Redigera behörigheter, flik

Här kan du ange hur Internet Explorer ska hantera allt innehåll och alla behörigheter som begärs av signerade och osignerade Java-appletar.

Följande behörigheter påverkas av inställningarna för osignerade och signerade behörigheter:

Användarstyrda filer

Dialoger

Kör

Skyddat virtuellt minne

Systeminformation

Utskrift

Åtkomst till alla filer

Åtkomst till alla nätverksadresser

Köra osignerat innehåll

Du kan ange behörigheter individuellt genom att ange **Kör osignerat innehåll** till **Kör begränsat**. Därefter kan du återställa varje behörighet till **Inaktivera** eller **Aktivera**. Om du anger **Inaktivera** eller **Aktivera** under **Kör osignerat innehåll**, kommer alla behörigheter under **Fler osignerade behörigheter** att använda den inställningen.

Markera en av följande inställningar för **Kör osignerat innehåll**:

- Om du vill köra osignerat innehåll med endast de behörigheter som är tillåtna i begränsat läge, markerar du **Kör begränsat**. Om du gör det kan du återställa varje behörighet till **Inaktivera** eller **Aktivera**.
- Om du vill avböja osignerat innehåll automatiskt utan att få ett meddelande om det, markerar du **Inaktivera**. Alla behörigheter under **Fler osignerade behörigheter** anges till **Inaktivera** och du kan inte återställa någon behörighet till **Aktivera**.
- Om du vill acceptera osignerat innehåll automatiskt utan att få ett meddelande om det, markerar du **Aktivera**. Alla behörigheter under **Fler osignerade behörigheter** anges till **Aktivera** och du kan inte återställa någon behörighet till **Inaktivera**.

Köra signerat innehåll

Du kan ange behörigheter individuellt genom att ange **Kör signerat innehåll** till **Fråga**, vilket anger alla behörigheter under **Fler signerade behörigheter** till **Fråga**. Därefter kan du återställa varje behörighet till **Inaktivera** eller **Aktivera**. Om du anger **Inaktivera** eller **Aktivera** kommer alla behörigheter under **Fler signerade behörigheter** att använda den inställningen.

Markera en av följande inställningar för **Kör signerat innehåll**:

- Om du vill bekräfta innan en Java-applet körs markerar du **Fråga**. Om du väljer **Fråga** för **Kör signerat innehåll** anges alla behörigheter under **Fler signerade behörigheter** in till **Fråga**, men du kan återställa varje behörighet till **Inaktivera** eller **Aktivera**.
- Om du vill avböja att köra signerat innehåll automatiskt utan att få ett meddelande om det, markerar du **Inaktivera**. Alla behörigheter under **Fler signerade behörigheter** anges till **Inaktivera** och du kan inte återställa någon behörighet till **Fråga** eller **Aktivera**.
- Om du vill acceptera att köra osignerat innehåll automatiskt utan att få ett meddelande om det, markerar du **Aktivera**. Alla behörigheter under **Fler signerade behörigheter** anges till **Aktivera** och du kan inte återställa någon behörighet till **Fråga** eller **Inaktivera**.

Stänger dialogrutan och sparar de ändringar du har gjort.

Klicka här om du vill återställa alla Java-behörigheter. Markera ett av följande och klicka sedan på **Återställ**.

- **Sparade behörigheter** Återställer de senast sparade behörigheterna. Ändringar som har gjorts efter de senast sparade inställningarna kommer att förloras.
- **Hög säkerhet** Återställer dessa behörigheter (den mest restriktiva behörigheten, appletar körs i säkert läge). Alla behörigheter under **Kör signerat innehåll** anges till **Fråga** och alla behörigheter under **Fler osignerade behörigheter** anges till **Inaktivera**.
- **Normal säkerhet** Återställer dessa behörigheter (appletar körs i begränsat läge med två extra behörigheter: Skyddat virtuellt minne och Användarstyrda filer). Alla behörigheter (förutom Skyddat virtuellt minne och Användarstyrda filer) under **Kör signerat innehåll** anges till **Fråga** och alla behörigheter under **Fler osignerade behörigheter** anges till **Inaktivera**.
- **Låg säkerhet** Återställer dessa behörigheter (den minst restriktiva behörigheten, appletar kör med alla behörigheter). Alla behörigheter under **Kör signerat innehåll** anges till **Aktivera** och alla behörigheter under **Fler osignerade behörigheter** anges till **Inaktivera**.

Visa behörigheter, flik

Dessa Java-behörigheter har angetts av nätverksadministratören.

En Java-applet kan behöva filåtkomst och tillgång till andra resurser på datorn för att kunna köras. Dessa åtgärder kräver särskilda behörigheter innan de kan utföras. Nätverksadministratören kanske redan har angett vilka behörigheter som kan godkännas. För de behörigheter som är tillåtna kan nätverksadministratören ange om du ska informeras när dessa behörigheter efterfrågas. I annat fall blir du bara informerad när en Java-applet efterfrågar fler behörigheter än vad som automatiskt tillåts.

Det finns tre typer av behörigheter:

Behörigheter aktiverade för osignerat innehåll Behörigheter som ges till osignerat hämtat innehåll (appletar körs i begränsat läge).

Behörigheter aktiverade för signerat innehåll Behörigheter som inte kräver ett godkännande från användaren.

Behörigheter inaktiverade för signerat innehåll Behörigheter som kräver användarens godkännande eller absolut inte godkänns.

Du kan dubbelklicka på var och en av dessa behörighetsrubriker om du vill visa de behörigheter och inställningar som anges.

Du kan tilldela följande behörigheter till dessa uppsättningar:

Anpassad

Användargränssnitt

Användarstyrda filer

ClientStore

Egenskaper

Filer

Körning

Multimedia

Nätverk

Reflektion

Register

Systeminformation

Säkerhet

Trådar

Utskrift

En behörighet som styr läs-, skriv- och borttagningsåtkomsten till filer.

En behörighet som styr möjligheten att utföra nätverksfunktioner eller nätverksrelaterade funktioner.

En behörighet som styr möjligheten att skapa och hantera konversationer och konversationsgrupper.

En behörighet som styr möjligheten att få åtkomst till eller hantera globala systemegenskaper.

En behörighet som styr möjligheten att köra andra program.

En behörighet som styr möjligheten att använda Reflection-API:t för att få åtkomst till medlemmar i en angiven klass.

En behörighet som styr åtkomsten till utskrifts-API:er.

En behörighet som styr möjligheten att få åtkomst till registret.

En behörighet som styr åtkomsten till JDK-säkerhetsklasserna **java.lang.security**.

En behörighet som styr åtkomsten till information som lagrats på klienten som är tillgängligt via klassen **ClientStore**.

En behörighet som styr möjligheten att använda en del av de utökade funktionerna i AWT.

En behörighet som styr åtkomsten till systeminformation.

En behörighet som styr möjligheten att visa dialogrutor för att utföra filåtgärder. Om en applet exempelvis behöver öppna en fil måste den visa standarddialogrutan **Öppna** och låta användaren välja vilken fil som ska öppnas. Appleten kan inte utföra filåtgärder på egen hand. På så sätt kan detta anses vara säkrare än att koden har direkt filåtkomst eftersom det då handlar om en direktåtgärd från användaren. Denna behörighet är av typen **Normal**.

En behörighet som styr användningen av utökad multimediafunktionalitet.

En behörighet som ger specifika styrningsmöjligheter över behörigheter för signerat innehåll.

En behörighet som styr möjligheten för signerad kod att skapa ett startutrymme på upp till 1 MB som kan användas för att spara temporär information. Java-appleten kommer inte tillåtas läsa eller skriva till några filer på användarens hårddisk. En signerad applet har bara tillgång till sitt eget startutrymme. Denna behörighet är av typen **Normal**.

En behörighet som styr möjligheten att visa dialogrutor.

En miljö som skyddar vissa resurser (exempelvis system, hårddiskar, nätverk, lokala datorer m m) från åtkomst utifrån när en Java-applet körs med användarstyrda behörigheter.