

## Guia Editar permissões

Especifica como você deseja que o Internet Explorer trate todo o conteúdo e as permissões solicitadas pelos miniaplicativos Java assinados e não assinados.

As seguintes permissões são afetadas pelas configurações das permissões não assinadas e assinadas:

[Acesso a todos os arquivos](#)

[Acesso a todos os endereços de rede](#)

[Diálogos](#)

[E/S de arquivo direcionado pelo usuário](#)

[Espaço de rascunho protegido](#)

[Executar](#)

[Impressão](#)

[Informações do sistema](#)

### Executar conteúdo não assinado

Você pode especificar as permissões individualmente, configurando **Executar conteúdo não assinado** como **Executar em modo seguro**. Depois você pode redefinir cada permissão individualmente como **Desativar** ou **Ativar**. Se você especificar **Desativar** ou **Ativar** em **Executar conteúdo não assinado**, todas as permissões em **Permissões não assinadas adicionais** usarão essa configuração.

Selecione uma das seguintes configurações para **Executar conteúdo não assinado**:

- Para executar o conteúdo não assinado com apenas as permissões que são permitidas na "[área de segurança](#)", clique em **Executar em modo seguro**. Se você proceder assim, poderá redefinir cada permissão individualmente como **Desativar** ou **Ativar**.
- Para recusar automaticamente o conteúdo não assinado sem ser consultado, clique em **Desativar**. Todas as permissões em **Permissões não assinadas adicionais** são definidas como **Desativar**; você não pode redefinir nenhuma permissão individualmente como **Ativar**.
- Para aceitar automaticamente o conteúdo não assinado sem ser consultado, clique em **Ativar**. Todas as permissões em **Permissões não assinadas adicionais** são definidas como **Ativar**; você não pode redefinir individualmente nenhuma permissão como **Desativar**.

### Executar conteúdo assinado

Você pode especificar individualmente as permissões, configurando **Executar conteúdo assinado** como **Prompt**, o que define todas as permissões em **Permissões assinadas adicionais** como **Prompt**. Depois, você pode redefinir cada permissão individualmente como **Desativar** ou **Ativar**. Se você especificar **Desativar** ou **Ativar**, todas as permissões em **Permissões assinadas adicionais** usarão essa configuração.

Selecione uma das seguintes configurações para **Executar conteúdo assinado**:

- Para ser consultado sobre sua aprovação antes que um miniaplicativo Java possa prosseguir com as permissões necessárias, clique em **Prompt**. Se você escolher **Prompt** em **Executar conteúdo assinado**, todas as permissões em **Permissões assinadas adicionais** são definidas como **Prompt**; entretanto você pode redefinir individualmente cada permissão como **Desativar** ou **Ativar**.
- Para recusar automaticamente a execução de conteúdo assinado sem ser consultado, clique em **Desativar**. Todas as permissões em **Permissões assinadas adicionais** são definidas como **Desativar**; você não pode redefinir individualmente nenhuma permissão como **Prompt** ou **Ativar**.
- Para aceitar automaticamente a execução de conteúdo assinado sem ser consultado, clique em **Ativar**. Todas as permissões em **Permissões assinadas adicionais** são definidas como **Ativar**; você não pode redefinir individualmente nenhuma permissão como **Prompt** ou **Desativar**.

Fecha essa caixa de diálogo e salva todas as alterações que você fez.

Clique aqui para redefinir todas as permissões Java. Selecione uma das seguintes opções e depois clique em **Redefinir**.

- **Permissões salvas** Redefine para as últimas permissões salvas conhecidas. Todas as alterações feitas desde as últimas configurações salvas serão perdidas.
- **Segurança alta** Redefine as permissões de alta segurança (as mais restritivas; os miniaplicativos são executados no modo seguro). Isso redefine todas as permissões em **Executar conteúdo assinado** como **Prompt** e **Permissões não assinadas adicionais** como **Desativar**.
- **Segurança média** Redefine as permissões de segurança média (os miniaplicativos são executados na área de segurança com duas permissões extras, que são: Espaço de rascunho e E/S de arquivo direcionado pelo usuário). Isso redefine todas as permissões (exceto Espaço de rascunho e E/S de arquivo direcionado pelo usuário) em **Executar conteúdo assinado** como **Prompt** e **Permissões não assinadas adicionais** como **Desativar**.
- **Segurança baixa** Redefine as permissões de segurança baixa (as menos restritiva; os miniaplicativos são executados com todas as permissões). Isso redefine todas as permissões em **Executar conteúdo assinado** como **Ativar** e **Permissões não assinadas adicionais** como **Desativar**.

## Guia Exibir Permissões

Essas permissões Java foram especificadas pelo administrador da sua rede.

Para que um miniaplicativo Java seja executado, ele pode requerer acesso aos arquivos e a outros recursos do seu computador. Estas ações requerem que permissões específicas sejam concedidas antes de serem executadas. O administrador da sua rede já pode ter especificado que permissões devem ser concedidas. Para as que são concedidas, o administrador da sua rede pode especificar se você deve ser notificado quando elas forem solicitadas. Senão, você só será notificado quando um miniaplicativo Java solicitar mais permissões do que as que são concedidas automaticamente.

Os três conjuntos de permissões são os seguintes:

**Permissões ativadas para conteúdo não assinado** Permissões concedidas a conteúdo não assinado do qual é feito o download (miniaplicativos serão executados na área de segurança).

**Permissões ativadas para conteúdo assinado** Permissões que não requerem a aprovação do usuário.

**Permissões desativadas para conteúdo assinado** Permissões que requerem a aprovação do usuário ou são totalmente negadas.

Você pode clicar duas vezes em cada um desses cabeçalhos da permissão para visualizar determinadas permissões e as configurações especificadas.

As seguintes permissões podem ser atribuídas a esses conjuntos:

Acesso à interface do usuário

Armazenamento de clientes

E/S de arquivo direcionado pelo usuário

E/S de arquivo

E/S de rede

Execução

Impressão

Informações do sistema

Multimídia

Personalizar

Propriedade

Reflexão

Registro

Segmentos

Segurança

Uma permissão que controla a leitura, gravação e acesso a arquivos para exclusão.

Uma permissão que controla a possibilidade de se executar operações de rede ou uma ação relacionada a rede.

Uma permissão que controla a possibilidade de se criar e processar segmentos e grupos de segmento.

Uma permissão que controla a possibilidade de se acessar ou manipular propriedades globais do sistema.



Uma permissão que controla a possibilidade de se executar outros programas.

Uma permissão que controla a possibilidade de se usar a API de reflexão para se obter acesso a membros de uma classe especial.

Uma permissão que controla o acesso às APIs de impressão.

Uma permissão que controla a possibilidade de se obter acesso ao Registro.

Uma permissão que controla o acesso às classes de segurança JDK, `java.lang.security`.

Uma permissão para controlar o acesso ao armazenamento no cliente que está disponível através da classe **Armazenamento de clientes**.

Uma permissão que controla a possibilidade de se usar algumas das funcionalidades aprimoradas de AWT.

Uma permissão que controla o acesso às informações do sistema.



Uma permissão que controla a possibilidade de se exibir caixas de diálogos de arquivo para executar operações de arquivo. Por exemplo, se um miniaplicativo precisar abrir um arquivo, ele deve apresentar a caixa de diálogo padrão **Arquivo Abrir** e, então, permitir que o usuário selecione o arquivo a ser aberto. O miniaplicativo não pode executar operações de arquivo por conta própria. Como resultado, essa operação é considerada mais segura do que o código ter acesso direto aos arquivos, uma vez que há o envolvimento direto do usuário. O nível dessa permissão é médio.

Uma permissão que controla o uso da funcionalidade de multimídia aprimorada.

Uma permissão que fornece controles precisos sobre os tipos de permissões que devem ser concedidas ao conteúdo assinado.

Uma permissão que controla a capacidade de o código assinado criar um espaço de rascunho de até 1MB que pode ser usado para armazenar informações temporárias. Um aplicativo não poderá ler ou gravar em qualquer outro arquivo na unidade de disco rígido do usuário. Um miniaplicativo assinado só pode acessar seu próprio espaço de rascunho. O nível dessa permissão é médio.

Uma permissão que controla a possibilidade de se apresentar caixas de diálogos.

Um ambiente para proteger certos recursos (por exemplo, sistema, disco rígido, rede, computador local, etc) de acesso externo onde um miniaplicativo Java pode ser executado com um conjunto de permissões controlado pelo usuário.

