

Karta Upravit oprávnění

Určuje, jakým způsobem se bude zacházet s veškerým obsahem a se všemi oprávněními, které jsou vyžadovány prostřednictvím podepsaných a nepodepsaných apletů v jazyce Java.

Nastavení pro oprávnění Nepodepsáno a Podepsáno má vliv na následující oprávnění:

[Čtení či zápis souboru](#)

[Čtení či zápis v síti](#)

[Spouštění](#)

[Dialogy](#)

[Systémové sekvence](#)

[Tisk](#)

[Chráněný odkládací prostor](#)

[Uživatелеm řízené čtení či zápis souboru](#)

Nepodepsaná oprávnění

Nastavíte-li volbu **Spustit nepodepsaný obsah** na možnost **RSpouu in sandbox**, můžete každé oprávnění samostatně nastavit na hodnotu **Vypnout** nebo **Zapnout**. Hodnota **Vypnout** nebo **Zapnout**, kterou jste určili ve volbě **Spustit nepodepsaný obsah**, bude použita pro všechna oprávnění ve volbě **Další nepodepsaná oprávnění**.

Zvolte jednu z následujících možností:

- Chcete-li nepodepsaný obsah spustit pouze s oprávněními, která jsou povolena v chráněné oblasti, klepněte na možnost **Spouštět v odděleném paměťovém prostoru**. Pokud pro volbu **Spustit nepodepsaný obsah** zvolíte tuto možnost, bude možné každé oprávnění jednotlivě nastavit na hodnotu **Vypnout** nebo **Zapnout**.
- Chcete-li nepodepsaný obsah automaticky bez upozornění odmítnout, klepněte na hodnotu **Vypnout**. Všechna oprávnění ve volbě **Další nepodepsaná oprávnění** budou tímto způsobem nastavena na hodnotu **Vypnout** a žádné oprávnění nebude možné jednotlivě nastavit na hodnotu **Zapnout**.
- Chcete-li nepodepsaný obsah automaticky bez upozornění přijmout, klepněte na hodnotu **Zapnout**. Všechna oprávnění ve volbě **Další nepodepsaná oprávnění** budou tímto způsobem nastavena na hodnotu **Zapnout** a žádné oprávnění nebude možné jednotlivě nastavit na hodnotu **Vypnout**.

Podepsaná oprávnění

Nastavíte-li volbu **Spustit podepsaný obsah** na hodnotu **Dotázat**, budou všechna oprávnění ve volbě **Další podepsaná oprávnění** nastavena na hodnotu **Dotázat** a poté bude možné každé oprávnění jednotlivě nastavit na hodnotu **Vypnout** nebo **Zapnout**. Nastavíte-li volbu **Spustit podepsaný obsah** na hodnotu **Vypnout** nebo **Zapnout**, bude toto nastavení použito pro všechna oprávnění ve volbě **Další podepsaná oprávnění**.

Zvolte jednu z následujících možností:

- Chcete-li pokračování vždy potvrdit, klepněte na hodnotu **Dotázat**. Zvolíte-li pro volbu **Spustit podepsaný obsah** hodnotu **Dotázat**, budou všechna oprávnění ve volbě **Další podepsaná oprávnění** nastavena na hodnotu **Dotázat**. Poté bude možné každé oprávnění jednotlivě nastavit na hodnotu **Vypnout** nebo **Zapnout**.
- Chcete-li podepsaný obsah automaticky bez upozornění odmítnout, klepněte na hodnotu **Vypnout**. Všechna oprávnění ve volbě **Další podepsaná oprávnění** budou tímto způsobem nastavena na hodnotu **Vypnout** a žádné oprávnění nebude možné jednotlivě nastavit na hodnotu **Dotázat** nebo **Zapnout**.
- Chcete-li podepsaný obsah automaticky bez upozornění přijmout, klepněte na hodnotu **Zapnout**. Všechna oprávnění ve volbě **Další podepsaná oprávnění** budou tímto způsobem nastavena na hodnotu **Zapnout** a žádné oprávnění nebude možné jednotlivě nastavit na hodnotu **Dotázat** nebo **Vypnout**.

Zavřete toto dialogové okno a uložte všechny provedené změny.

Klepněte zde, chcete-li pro všechna oprávnění pro jazyk Java obnovit původní nastavení. Zvolte jednu z následujících možností a poté klepněte na tlačítko **Obnovit**.

- **Uložená oprávnění** Obnoví poslední známá uložená oprávnění. Tímto způsobem budou ztraceny všechny změny, které byly od posledního uložení provedeny.
- **Vysoké zabezpečení** Nastaví oprávnění na vysoké zabezpečení (největší omezení; aplety budou spouštěny v chráněném režimu). Tímto způsobem budou všechna oprávnění ve volbě **Spustit podepsaný obsah** nastavena na hodnotu **Dotázat** a všechna oprávnění ve volbě **Další nepodepsaná oprávnění** na hodnotu **Vypnout**.
- **Střední zabezpečení** Nastaví oprávnění na střední zabezpečení (aplety budou spouštěny s určitými omezeními). Tímto způsobem budou všechna oprávnění ve volbě **Spustit podepsaný obsah** (kromě Chráněný odkládací prostor a Uživatelem řízené čtení či zápis souboru) nastavena na hodnotu **Dotázat** a všechna oprávnění ve volbě **Další nepodepsaná oprávnění** na hodnotu **Vypnout**.
- **Nízké zabezpečení** Nastaví oprávnění na nízké zabezpečení (nejmenší omezení; aplety budou spouštěny se všemi oprávněními). Tímto způsobem budou všechna oprávnění ve volbě **Spustit podepsaný obsah** nastavena na hodnotu **Zapnout** a všechna oprávnění ve volbě **Další nepodepsaná oprávnění** na hodnotu **Vypnout**.

Karta Zobrazit oprávnění

Tato oprávnění jsou oprávnění pro jazyk Java a byla takto zadána správcem sítě.

Aplet v jazyce Java může pro své spuštění vyžadovat přístup k některým souborům a dalším prostředkům v počítači. Pro každou z těchto akcí je nutné vlastnit příslušné oprávnění, které musí být přiděleno před provedením dané akce. Správce sítě zřejmě již tato oprávnění nastavil. Pro přidělená oprávnění může správce určit, zda budete před požadavkem na toto oprávnění upozorněni. Pokud nebude toto nastavení provedeno, nezobrazí se v případě požadavku na oprávnění, která nejsou automaticky přidělována správcem sítě, žádné upozornění.

Lze použít tři sady oprávnění:

Oprávnění zapnuta pro Nepodepsaný obsah Oprávnění přidělená pro stáhnutý nepodepsaný obsah

Oprávnění zapnuta pro Podepsaný obsah Oprávnění, která nepožadují potvrzení uživatelem

Oprávnění vypnuta pro Podepsaný obsah Oprávnění, která požadují potvrzení uživatelem nebo jsou zcela odepřena

Chcete-li zobrazit příslušná oprávnění a jejich nastavení, poklepejte na některý z těchto nadpisů.

K těmto sadám mohou být přiřazena následující oprávnění:

Systemové informace

Reflexe

Přístup k uživatelskému rozhraní

Čtení či zápis souboru

Čtení či zápis v síti

Podprocesy

Uživatelským řízené čtení či zápis souboru

Ukládání klienta

Vlastnost

Spouštění

Tisk

Registr

Zabezpečení

Multimédia

Vlastní

Oprávnění, které řídí přístup pro čtení, zápis a odstraňování souborů.

Oprávnění, které řídí schopnost provádět síťové operace nebo akce se sítí související.

Oprávnění, které řídí schopnost vytvářet a pracovat s podprocesy jejich skupinami.

Oprávnění, které řídí schopnost přistupovat a pracovat s globálními systémovými vlastnostmi.

Oprávnění, které řídí schopnost spouštět jiné programy.

Oprávnění, které řídí schopnost používat reflexní rozhraní API. Prostřednictvím tohoto rozhraní lze získat přístup ke členům určité třídy.

Oprávnění, které řídí přístup k tiskovým rozhraním API.

Oprávnění, které řídí schopnost získat přístup k registrům.

Oprávnění, které řídí přístup ke třídám zabezpečení JDK **java.lang.security**.

Oprávnění pro řízení přístupu k paměťovému prostoru klienta, který je dostupný prostřednictvím třídy **ClientStore**.

Oprávnění, které řídí schopnost používat některé rozšířené funkce AWT.

Oprávnění, které řídí přístup k systémovým informacím.

Oprávnění, které řídí schopnost zobrazit dialogová okna k provádění operací se soubory. Pokud je například apletem vyžadováno otevření souboru, musí být použit standardní dialog Otevřít, který uživateli umožňuje soubor pro otevření zvolit. Aplet nemůže sám o sobě operace se soubory provádět. Takto je daná operace bezpečnější než přímý přístup do souboru, protože je zde přímý zásah uživatele. Toto oprávnění je oprávnění střední úrovně.

Oprávnění, které řídí používání rozšířených multimediálních funkcí.

Oprávnění, které řídí schopnost provádět uživatelem definované operace.

Oprávnění, které řídí schopnost vytvářet chráněný odkládací prostor, který lze použít k ukládání dočasných informací. Aplet nebude moci číst ani zapisovat jiné soubory na pevný disk uživatele. Podepsaný aplet má přístup pouze do vlastního chráněného odkládacího prostoru. Toto oprávnění je oprávnění střední úrovně.

Oprávnění, které řídí schopnost zobrazit dialogová okna.

