Ficha Editar permisos

Especifica cómo desea que Internet Explorer trate el contenido y los permisos que solicitan los subprogramas Java firmados y sin firmar.

La configuración de Permisos firmados y Permisos sin firmar afecta a los siguientes permisos:

Archivo E/S directo del usuario

Diálogos

Ejecutar

Espacio temporal protegido

Impresión

Información del sistema

Tener acceso a todas las direcciones de red

Tener acceso a todos los archivos

Ejecutar el contenido sin firmar

Para especificar permisos individualmente, asigne a la opción **Ejecutar el contenido sin firmar** el valor **Ejecutar en el recinto de seguridad**. A continuación puede restablecer cada permiso individualmente a **Desactivar** o **Activar**. Si especifica **Desactivar** o **Activar** bajo **Ejecutar el contenido sin firmar**, todos los permisos que aparecen debajo de **Permisos adicionales sin firmar** usarán el valor especificado.

Seleccione una de las siguientes opciones en **Ejecutar el contenido sin firmar**:

- Para ejecutar contenido sin firmar sólo con los permisos permitidos en el "recinto de seguridad", haga clic en **Ejecutar en el recinto de seguridad**. Si lo hace, puede restablecer cada permiso individualmente a **Desactivar** o **Activar**.
- Para denegar automáticamente el contenido sin firmar sin preguntarle, haga clic en **Desactivar**. Todos los permisos que aparecen debajo de **Permisos adicionales sin firmar** se establecen a **Desactivar**; no podrá restablecer ningún permiso individualmente a **Activar**.
- Para aceptar automáticamente el contenido sin firmar sin preguntarle, haga clic en **Activar**. Todos los permisos que aparecen debajo de **Permisos adicionales sin firmar** se establecen a **Activar**; no podrá restablecer ningún permiso individualmente a **Desactivar**.

Ejecutar el contenido firmado

Para especificar permisos individualmente, asigne a la opción **Ejecutar el contenido firmado** el valor **Preguntar al usuario**, que establece a **Preguntar al usuario** todos los permisos que aparecen debajo de **Permisos firmados adicionales**. A continuación puede restablecer cada permiso individualmente a **Desactivar** o **Activar**. Si especifica **Desactivar** o **Activar**, todos los permisos que aparecen debajo de **Permisos firmados adicionales** usarán el valor especificado.

Seleccione una de las siguientes opciones para **Ejecutar el contenido firmado**:

- Para pedir confirmación al usuario antes de que un subprograma de Java pueda continuar con sus permisos solicitados, haga clic en **Preguntar al usuario**. Si elige **Preguntar al usuario** para **Ejecutar el contenido firmado**, todos los permisos que aparecen debajo de **Permisos firmados adicionales** se establecen a **Preguntar al usuario**; no obstante, puede restablecer cada permiso individualmente a **Desactivar** o **Activar**.
- Para denegar automáticamente la ejecución del contenido firmado sin preguntarle, haga clic en **Desactivar**. Todos los permisos que aparecen debajo de **Permisos firmados adicionales** se establecen a **Desactivar**; no podrá restablecer ningún permiso individualmente a **Preguntar al usuario** o **Activar**.
- Para aceptar automáticamente la ejecución del contenido firmado sin preguntarle, haga clic en **Activar**. Todos los permisos que aparecen debajo de **Permisos firmados adicionales** se establecen a **Activar**; no podrá restablecer ningún permiso individualmente a **Preguntar al usuario** o **Desactivar**.

Cierra este cuadro de diálogo y guarda todos los cambios que ha realizado.

Haga clic aquí para restablecer todos los permisos de Java. Seleccione una de las siguientes opciones y haga clic en **Restablecer**.

- **Permisos guardados** Restablece los últimos permisos guardados conocidos. Se perderán todos los cambios realizados desde la última vez que se guardaron los valores.
- **Alta seguridad** Restablece los permisos a alta seguridad (son los permisos más restrictivos y los subprogramas se ejecutan en modo seguro). Restablece a **Preguntar al usuario** todos permisos que aparecen debajo de **Ejecutar el contenido firmado** y a **Desactivar** los que aparecen bajo **Permisos adicionales sin firmar**.
- **Media seguridad** Restablece los permisos a seguridad media (los subprogramas se ejecutan en el recinto de seguridad con dos permisos adicionales, Scratch Space y User Directed File I/O). Restablece a **Preguntar al usuario** todos los permisos (excepto Scratch Space y User Directed File I/O) que aparecen debajo de **Ejecutar el contenido firmado** y a **Desactivar** los que aparecen bajo **Permisos adicionales sin firmar**.
- **Baja seguridad** Restablece los permisos a baja seguridad (son los permisos menos restrictivos y los subprogramas se ejecutan con todos los permisos). Restablece a **Activar** todos los permisos que aparecen debajo de **Ejecutar el contenido firmado** y a **Desactivar** los que aparecen bajo **Permisos adicionales sin firmar**.

Ficha Permisos de lectura

Estos permisos Java son los especificados por el administrador de red.

Para que se ejecute un subprograma Java, puede requerir el acceso a archivos y otros recursos del equipo. Estas acciones requieren la concesión de permisos específicos para que se puedan llevar a cabo. Es posible que el administrador de red ya haya especificado los permisos permitidos. Además, el administrador de red puede especificar si se le va a notificar cuando se soliciten dichos permisos. Si no lo hace, sólo se le notificará cuando un subprograma Java solicite más permisos que los permitidos automáticamente.

Hay tres grupos de permisos:

Permisos activados para contenido sin firmar Permisos concedidos a contenido descargado sin firma (los subprogramas se ejecutarán en el recinto de seguridad).

Permisos activados para contenido firmado Permisos que no requieren aprobación por parte del usuario.

Permisos desactivados para contenido firmado Permisos que requieren aprobación por parte del usuario o totalmente denegados.

Puede hacer doble clic en cada tipo de permisos que se muestran a continuación para ver los permisos concretos y la configuración especificada.

Los siguientes permisos se pueden asignar a los grupos descritos anteriormente:

Client Storage (Almacenamiento del cliente)

Custom (Personalizadas)

Execution (Ejecutar)

File I/O (Acceso E/S a todos los archivos)

Multimedia

Net I/O (Acceso E/S a todas las direcciones de red)

Printing (Impresión)

Property (Propiedad)

Reflection (Reflexión)

Registry (Registro)

Security (Seguridad)

System Information (Información del sistema)

Threads (Subprocesos)

User Directed File IO (Archivo E/S directo del usuario)

User Interface Access (Acceso a la interfaz de usuario)

Permiso que controla el acceso de lectura, escritura y eliminación de archivos.

Permiso que controla la capacidad para realizar operaciones de red o una acción relacionada con la red.

Permiso que controla la capacidad para crear y manipular subprocesos y grupos de subprocesos.

Permiso que controla la capacidad para tener acceso o manipular las propiedades globales del sistema.

Permiso que controla la capacidad para ejecutar otros programas.

Permiso que controla la capacidad para usar las API de reflexión para obtener acceso a los miembros de una determinada clase.

Permiso que controla el acceso a las API de impresión.

Permiso que controla la capacidad para obtener acceso al registro.

Permiso que controla el acceso a las clases de seguridad JDK, **java.lang.security**.

Permiso que controla el acceso al almacenamiento del cliente disponible mediante la clase **ClientStore**.

Permiso que controla la capacidad para usar la funcionalidad mejorada de AWT.

Permiso que controla el acceso a información del sistema.

Permiso que controla la capacidad para mostrar cuadros de diálogo de archivos para realizar operaciones de archivos. Por ejemplo, si un subprograma necesita abrir un archivo debe mostrar el cuadro de diálogo estándar Abrir archivo y permitir al usuario seleccionar el archivo que se va a abrir. El subprograma no puede realizar por sí mismo operaciones de archivos. Por tanto, esta operación se considera más segura que el código con acceso directo a archivos, ya que existe participación directa del usuario. Este nivel de permiso es Medio.

Permiso que controla el uso de la funcionalidad multimedia mejorada.

Permiso que proporciona controles precisos sobre el tipo de permisos que se van a conceder para el contenido firmado.

Permiso que controla la capacidad para que el código formado cree un espacio de borrador de hasta 1 MB que se puede usar para almacenar información temporal. Un subprograma Java no podrá leer ni escribir en otros archivos del disco duro del usuario. Un subprograma firmado sólo puede tener acceso a su propio espacio de borrador. Este nivel de permiso es Medio.

Permiso que controla la capacidad para mostrar cuadros de diálogo.

Entorno para proteger ciertos recursos (por ejemplo, sistema, disco duro, red, equipo local, etc.) frente al acceso exterior cuando un subprograma Java puede ejecutarse con un conjunto de permisos controlados por el usuario.