Separador Editar permissões

Especifica o modo como pretende que o Internet Explorer lide com todo o conteúdo e permissões pedidas por aplicações de Java assinadas e não assinadas.

As permissões que se seguem são afectadas pelas definições atribuídas a permissões não assinadas e assinadas:

Access to all Files

Access to all Network Addresses

Execute

Dialogs

System Information

Printing

Protected Scratch Space

User Directed File I/O

Executar conteúdo não assinado

Poderá especificar permissões individualmente definindo **Executar conteúdo não assinado** para **Executar em sandbox**. Em seguida, poderá repor cada uma das permissões individualmente para **Desactivar** ou **Activar**. Se especificar **Desactivar** ou **Activar** em **Executar conteúdo não assinado**, todas as permissões contidas em **Permissões não assinadas adicionais** utilizarão essa definição.

Seleccione uma das seguintes definições para **Executar conteúdo não assinado**:

- Para executar conteúdo não assinado apenas com as permissões permitidas em "sandbox," faça clique sobre **Executar em sandbox**. Se seleccionar, poderá repor cada uma das permissões individualmente para **Desactivar** ou **Activar**.
- Para recusar automaticamente conteúdo não assinado sem que lhe seja perguntado nada, faça clique sobre **Desactivar**. Todas as permissões contidas em **Permissões não assinadas adicionais** serão definidas para **Desactivar**; não pode repor nenhuma das permissões individualmente para **Activar**.
- Para aceitar automaticamente conteúdo não assinado sem que lhe seja perguntado nada, faça clique sobre **Activar**. Todas as permissões contidas em **Permissões não assinadas adicionais** serão definidas para **Activar**; não pode repor nenhuma das permissões individualmente para **Desactivar**.

Executar conteúdo assinado

Poderá especificar permissões individualmente definindo **Executar conteúdo assinado** para **Pedir**, procedimento que definirá todas as permissões contidas em **Permissões assinadas adicionais** para **Pedir**. Em seguida, poderá repor cada uma das permissões individualmente para **Desactivar** ou **Activar**. Se especificar **Desactivar** ou **Activar**, todas as permissões contidas em **Permissões assinadas adicionais** utilizarão essa definição.

Seleccione uma das seguintes definições para **Executar conteúdo assinado**:

- Para que seja pedida a sua aprovação antes de prosseguir uma aplicação de Java com as respectivas permissões solicitadas, faça clique sobre **Pedir**. Se seleccionar **Pedir** para **Executar conteúdo assinado**, todas as permissões contidas em **Permissões assinadas adicionais** serão definidas para **Pedir**; no entanto, pode repor cada uma das permissões individualmente para **Desactivar** ou **Activar**.
- Para recusar automaticamente a execução de conteúdo assinado sem que lhe seja perguntado nada, faça clique sobre **Desactivar**. Todas as permissões contidas em **Permissões assinadas adicionais** serão definidas para **Desactivar**; não pode repor nenhuma das permissões individualmente para **Pedir** ou **Activar**.
- Para aceitar automaticamente a execução de conteúdo assinado sem que lhe seja perguntado nada, faça clique sobre **Activar**. Todas as permissões contidas em **Permissões assinadas adicionais** serão definidas para **Activar**; não pode repor nenhuma das permissões individualmente para **Pedir** ou **Desactivar**.

Fecha esta caixa de diálogo e guarda todas as alterações entretanto efectuadas.

Faça clique aqui para repor todas as permissões de Java. Seleccione um dos itens que se seguem e, em seguida, faça clique sobre **Repor**.

- **Permissões guardadas** Repõe as permissões tal como estas foram guardadas pela última vez. Todas as alterações efectuadas depois disso serão perdidas.
- **Segurança alta** Repõe as permissões para **Segurança alta** (estado mais restritivo; as aplicações são executadas em modo seguro). Este procedimento irá repor todas as permissões contidas em **Executar conteúdo assinado** para **Pedir** e as de **Permissões não assinadas adicionais** para **Desactivar**.
- **Segurança média** Repõe as permissões para **Segurança média** (as aplicações são executadas em "sandbox" com duas permissões adicionais, nomeadamente, Scratch Space e User Directed File I/O). Este procedimento irá repor todas as permissões (à excepção de Scratch Space e User Directed File I/O) contidas em **Executar conteúdo assinado** para **Pedir** e as de **Permissões não assinadas adicionais** para **Desactivar**.
- **Segurança baixa** Repõe as permissões para **Segurança baixa** (estado menos restritivo; as aplicações são executadas com todas as permissões). Este procedimento irá repor todas as permissões contidas em **Executar conteúdo assinado** para **Activar** e as de **Permissões não assinadas adicionais** para **Desactivar**.

Separador Ver permissões

Estas permissões de Java foram especificadas pelo administrador da rede.

Para que seja possível a execução de uma aplicação de Java, poderá ser necessário o acesso a ficheiros e outros recursos existentes no computador. Estas acções requerem permissões específicas que deverão ser concedidas antes da execução das acções. O administrador da rede pode já ter especificado as permissões que deverão ser concedidas. No que diz respeito às que são permitidas, o administrador da rede pode especificar se o utilizador deverá ou não ser notificado sempre que forem solicitadas. Caso contrário, o utilizador só será notificado quando uma aplicação de Java solicitar mais permissões do que as que são automaticamente concedidas.

Seguem-se as três categorias de permissões:

Permissões activadas para conteúdo não assinado Permissões concedidas a conteúdo transferido não assinado (as aplicações serão executadas em “sandbox”).

Permissões activadas para conteúdo assinado Permissões que não requerem a aprovação do utilizador.

Permissões desactivadas para conteúdo assinado Permissões que requerem a aprovação do utilizador ou que são absolutamente recusadas.

Pode fazer duplo clique sobre cada um dos títulos destas permissões para ver as permissões e definições específicas indicadas.

Poderão ser atribuídas as seguintes permissões às categorias anteriormente mencionadas:

Client Storage

Custom

Execution

File I/O

Multimedia

Net I/O

Printing

Property

Reflection

Registry

Security

System Information

Threads

User Directed File I/O

User Interface Access

Uma permissão que controla o acesso de leitura, escrita e eliminação a ficheiros.

Uma permissão que controla a capacidade de executar operações de rede ou uma acção relacionada com a rede.

Uma permissão que controla a capacidade de criar e manipular threads e grupos de thread.

Uma permissão que controla a capacidade de aceder ou manipular propriedades de sistema globais.

Uma permissão que controla a capacidade de executar outros programas.

Uma permissão que controla a capacidade de utilizar a API de reflexão para obter acesso a membros de uma classe especificada.

Uma permissão que controla o acesso às API de impressão.

Uma permissão que controla a capacidade de obter acesso ao registo.

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

Uma permissão para controlar o acesso ao armazenamento do cliente disponível através da classe **ClientStore**.

Uma permissão que controla a capacidade de utilizar alguma da funcionalidade avançada do AWT.

Uma permissão que controla o acesso ao sistema de informações.

Uma permissão que controla a capacidade de mostrar caixas de diálogo de ficheiro para a execução de operações relacionadas com ficheiros. Por exemplo, se a aplicação necessitar de abrir um ficheiro, deverá ser apresentada a caixa de diálogo padrão **Abrir ficheiro**, de modo a permitir ao utilizador seleccionar o ficheiro a abrir. A aplicação não poderá executar operações relacionadas com ficheiros por si só. Como resultado, esta operação é considerada como sendo mais segura do que a utilização de um código com acesso directo ao ficheiro uma vez que pressupõe o envolvimento directo por parte do utilizador. Este nível de permissão corresponde ao médio.

Uma permissão que controla a utilização de funcionalidade de multimédia avançada.

Uma permissão que fornece controlos exactos sobre o tipo de permissões a conceder a conteúdo assinado.

Uma permissão que controla a capacidade para o código assinado de criar até 1 MB de área de trabalho que poderá ser utilizada para armazenar informações temporárias. Uma aplicação de Java não terá permissão para ler ou escrever noutros ficheiros contidos no disco rígido do utilizador. Uma aplicação assinada só poderá aceder à sua própria área de trabalho. Este nível de permissão corresponde ao médio.

Uma permissão que controla a capacidade de apresentar caixas de diálogo.

Um ambiente para proteger determinados recursos (por exemplo, o sistema, o disco rígido, a rede, o computador local, etc.) contra o acesso do exterior em que uma aplicação de Java pode ser executada com uma categoria de permissões controlada pelo utilizador.