

## Permissões solicitadas

O miniaplicativo Java requisitou as permissões que são exibidas na caixa de diálogo **Alerta de segurança**. Para que um miniaplicativo Java seja executado, ele pode requerer acesso aos arquivos e outros recursos do seu computador. Estas ações requerem permissões específicas para serem executadas. O administrador da sua rede pode já ter especificado as permissões que devem ser concedidas. O administrador de sua rede pode especificar se deve notificá-lo quando as permissões forem solicitadas. Senão, você só será notificado quando um miniaplicativo Java solicitar mais permissões do que as automaticamente concedidas.

Considerando o que você sabe do editor do software e as permissões que este programa está solicitando, você deve decidir se deve instalar e executar este miniaplicativo Java. Se você não se sentir à vontade fazendo isto, clique em **OK** na caixa de diálogo **Alerta de segurança** e depois clique em **Não** na caixa de diálogo **Aviso de segurança**.

Para obter mais informações sobre as seguintes permissões, clique na sua seleção:

[Armazenamento de clientes](#)

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

[E/S de arquivo](#)

[E/S de rede](#)

[E/S](#)

[Execução](#)

[Fluxos do sistema](#)

[Impressão](#)

[Multimídia](#)

[Personalizar](#)

[Propriedade](#)

[Reflexão](#)

[Registro](#)

[Segmentos](#)

[Segurança](#)

Para obter informações sobre a visualização das configurações de permissões em seu computador, consulte **Tópicos relacionados**.

---

{button ,AL("A\_IDH\_SEC\_ALERT\_VIEW\_JAVA\_CUSTOM\_SETTINGS")} [Tópicos relacionados](#)

Exibe o tipo de acesso que você está visualizando ou alterando. Você pode clicar em um tipo de acesso e depois especificar as configurações para aquele tipo de acesso.

Fornecer um espaço para que você digite o nome do arquivo a ser adicionado à lista de arquivos que têm um acesso especificado. Você pode digitar nomes de arquivos específicos ou pode usar curingas, como, por exemplo, \*.exe.

Lista os arquivos aos quais você permitirá o acesso especificado.

Adiciona o item à lista que será incluída nessas permissões.

Remove o item selecionado da lista.

Fornece um espaço para que você digite o nome do arquivo a ser excluído da lista de arquivos que têm um acesso especificado.

Lista os nomes dos arquivos aos quais você não permitirá o acesso especificado.



Especifica se você permitirá o acesso à base de código de um URL de arquivo.

Exibe o tipo de acesso que você está visualizando ou alterando.

Fornecer um espaço para que você digite uma entrada de registro a ser adicionada à lista de entradas de registro que têm um acesso especificado.

Lista as entradas do registro às quais você permitirá o acesso especificado.

Fornece um espaço para que você digite uma entrada de registro a ser excluída da lista de entradas de registro às quais você permitirá o acesso especificado.

Lista as entradas de registro às quais você não permitirá o acesso especificado.

Especifica se deve ser permitido que miniaplicativos Java criem caixas de diálogo.

Especifica se deve ser permitido que miniaplicativos Java criem uma janela de nível superior.



Especifica se deve ser exibido um aviso quando um miniaplicativo Java pedir para criar uma janela de nível superior.

Especifica se deve ser permitido que um miniaplicativo Java use a **Área de transferência** do computador para cortar, copiar ou colar informações.

Especifica que deve ser concedido aos miniaplicativos Java acesso irrestrito às propriedades do sistema.

Permite o acesso às propriedades do sistema e sufixos que você especificar, nega o acesso às propriedades do sistema que você excluir.

Fornecer um espaço para que você digite os sufixos aos quais você permite que os miniaplicativos Java tenham acesso.

Fornecer um espaço para que você digite as propriedades do sistema às quais você permite que os aplicativos Java tenham acesso.

Fornecer um espaço para que você digite as propriedades do sistema às quais você não deseja que os aplicativos Java tenham acesso.

Especifica se deve ser permitido um tipo de carregador que tenha sido associado a este objeto de permissão pública.



Especifica se deve ser permitido um tipo de carregador que se refira a qualquer carregador diferente daquele associado a este objeto de permissão pública.

Especifica se deve ser permitido um tipo de carregador que se refira a classes do sistema público.

Especifica se deve ser permitido um tipo de carregador que tenha sido associado a esse objeto de permissão.

Especifica se deve ser permitido um tipo de carregador que se refira a qualquer outro diferente daquele associado a esse objeto de permissão.

Especifica se deve ser permitido um tipo de carregador que se refira a classes declaradas do sistema.

Especifica se deve ser permitido que os miniaaplicativos Java leiam arquivos, se o usuário o permitir.

Especifica se deve ser permitido que os miniaplicativos Java gravem nos arquivos, se o usuário o permitir.

Especifica quanto espaço de armazenamento no computador do usuário deve ser permitido que os miniaplicativos usem.



Especifica se deve ser permitido que miniaplicativos Java ignorem limites de armazenamento especificados pelo usuário para todos os arquivos de Internet.

Especifica se arquivos ambulantes podem ser criados. Os arquivos ambulantes são criados no perfil do usuário e estão presentes em qualquer computador a que o usuário esteja conectado.

Especifica se os aplicativos definidos em **Permitir execução** podem ser executados.

Especifica que programas podem ser executados.

Especifica que programas não podem ser executados.

Especifica se deve ser permitido acesso irrestrito ao segmento.

Especifica se deve ser permitido acesso irrestrito ao grupo de segmentos.

Especifica se o objeto de permissão permite que o fluxo System.in seja configurado.



Especifica se o objeto de permissão permite que o fluxo System.out seja configurado.

Especifica se o objeto de permissão permite que o fluxo System.err seja configurado.

Especifica se as classes que possuem a `PrintingPermission` poderão usar os serviços de impressão.

Especifica se deve ser permitido o acesso aos aspectos estendidos das APIs de Microsoft DirectX.

Especifica se deve ser permitido o acesso às classes de segurança JDK, `java.lang.security`.

Exibe o tipo de comunicação que você está visualizando ou alterando. A tabela a seguir mostra tipos de comunicações e as configurações disponíveis para as mesmas.

**Para especificar as configurações para isto**

Comunicação geral para hosts específicos

Conexões em interfaces e portas específicas

Ingressar em grupos específicos de difusão limitada

Configurações que substituem quaisquer regras de porta individual

**Clique aqui**

**Conectar endereços**

**Acoplar endereços**

**Endereços de difusão limitada**

**Portas globais**

Fornece espaços para que você digite um host e porta que se deseja adicionar à lista de hosts e portas com os quais você permite a comunicação especificada.

Lista os hosts e portas com os quais você permitirá a comunicação especificada.



Fornece espaços para que você digite um host e porta para excluir da lista de hosts e portas com as quais você permite a comunicação especificada.

Lista os hosts e portas com os quais você não permitirá a comunicação especificada.

Especifica se você deseja se conectar ao URL de um arquivo.

Especifica se você deseja se conectar a um URL que não é de um arquivo.

Fornece espaços para que você digite o nome e dados das permissões que você deseja adicionar à lista de configurações de permissões personalizadas.

Lista o nome e dados das configurações de permissões personalizadas que você adicionou.

Clique aqui para definir o nível de segurança como **Alto (mais seguro)**.

Clique aqui para definir o nível de segurança como **Médio**.



### Para visualizar configurações personalizadas

As permissões são definidas pelo administrador de rede através do Internet Explorer Administration Kit. Normalmente você não pode editar essas configurações, mas pode visualizá-las. Proceda desta forma com as seguintes etapas.

- 1 Clique com o botão direito do mouse no ícone **Internet**, na sua área de trabalho, e depois clique em **Propriedades**.
- 2 Clique na guia **Segurança** e depois clique em **Personalizar**.
- 3 Na lista **Configurações**, sob **Java**, clique em **Personalizar**.
- 4 Clique no botão **Configurações personalizadas do Java** na parte inferior da caixa de diálogo.

### Observações

- Se o botão **Editar** aparecer na parte inferior da caixa de diálogo **Configurações do Java**, você poderá alterar as configurações.
- Se o botão **Editar** não aparecer e você precisar alterar as configurações, entre em contato com o seu administrador de rede.

---

{button ,AL("A\_IDH\_SEC\_ALERT\_MORE\_INFO")} [Tópicos relacionados](#)

Fecha esta caixa de diálogo e salva todas as alterações efetuadas.

Fecha esta caixa de diálogo sem salvar nenhuma alteração efetuada.

### **Caixa de diálogo Editor de zona**

Dentro desta zona, você pode atribuir permissões a **Não assinado**, **Permissão sem aviso** e **Consultado/Negado**. Qualquer permissão que não for atribuída a **Não assinado** ou **Permitido sem aviso**, é atribuída a **Consultado/Negado**.

Dentro das permissões atribuídas a **Consultado/Negado**, você pode atribuir permissões específicas a **Consultado**. Qualquer permissão restante é atribuída a **Negado**. Como alternativa, você pode atribuir permissões específicas a **Negado**, e qualquer permissão restante é atribuída a **Consultado**.

Se você deseja conceder automaticamente as permissões sem ter que abrir a caixa de diálogo correspondente e ativar todas as permissões, você pode selecionar **Permitir todo o conjunto de permissões**.

## **Caixa de diálogo Personalizar permissões**

Esta caixa de diálogo exibe que permissões de Java foram especificadas pelo seu administrador de rede.

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

Cada uma das seguintes guias representa um tipo de conjunto de permissões:

| <b>Guia</b>                | <b>Permissões</b>  |
|----------------------------|--|
| <b>Não assinado</b>        | Concedidas a conteúdo não assinado com download feito        |
| <b>Permissão sem aviso</b> | Não requerem aprovação do usuário                            |
| <b>Consultado/Negado</b>   | Requerem a aprovação do usuário ou são absolutamente negadas |

As seguintes permissões podem ser atribuídas a estas guias:

Armazenamento de clientes

E/S de arquivo direcionado pelo usuário

E/S de arquivo

E/S de rede

E/S

Execução

Fluxos do sistema

Impressão

Multimídia

Personalizar

Propriedade

Reflexão

Registro

Segmentos

Segurança

### **Guia Arquivo de E/S**

Use esta guia para especificar os arquivos e tipos de arquivos que você aceitará no conjunto de permissões desta zona. Por padrão, todos os arquivos estão excluídos, você não precisa especificar os arquivos a excluir, a não ser que sejam um subconjunto dos arquivos que você está incluindo. Por exemplo, se você incluir um arquivo de multimídia do tipo (\*.avi), você pode excluir um arquivo específico desse tipo (Meu\_arquivo.avi). Você pode especificar diferentes permissões para diferentes tipos de acesso: Ler, Gravar e Excluir.

### **Observação**

- A **Ajuda** está disponível para cada configuração nesta caixa de diálogo. Selecione ou clique na configuração ou no botão sobre o qual você deseja obter informações e depois pressione F1.

## **Guia Registro**

Use esta guia para especificar as entradas do Registro que você aceitará nesse conjunto de permissões para esta zona. Por padrão, todas as entradas do Registro estão excluídas, você não precisa especificar as entradas do Registro a excluir, a não ser que sejam um subconjunto das entradas do Registro que você está incluindo. Por exemplo, se você incluir HKEY\_CURRENT\_USER, você pode excluir uma categoria do Registro específica sob a entrada (HKEY\_CURRENT\_USER\NETWORK). Você pode especificar diferentes permissões para diferentes tipos de acesso: Ler, Gravar, Excluir, Abrir e Criar.

### **Observação**

- A **Ajuda** está disponível para cada configuração nesta caixa de diálogo. Selecione ou clique na configuração ou no botão sobre o qual você deseja obter informações e depois pressione F1.

## Guia UI

Use esta guia para especificar as permissões para algumas das ações mais comuns que um miniaplicativo Java pode solicitar no computador de um usuário, como criar uma janela ou caixa de diálogo, acessar propriedades do sistema (como, por exemplo, arquivos .ini) ou verificar informações para determinar como são estruturadas de forma que o miniaplicativo possa consultar as informações. Estas permissões podem estar listadas nas configurações personalizadas do Java do usuário ou em uma caixa de diálogo **Aviso de segurança**, quando um miniaplicativo Java solicita permissões que excedem àquelas concedidas automaticamente.

### Observação

- A **Ajuda** está disponível para cada configuração nesta caixa de diálogo. Selecione ou clique na configuração ou no botão sobre o qual você deseja obter informações e depois pressione F1.



### **Guia Diversos**

Use esta guia para especificar permissões para leitura, gravação e armazenamento de arquivos e execução de programas, segmentos e outras permissões. Estas permissões podem estar listadas nas configurações personalizadas do Java do usuário ou em uma caixa de diálogo **Aviso de segurança**, quando um miniaplicativo Java solicita permissões que excedem àquelas consentidas automaticamente.

### **Observação**

- A **Ajuda** está disponível para cada configuração nesta caixa de diálogo. Selecione ou clique na configuração ou no botão sobre o qual você deseja obter informações e depois pressione F1.

## **Guia Net IO**

Use esta guia para especificar o tipo de conexões que você permitirá e com que hosts e portas. Por padrão, todos os hosts e portas estão excluídos, você não precisa especificar os hosts e portas a excluir, a não ser que sejam um subconjunto dos hosts e portas que você está incluindo. Você pode especificar diferentes permissões para diferentes tipos de conexões: Conectar endereços, Acoplar endereços, Endereços de difusão limitada e Portas globais.

### **Observação**

- A **Ajuda** está disponível para cada configuração nesta caixa de diálogo. Selecione ou clique na configuração ou no botão sobre o qual você deseja obter informações e depois pressione F1.

### **Guia Personalizar**

Use esta guia para especificar as configurações de **Personalizar permissão** pelo nome ou tipo de dados.

#### **Observação**

- A **Ajuda** está disponível para cada configuração nesta caixa de diálogo. Selecione ou clique na configuração ou no botão sobre o qual você deseja obter informações e depois pressione F1.

Um pedido ou permissão para acessar ou controlar o acesso aos arquivos.

Um pedido ou permissão para efetuar operações de rede ou uma ação relativa à rede.

Uma permissão que controla a habilidade de criar e manipular segmentos e grupos de segmento.

Um pedido ou permissão para acessar ou manipular propriedades globais do sistema.

Um pedido ou permissão para controlar ou executar outros programas.



Um pedido ou permissão para efetuar operações de reflexão ou usar APIs de reflexão para ter acesso aos membros de uma classe especificada.

Uma permissão que controla o acesso às APIs de impressão.

Uma permissão que controla a habilidade de obter acesso ao Registro ou um pedido para acessar uma chave do Registro.

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

Uma permissão que controla a habilidade do código assinado de criar espaço de rascunho de até 1 MB, através do `ClientStoragePermission`, que pode ser usado para armazenar informações temporárias. A um miniaplicativo Java não será permitido ler ou escrever em quaisquer outros arquivos no disco rígido do usuário. Um miniaplicativo assinado somente pode acessar seu próprio espaço de rascunho. O nível desta permissão é médio.

Um pedido para usar um aspecto estendido das APIs da interface do usuário. Também uma permissão que controla a habilidade de usar parte da funcionalidade avançada do Application Windowing Toolkit (AWT).

Uma permissão que controla a habilidade de alterar os valores dos fluxos de sistema **java.lang.System.in**, **java.lang.System.out** e **java.lang.System.err**.

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 para aceitar o uso de uma funcionalidade de multimídia avançada.

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

