

## Kategorien Rediger tillatelser

Angir hvordan du vil at Internet Explorer skal behandle innholdet og tillatelsene som kreves av signerte og usignerte Java-appleter.

Følgende tillatelser påvirkes av innstillingene for usignerte og signerte tillatelser:

[Tilgang til alle filer](#)

[Tilgang til alle nettverksadresser](#)

[Kjøring](#)

[Dialogbokser](#)

[Systeminformasjon](#)

[Utskrift](#)

[Beskyttet område for midlertidig lagring](#)

[Brukerstyrt filtilgang](#)

### Kjør usignert innhold

Du kan angi tillatelser hver for seg ved å sette **Kjør usignert innhold** til **Kjør Java innkapslet**. Deretter kan du tilbakestille hver tillatelse til **Deaktiver** eller **Aktiver**. Hvis du angir **Deaktiver** eller **Aktiver** i **Kjør usignert innhold**, vil alle tillatelsene under **Flere usignerte tillatelser** få denne innstillingen.

Velg én av følgende innstillinger for **Kjør usignert innhold**:

- Hvis du vil kjøre usignert innhold med bare de tillatelsene som finnes i "[innkapslingen](#)" (sandbox), velger du **Kjør Java innkapslet**. Hvis du gjør dette, kan du tilbakestille hver tillatelse til **Deaktiver** eller **Aktiver**.
- Hvis du automatisk vil avvise usignert innhold uten å bli spurt, velger du **Deaktiver**. Alle tillatelser under **Flere usignerte tillatelser** blir deaktivert. Du kan ikke tilbakestille dem til **Aktiver**.
- Hvis du automatisk vil godkjenne usignert innhold uten å bli spurt, velger du **Aktiver**. Alle tillatelser under **Flere usignerte tillatelser** blir aktivert. Du kan ikke tilbakestille dem til **Deaktiver**.

### Kjør signert innhold

Du kan angi tillatelser hver for seg ved å sette **Kjør signert innhold** til **Spør**. Dette medfører at alle tillatelsene under **Flere signerte tillatelser** settes til **Spør**. Deretter kan du tilbakestille hver tillatelse med **Deaktiver** eller **Aktiver**. Hvis du velger **Deaktiver** eller **Aktiver**, vil alle tillatelsene under **Flere signerte tillatelser** få denne innstillingen.

Velg én av følgende innstillinger for **Kjør signert innhold**:

- Hvis du vil bli spurt om godkjenning før en Java-applet kan fortsette med de forespurte tillatelsene, klikker du **Spør**. Hvis du velger **Spør** for **Kjør signert innhold**, settes alle tillatelsene under **Flere signerte tillatelser** til **Spør**. Du kan imidlertid tilbakestille hver tillatelse til **Deaktiver** eller **Aktiver**.
- Hvis du automatisk vil avvise kjøring av signert innhold uten å bli spurt, velger du **Deaktiver**. Alle tillatelser under **Flere signerte tillatelser** settes til **Deaktiver**. Du kan ikke tilbakestille dem til **Spør** eller **Aktiver**.
- Hvis du automatisk vil godkjenne kjøring av signert innhold uten å bli spurt, velger du **Aktiver**. Alle tillatelser under **Flere signerte tillatelser** settes til **Aktiver**. Du kan ikke tilbakestille dem til **Spør** eller **Deaktiver**.

Lukker denne dialogboksen, og lagrer endringer du har utført.

Klikk her for å tilbakestille alle Java-tillatelser. Gjør ett av følgende, og velg deretter **Tilbakestill**.

- **Lagrede tillatelser** Tilbakestilles til den sist kjente, lagrede tillatelsen. Endringer som er utført etter siste lagring, går tapt.
- **Høy sikkerhet** Tilbakestilles til tillatelser med høy sikkerhet (mest restriktiv – appleter kjører i sikkermodus). Denne funksjonen tilbakestiller alle tillatelsene under **Kjør signert innhold** til **Spør** og under **Flere usignerte tillatelser** til **Deaktiver**.
- **Middels sikkerhet** Tilbakestilles til tillatelser med middels sikkerhet (appleter kjører i innkapslingen med to ekstra tillatelser, Beskyttet område for midlertidig lagring og Brukerstyrt filtilgang). Denne funksjonen tilbakestiller alle tillatelsene (unntatt tillatelsene Beskyttet område for midlertidig lagring og Brukerstyrt filtilgang) under **Kjør signert innhold** til **Spør** og under **Flere usignerte tillatelser** til **Deaktiver**.
- **Lav sikkerhet** Tilbakestilles til tillatelser med lav sikkerhet (minst restriktiv – appleter kjører med alle tillatelser). Denne funksjonen tilbakestiller alle tillatelser under **Kjør signert innhold** til **Aktiver** og under **Flere usignerte tillatelser** til **Deaktiver**.

## Kategorien Vis tillatelser

Disse Java-tillatelsene er definert av din systemansvarlig.

Hvis en Java-applet skal kunne kjøre, krever den filtilgang og andre ressurser på maskinen. Disse handlingene krever spesielle tillatelser før de kan utføres. Systemansvarlig kan allerede ha angitt hvilke tillatelser som kan brukes, og han kan angi om han skal gi deg beskjed når disse kreves. Hvis systemansvarlig ikke angir dette, vil du bare få beskjed når en Java-applet krever flere tillatelser enn det som automatisk tillates.

De tre typene tillatelser er:

**Tillatelser som er aktivert for usignert innhold** Tillatelser som gis for usignert innhold som er lastet ned (appletter kjøres i innkapslingen).

**Tillatelser som er aktivert for signert innhold** Tillatelser som ikke krever godkjenning fra brukeren.

**Tillatelser som er deaktivert for signert innhold** Tillatelser som krever godkjenning fra brukeren eller som ikke godkjennes.

Du kan dobbeltklikke hver type tillatelser for å vise hver enkelt tillatelse og dens angitte innstilling.

Følgende tillatelser kan tilordnes disse tre typene:

[Klientlagring](#)

[Egendefinert](#)

[Kjøring](#)

[Filtilgang](#)

[Multimedia](#)

[Nettverkstilgang](#)

[Utskrift](#)

[Egenskaper](#)

[Refleksjon](#)

[Register](#)

[Sikkerhet](#)

[Systeminformasjon](#)

[Tråder](#)

[Brukerstyrt filtilgang](#)

[Tilgang til brukergrensesnitt](#)

En tillatelse som kontrollerer lese-, skrive- og slettetilgang til filer.

En tillatelse som kontrollerer muligheten for å utføre nettverksoperasjoner eller en nettverksrelatert handling.

En tillatelse som kontrollerer muligheten for å lage og endre tråder og trådgrupper.

En tillatelse som kontrollerer muligheten for å få tilgang til eller endre egenskaper for et globalt system.



En tillatelse som kontrollerer muligheten for å kjøre andre programmer.

En tillatelse som kontrollerer muligheten for å bruke refleksjons-APIen for å få tilgang til medlemmer av en angitt klasse.

En tillatelse som kontrollerer tilgang til utskrifts-APIene.

En tillatelse som kontrollerer muligheten for å få tilgang til registret.

En tillatelse som kontrollerer tilgang til JDK-sikkerhetsklassene **java.lang.security**.

En tillatelse som kontrollerer tilgang til lagring på klientsiden, som er tilgjengelig via **ClientStore**-klassen.

En tillatelse som kontrollerer muligheten for å bruke den forbedrede funksjonaliteten for AWT.

En tillatelse som kontrollerer tilgang til systeminformasjon.



En tillatelse som kontrollerer muligheten for å vise dialogbokser som utfører filoperasjoner. Hvis for eksempel en applet trenger å åpne en fil, må standarddialogboksen Åpne fil vises, og brukeren må deretter merke filen som skal åpnes. Appleten kan ikke utføre filoperasjoner på egen hånd. Denne operasjonen anses derfor for å være sikrere enn hvis koden har direkte filtilgang, fordi brukeren er direkte involvert. Dette tillatelsesnivået heter Middels.

En tillatelse som kontrollerer bruken av forbedret multimediefunksjonalitet.

En tillatelse som gir nøyaktig kontroll over hvilke typer tillatelser som kan gi tilgang til signert innhold.

En tillatelse som kontrollerer muligheten for en signert kode å lage et område på opptil 1 MB som kan brukes til å lagre midlertidig informasjon. En Java-applet kan ikke lese fra eller skrive til andre filer på brukerens harddisk. En signert applet kan bare få tilgang til sitt eget område for midlertidig lagring. Dette tillatelsesnivået heter Middels.

En tillatelse som kontrollerer muligheten for å vise dialogbokser.

Et miljø for å beskytte bestemte ressurser (for eksempel system, harddisk, nettverk, lokal maskin og så videre) fra ekstern tilgang der en Java-applet kan kjøres med et brukerkontrollert sett med tillatelser.

