czasu ostatniego zapisu ustawień zostaną utracone.
- **Wysoki poziom zabezpieczeń** Resetuje do uprawnień wysokiego bezpieczeństwa (najbardziej restrykcyjne, aplety działają w trybie bezpiecznym). Wszystkie uprawnienia w polu **Uruchamiaj podpisane zawartości** resetowane do wartości **Monituj**, a w polu **Dodatkowe niepodpisane uprawnienia** do wartości **Wyłącz**.
- **Średni poziom zabezpieczeń** Resetuje do uprawnień średniego bezpieczeństwa (aplety działają z pewnymi restrykcjami). Wszystkie uprawnienia (poza Przestrzeń dostępna i Dostęp do plików wybrany przez użytkownika) w polu **Uruchamiaj podpisane zawartości** resetowane do wartości **Monituj**, a w polu **Dodatkowe niepodpisane uprawnienia** do wartości **Wyłącz**.
- **Niski poziom zabezpieczeń** Resetuje do uprawnień niskiego bezpieczeństwa (najmniej restrykcyjne, aplety działają ze wszystkimi uprawnieniami). Wszystkie uprawnienia w polu **Uruchamiaj podpisane zawartości** resetowane do wartości **Włącz**, a w polu **Dodatkowe niepodpisane uprawnienia** do wartości **Wyłącz**.

Przeглядanie uprawnień - karta

Te uprawnienia s¹ uprawnieniami Java okreœlonymi przez administratora sieci.

Aby aplet Java mógł dzia³aæ, mo¿e wymagaæ dostêpu do plików i innych zasobów komputera. Wykonanie ka¿dego typu czynnoœci wymaga specjalnych uprawnień. Administrator sieci mo¿e okreœliæ, jakie uprawnienia s¹ dozwolone. Dla dozwolonych uprawnień administrator sieci mo¿e okreœliæ, czy bêd¹ pojawia³y siê powiadomienia o wymaganiu tych uprawnień. W przeciwnym przypadku powiadomienia pojawiaj¹ siê jedynie wówczas, gdy aplet Java wymaga wiêcej uprawnień ni¿ zosta³o automatycznie przydzielone przez administratora sieci.

Istniej¹ trzy zestawy uprawnień:

Uprawnienia nadane niepodpisanej zawartoœci Uprawnienia przydzielone pobranej zawartoœci niepodpisanej

Uprawnienia, które podpisana zawartoœæ posiada Uprawnienia, które nie wymagaj¹ potwierdzenia przez u¿ytkownika

Uprawnienia, które podpisanej zawartoœci zosta³y odmówione Uprawnienia, które wymagaj¹ potwierdzenia przez u¿ytkownika lub s¹ absolutnie zakazane

Mo¿esz klikn¹æ dwukrotnie nag³ówek ka¿dego z uprawnień, aby wyœwietliæ konkretne uprawnienia i okreœlone ustawienia.

Zestawom tym mo¿na przypisaæ nastêpuj¹ce uprawnienia:

W³aœciwoœci systemu

Refleksja

Dostêp do interfejsu u¿ytkownika

Operacje I/O na plikach

Operacje I/O sieci

W¹tki

Operacje I/O u¿ytkownika na plikach

Magazyn klienta

W³aœciwoœæ

Wykonanie

Drukowanie

Rejestr

Zabezpieczenie

Multimedia

Niestandardowe

Uprawnienie, które kontroluje dostęp do odczytu, zapisu i usuwania plików.

Uprawnienie, które kontroluje możliwość wykonywania operacji sieciowych lub czynności związanych z siecią.

Uprawnienie, które kontroluje możliwość tworzenia w³tków i grup w³tków oraz manipulowania nimi.

Uprawnienie, które kontroluje możliwość dostępu do globalnych w³aœciwoœci systemu i manipulowania nimi.

Uprawnienie, które kontroluje możliwość uruchamiania innych programów.

Uprawnienie, które kontroluje możliwość użycia interfejsu Reflection API w celu uzyskania dostępu do elementów podanej klasy.

Uprawnienie, które kontroluje dostęp do interfejsów API drukowania.

Uprawnienie, które kontroluje możliwość uzyskania dostępu do rejestru.

Uprawnienie, które kontroluje dostęp dla klas zabezpieczeń JDK **java.lang.security**.

Uprawnienie do kontrolowania dostępu do magazynu po stronie klienta, który jest dostępny przez klasę **ClientStore**.

Uprawnienie, które kontroluje możliwość użycia niektórych rozszerzonych funkcji AWT.

Uprawnienie, które kontroluje dostęp do informacji systemowych.

Uprawnienie, które kontroluje możliwość wyświetlania okien dialogowych plików do operacji na plikach. Na przykład, jeśli aplet chce otworzyć plik, musi skorzystać ze standardowego okna dialogowego Otwórz plik, aby pozwolić wybrać użytkownikowi plik do otwarcia. Aplet nie będzie mógł wykonywać operacji na plikach samodzielnie. Dzięki temu działanie jest bezpieczniejsze niż w przypadku kodu bezpośredniego dostępu do pliku, bowiem wiąże się z zaangażowaniem użytkownika. Uprawnienie to jest uprawnieniem "średniego" poziomu.

Uprawnienie, które kontroluje użycie rozszerzonych funkcji multimedialnych.

Uprawnienie, które kontroluje możliwość wykonywania operacji niestandardowych.

Uprawnienie, które kontroluje możliwość tworzenia miejsca pomocniczego, które może być wykorzystywane do przechowywania tymczasowych informacji. Aplet nie będzie mógł czytać ani zapisywać żadnych innych plików na dysku twardym użytkownika. Podpisany aplet może mieć dostęp jedynie do własnego miejsca pomocniczego. Uprawnienie to jest uprawnieniem "średniego" poziomu.

Uprawnienie, które kontroluje możliwość przedstawiania okien dialogowych.

