

Onglet Autorisations d'édition

Indique de quelle façon vous souhaitez voir Internet Explorer gérer les contenus et les autorisations demandées par les mini-applications Java signées et non signées.

Les autorisations suivantes sont affectées par les paramètres des autorisations non signées et signées :

[Access to all Files](#)

[Access to all Network Addresses](#)

[Execution](#)

[Dialogs](#)

[System Information](#)

[Printing](#)

[Protected Scratch Space](#)

[User Directed File I/O](#)

Exécution d'un contenu non signé

Vous pouvez spécifier des autorisations individuelles en choisissant **Exécuter en sandbox** pour **Exécuter le contenu non signé**. Dès lors, vous pouvez rétablir chaque autorisation individuelle à **Désactiver** ou **Activer**. Si vous spécifiez **Désactiver** ou **Activer** dans **Exécuter le contenu non signé**, toutes les autorisations contenues dans **Autorisations non signées complémentaires** utiliseront ce paramètre.

Sélectionnez l'un des paramètres suivants pour **Exécuter le contenu non signé** :

- Pour exécuter le contenu non signé à l'aide uniquement des autorisations données dans la "[sandbox](#)", cliquez sur **Exécuter en sandbox**. Si vous choisissez **Exécuter en sandbox** pour **Exécuter le contenu non signé**, vous pouvez rétablir chaque autorisation individuelle à **Désactiver** ou **Activer**.
- Pour refuser automatiquement tout contenu non signé sans en être averti, cliquez sur **Désactiver**. Toutes les autorisations contenues dans **Autorisations non signées complémentaires** correspondent à **Désactiver** et vous ne pouvez rétablir les autorisations individuelles à **Activer**.
- Pour accepter automatiquement tout contenu signé sans en être averti, cliquez sur **Activer**. Toutes les autorisations contenues dans **Autorisations non signées complémentaires** correspondent à **Activer** et vous ne pouvez rétablir les autorisations individuelles à **Désactiver**.

Exécution d'un contenu signé

Vous pouvez spécifier des autorisations individuelles en choisissant **Demander** pour **Exécuter le contenu signé**, ce qui permet d'affecter **Demander** à toutes les autorisations contenues dans **Autorisations signées complémentaires**. Dès lors, vous pouvez rétablir chaque autorisation individuelle à **Désactiver** ou **Activer**. Si vous spécifiez **Désactiver** ou **Activer**, toutes les autorisations contenues dans **Autorisations signées complémentaires** utiliseront ce paramètre.

Sélectionnez l'un des choix suivants pour **Exécuter le contenu signé** :

- Pour recevoir une demande d'approbation avant qu'une mini-application Java continue avec ses autorisations demandées, cliquez sur **Demander**. Si vous choisissez **Demander** pour **Exécuter le contenu signé**, toutes les autorisations contenues dans **Autorisations signées complémentaires** correspondent à **Demander**, mais vous pouvez rétablir chaque autorisation individuelle à **Désactiver** ou **Activer**.
- Pour refuser automatiquement l'exécution de tout contenu signé sans en être averti, cliquez sur **Désactiver**. Toutes les autorisations contenues dans **Autorisations signées complémentaires** correspondent à **Désactiver** mais vous ne pouvez rétablir chaque autorisation individuelle à **Demander** ou **Activer**.
- Pour accepter automatiquement l'exécution de tout contenu signé sans en être averti, cliquez sur **Activer**. Toutes les autorisations contenues dans **Autorisations signées complémentaires** correspondent à **Activer** et vous ne pouvez rétablir les autorisations individuelles à **Demander** ou **Désactiver**.

Ferme la boîte de dialogue et enregistre les changements effectués.

Cliquez dessus pour rétablir toutes les autorisations Java. Sélectionnez l'un des choix suivants, puis cliquez sur **Rétablir**.

- **Autorisations enregistrées** Rétablit les dernières autorisations enregistrées connues. Toutes les modifications apportées depuis le dernier enregistrement des paramètres seront perdues.
- **Haute sécurité** Rétablit les autorisations de haute sécurité (les plus restrictives ; les mini-applications s'exécutent en mode sans échec). Cela permet de rétablir toutes les autorisations contenues dans **Exécuter le contenu signé** à **Demander** et toutes celles contenues dans **Autorisations non signées complémentaires** à **Désactiver**.
- **Sécurité moyenne** Rétablit les autorisations de sécurité moyenne (les mini-applications s'exécutent dans la sandbox avec deux autorisations supplémentaires ; Espace Scratch et Accès utilisateur au fichier sélectionné). Cela permet de rétablir toutes les autorisations (sauf Espace Scratch et Accès utilisateur au fichier sélectionné) contenues dans **Exécuter le contenu signé** à **Demander** et toutes celles contenues dans **Autorisations non signées complémentaires** à **Désactiver**.
- **Basse sécurité** Rétablit les autorisations de basse sécurité (les moins restrictives ; les mini-applications s'exécutent avec toutes les autorisations). Cela permet de rétablir toutes les autorisations contenues dans **Exécuter le contenu signé** à **Activer** et toutes celles contenues dans **Autorisations non signées complémentaires** à **Désactiver**.

Onglet Afficher les autorisations

Ces autorisations Java ont été spécifiées par votre administrateur réseau.

Pour permettre à une mini-application Java de s'exécuter, il lui est parfois nécessaire d'accéder à des fichiers ou des ressources de votre ordinateur. Ces actions nécessitent que des autorisations spécifiques soient accordées avant que l'action ne soit réalisée. Il se peut que votre administrateur réseau ait déjà spécifié les autorisations accordées. Lorsque les autorisations sont accordées, votre administrateur réseau peut vous en avertir, ou non, au moment où ces autorisations sont requises. Dans le cas contraire, vous ne serez averti que lorsqu'une mini-application Java demandera des autorisations dépassant celles qui lui sont accordées automatiquement.

Il existe trois ensembles d'autorisations :

Permissions Enabled for Unsigned Content Autorisations accordées au contenu téléchargé non signé (les mini-applications seront exécutées en sandbox).

Permissions Enabled for Signed Content Autorisations ne nécessitant pas l'approbation de l'utilisateur.

Permissions Disabled for Signed Content Autorisations nécessitant l'approbation de l'utilisateur ou catégoriquement refusées.

Vous pouvez double-cliquer sur chacun des titres d'autorisations pour afficher les autorisations et les paramètres correspondants.

Les autorisations suivantes peuvent être assignées à ces ensembles :

[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](#)

Autorisation contrôlant l'accès en lecture, écriture et suppression des fichiers.

Autorisation contrôlant la réalisation de plusieurs opérations ou d'une action liées au réseau.

Autorisation contrôlant la création et la manipulation des threads ou des groupes de thread.

Autorisation contrôlant l'accès ou la manipulation des propriétés globales du système.

Autorisation contrôlant l'exécution des autres programmes.

Autorisation contrôlant l'utilisation de l'API Réflexion pour accéder aux membres d'une classe spécifiée.

Autorisation contrôlant l'accès aux API d'impression.

Autorisation contrôlant l'accès au registre.

Autorisation contrôlant l'accès aux classes de sécurité du JDK **java.lang.security**.

Autorisation contrôlant l'accès au stockage côté client, disponible par l'intermédiaire de la classe **ClientStore**.

Autorisation contrôlant l'utilisation de certaines des fonctionnalités améliorées de l'ensemble des classes AWT.

Autorisation contrôlant l'accès aux informations sur le système.

Autorisation contrôlant l'affichage des boîtes de dialogue liées aux fichiers afin d'effectuer des opérations sur les fichiers. Par exemple, si une mini-application veut ouvrir un fichier, elle doit présenter la boîte de dialogue standard Ouverture et permettre à l'utilisateur de sélectionner le fichier voulu. La mini-application ne pourra effectuer d'opérations sur les fichiers de façon autonome. Ainsi, cette opération est plus sécurisante que du code permettant d'accéder directement aux fichiers car l'utilisateur est directement impliqué. Cette autorisation est une autorisation de niveau « Moyen ».

Autorisation contrôlant l'utilisation des fonctionnalités améliorées des composants multimédias.

Autorisation offrant des contrôles spécifiques sur les types d'autorisations à accorder aux informations signées.

Autorisation contrôlant la capacité d'un code avec signature de créer jusqu'à 1 Mo d'espace Scratch par le biais de ClientStoragePermission, qui peut servir à stocker temporairement des informations. Aucune mini-application Java ne sera autorisée à lire ni écrire dans aucun autre fichier situé sur le disque dur de l'utilisateur. Une mini-application signée ne peut accéder qu'à son propre espace Scratch. Ce niveau d'autorisation est « Moyen ».

Autorisation contrôlant la présentation de boîtes de dialogue.

Environnement de protection de certaines ressources (comme le système, le disque dur, le réseau, l'ordinateur local) contre des accès extérieurs dans lesquels une mini-application Java peut être exécutée avec des ensembles d'autorisation contrôlés par l'utilisateur.

