Edycja uprawnieñ - karta

Okreœla, jak Internet Explorer ma obs³ugiwaæ ca³ zawartoœæ oraz uprawnienia wymagane przez podpisane i nie podpisane aplety Java.

Ustawienia dla uprawnieñ nie podpisanych i podpisanych wp³ywaj¹ na:

Chroniona przestrzeñ dostêpna

Dialogi

Dostêp do plików wybrany przez u¿ytkownika

Dostêp do wszystkich adresów sieciowych

Dostêp do wszystkich plików

Drukowanie

Informacje o systemie

Wykonywanie

Uruchamiaj niepodpisan¹ zawartoœæ

Uprawnienia mo¿esz okreœliæ indywidualnie, ustawiaj¹c w polu **Uruchamiaj niepodpisan¹ zawartoœæ** wartoœæ **Uruchamiaj w piaskownicy**. Nastêpnie mo¿esz zresetowaæ oddzielnie ka¿de uprawnienie, nadaj¹c mu wartoœæ **Wy³cz** lub **W³cz** w polu **Uruchamiaj niepodpisan¹ zawartoœæ**. Jeœli wybierzesz wartoœæ **Wy³cz** lub **W³cz** w polu **Uruchamiaj niepodpisan¹ zawartoœæ**, ustawienie to bêdzie stosowane dla wszystkich uprawnieñ w obszarze **Dodatkowe niepodpisane uprawnienia**.

Wybierz jedn¹ z nastêpuj¹cych mo¿liwoœci dla pola **Uruchamiaj niepodpisan¹ zawartoœæ**:

- Aby uruchomiæ nie podpisan¹ zawartoœæ jedynie z uprawnieniami dozwolonymi w „piaskownicy", kliknij opcjê **Uruchamiaj w piaskownicy**. Jeœli wybierzesz tê opcjê, mo¿esz zresetowaæ oddzielnie ka¿de uprawnienie, nadaj¹c mu wartoœæ **Wy³cz** lub **W³cz**.
- Aby automatycznie odrzucaæ nie podpisan¹ zawartoœæ bez monitowania, kliknij opcjê **Wy³cz**. Wszystkie uprawnienia w polu **Dodatkowe niepodpisane uprawnienia** maj¹ przypisan¹ wartoœæ **Wy³cz**; nie mo¿na indywidualnie zresetowaæ ¿adnego uprawnienia do wartoœci **W³cz**.
- Aby automatycznie akceptowaæ nie podpisan¹ zawartoœæ bez monitowania, kliknij opcjê **W³cz**. Wszystkie uprawnienia w polu **Dodatkowe niepodpisane uprawnienia** maj¹ przypisan¹ wartoœæ **W³cz**; nie mo¿na indywidualnie zresetowaæ ¿adnego uprawnienia do wartoœci **Wy³cz**.

Uruchamiaj podpisan¹ zawartoœæ

Uprawnienia mo¿esz okreœliæ indywidualnie, ustawiaj¹c w polu **Uruchamiaj podpisan¹ zawartoœæ** wartoœæ **Monituj**, która ustawia wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** na wartoœæ **Monituj**. Nastêpnie mo¿esz zresetowaæ oddzielnie ka¿de uprawnienie, nadaj¹c mu wartoœæ **Wy³cz** lub **W³cz**. Jeœli wybierzesz wartoœæ **Wy³cz** lub **W³cz**, ustawienie to bêdzie stosowane dla wszystkich uprawnieñ w obszarze **Dodatkowe podpisane uprawnienia**.

Wybierz jedn¹ z nastêpuj¹cych mo¿liwoœci dla pola **Uruchamiaj podpisan¹ zawartoœæ**:

- Aby uzyskiwaæ monity o akceptacjê przed uruchomieniem apletu Java z jego wymaganymi uprawnieniami, kliknij opcjê **Monituj**. Jeœli wybierzesz opcjê **Monituj** w polu **Uruchamiaj podpisan¹ zawartoœæ**, wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** maj¹ przypisan¹ wartoœæ **Monituj** i mo¿na ka¿de z nich indywidualnie zresetowaæ do wartoœci **Wy³cz** lub **W³cz**.
- Aby automatycznie odrzucaæ uruchamianie podpisanej zawartoœci bez monitowania, kliknij opcjê **Wy³cz**. Wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** maj¹ przypisan¹ wartoœæ **Wy³cz**; nie mo¿na indywidualnie zresetowaæ ¿adnego uprawnienia do wartoœci **Monituj** lub **W³cz**.
- Aby automatycznie akceptowaæ uruchamianie nie podpisanej zawartoœci bez monitowania, kliknij opcjê **W³cz**. Wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** maj¹ przypisan¹ wartoœæ **W³cz**; nie mo¿na indywidualnie zresetowaæ ¿adnego uprawnienia do wartoœci **Monituj** lub **Wy³cz**.

Zamyka to okno dialogowe i zapisuje wprowadzone zmiany.

Kliknij, aby zresetowaæ wszystkie uprawnienia Java. Wybierz jedn¹ z nastêpuj¹cych opcji, a nastêpnie kliknij przycisk **Resetuj**.

- **Zapisane uprawnienia** Resetuje do ostatnich zapisanych uprawnieñ. Wszystkie zmiany wprowadzone od czasu ostatniego zapisu ustawieñ zostan¹ utracone.
- **Wysoki poziom zabezpieczeñ** Resetuje do uprawnieñ wysokiego bezpieczeñstwa (najbardziej restrykcyjne, aplety dzia³aj¹ w trybie bezpiecznym). Wszystkie uprawnienia w polu **Uruchamiaj podpisan¹ zawartoœæ** s¹ resetowane do wartoœci **Monituj**, a w polu **Dodatkowe niepodpisane uprawnienia** do wartoœci **Wy³cz**.
- **Œredni poziom zabezpieczeñ** Resetuje do uprawnieñ œredniego bezpieczeñstwa (aplety dzia³aj¹ w piaskownicy z dwoma dodatkowymi restrykcjami, Przestrzeñ dostêpna i Dostêp do plików wybrany przez u¿ytkownika). Wszystkie uprawnienia (oprócz Przestrzeñ dostêpna i Dostêp do plików wybrany przez u¿ytkownika) w polu **Uruchamiaj podpisan¹ zawartoœæ** s¹ resetowane do wartoœci **Monituj**, a w polu **Dodatkowe niepodpisane uprawnienia** do wartoœci **Wy³cz**.
- **Niski poziom zabezpieczeñ** Resetuje do uprawnieñ niskiego bezpieczeñstwa (najmniej restrykcyjne, aplety dzia³aj¹ ze wszystkimi uprawnieniami). Wszystkie uprawnienia w polu **Uruchamiaj podpisan¹ zawartoœæ** s¹ resetowane do wartoœci **W³cz**, a w polu **Dodatkowe niepodpisane uprawnienia** do wartoœci **Wy³cz**.

Przegl¹danie uprawnieñ - karta

Te uprawnienia Java okreœlonymi przez administratora sieci.

Aby aplet Java mógł dzia³aæ, mo¿e wymagaæ dostêpu do plików i innych zasobów komputera. Czynnoœci te wymagaj¹ specjalnych uprawnieñ, które musz¹ byæ udzielone przed ich podjêciem. Administrator sieci mógł ju¿ okreœliæ, jakie uprawnienia s¹ dozwolone. Dla dozwolonych uprawnieñ administrator sieci mo¿e okreœliæ, czy bêd¹ pojawia³y siê powiadomienia o wymaganiu tych uprawnieñ. W przeciwnym przypadku powiadomienia pojawiaj¹ siê jedynie wówczas, gdy aplet Java wymaga wiêcej uprawnieñ ni¿ zosta³o to automatycznie przydzielone przez administratora sieci.

Istniej¹ nastêpuj¹ce trzy zestawy uprawnieñ:

Uprawnienia nadane niepodpisanej zawartoœci Uprawnienia przydzielone pobranej zawartoœci nie podpisanej (aplety bêd¹ uruchamiane w piaskownicy).

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 uprawnieñ, aby wyœwietliæ konkretne uprawnienia i okreœlone ustawienia.

Zestawom tym mo¿na przypisaæ nastêpuj¹ce uprawnienia:

Dostêp do interfejsu u¿ytkownika

Drukowanie

Informacje o systemie

Magazyn klienta

Multimedia

Niestandardowe

Operacje I/O na plikach

Operacje I/O sieci

Operacje I/O u¿ytkownika na plikach

Refleksja

Rejestr

W¹tki

W³aœciwoœæ

Wykonanie

Zabezpieczenie

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

Uprawnienie, które kontroluje mo¿liwoœæ wykonywania operacji sieciowych lub czynnoœci zwi¹zanych z sieci¹.

Uprawnienie, które kontroluje mo¿liwoœæ tworzenia w¹tków i grup w¹tków oraz manipulowania nimi.

Uprawnienie, które kontroluje mo¿liwoœæ dostêpu do globalnych w³aœciwoœci systemu i manipulowania nimi.

Uprawnienie, które kontroluje mo¿liwoœæ uruchamiania innych programów.

Uprawnienie, które kontroluje mo¿liwoœæ u¿ycia interfejsu Reflection API w celu uzyskania dostêpu do elementów podanej klasy.

Uprawnienie, które kontroluje dostêp do interfejsów API drukowania.

Uprawnienie, które kontroluje mo¿liwoœæ uzyskania dostêpu do rejestru.

Uprawnienie, które kontroluje dostêp dla klas zabezpieczeñ JDK, java.lang.security.

Uprawnienie do kontrolowania dostêpu do magazynu po stronie klienta, który jest dostêpny przez klasê ClientStore.

Uprawnienie, które kontroluje mo¿liwoœæ u¿ycia niektórych rozszerzonych funkcji AWT.

Uprawnienie, które kontroluje dostêp do informacji systemowych.

Uprawnienie, które kontroluje możliwość wyświetlania okien dialogowych plików do operacji na plikach. Na przykład, jeśli aplet wymaga otwarcia pliku, musi skorzystać ze standardowego okna dialogowego **Otwórz plik**, aby następnie pozwolić wybrać użytkownikowi plik do otwarcia. Aplet nie będzie mógł wykonywać operacji na plikach samodzielnie. Dzięki temu operacja jest bezpieczniejsza niż w przypadku kodu realizującego bezpośredni dostęp do pliku, ponieważ wymaga bezpośredniego zaangażowania użytkownika. Poziom tego uprawnienia jest określany jako średni.

Uprawnienie, które kontroluje u¿ycie rozszerzonych funkcji multimedialnych.

Uprawnienie, które zapewnia mo¿liwoœæ dok³adnej kontroli rodzaju uprawnieñ udzielanych podpisanej zawartoœci.

Uprawnienie, które kontroluje możliwość tworzenia do 1 MB miejsca pomocniczego 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.

Uprawnienie, które kontroluje mo¿liwoœæ przedstawiania okien dialogowych.

Œrodowisko chroni¹ce pewne zasoby (na przyk³ad system, dysk twardy, sieæ, komputer lokalny itd.) przed dostêpem z zewn¹trz, w którym aplet Java mo¿e byæ uruchomiony z kontrolowanym przez u¿ytkownika zestawem uprawnieñ.