

Pour obtenir des informations à jour sur les pratiques de traitement des données de Microsoft, passez en revue l'[Énoncé de confidentialité Microsoft](#). Vous pouvez également en savoir plus sur les derniers outils que nous proposons pour accéder à vos données et les contrôler, ainsi que sur la manière dont vous pouvez nous contacter si vous avez une demande en matière de confidentialité.

# Déclaration de confidentialité de Windows 8.1 et de Windows Server 2012 R2

## Point essentiel

Déclaration Fonctionnalités Applications Serveur

Dans cette page

Dernière mise à jour : avril 2014

[Vos informations personnelles](#)

Ces points clés de la Déclaration de confidentialité Windows 8.1 et Windows Server 2012 R2 complète (« Déclaration de confidentialité Windows ») expliquent en détail la collecte de données et les pratiques d'utilisation de Windows 8.1 et Windows Server 2012 R2

[Vos choix](#)

[Utilisation des informations](#)

(« Windows »). Ils mettent l'accent sur les fonctionnalités en ligne. En aucun cas il ne s'agit d'une liste exhaustive. Ils ne s'appliquent pas aux autres sites Microsoft en ligne ou hors connexion, ni aux autres produits ou services.

[Comment nous contacter](#)

Cette déclaration de confidentialité comprend les sections suivantes :

- **Points clés** (cette page)
- [Déclaration](#), qui constitue l'intégralité de la Déclaration de confidentialité de Windows 8.1, et qui inclut des liens vers les déclarations de confidentialité relatives aux fonctionnalités de Windows qui possèdent leur propre déclaration

- [Avenant aux fonctionnalités](#), qui décrit les fonctionnalités qui ont un impact de confidentialité dans Windows 8.1 et Windows Server 2012 R2
- [Avenant aux applications](#), qui décrit les applications qui ont un impact de confidentialité dans Windows 8.1
- [Avenant à la version serveur](#), qui décrit les fonctionnalités supplémentaires qui ont un impact sur les informations personnelles dans Windows Server 2012 R2

Pour plus d'informations sur la façon dont nous protégeons votre ordinateur, vos informations personnelles et votre famille en ligne, visitez le Centre de Sécurité.

#### Vos informations personnelles

- Certaines fonctionnalités de Windows peuvent avoir besoin de votre autorisation pour la collecte ou l'utilisation d'informations provenant de votre ordinateur, notamment vos informations personnelles. Windows utilise ces informations tel qu'indiqué dans la Déclaration de confidentialité Windows 8.1 [complète](#), ainsi que dans l' [Avenant aux fonctionnalités](#), l' [Avenant aux applications](#) et l' [Avenant à la version serveur](#).
- Certaines fonctionnalités de Windows peuvent, avec votre autorisation, partager vos informations personnelles sur Internet.
- Si vous choisissez d'inscrire votre logiciel, vous êtes invité à fournir des informations personnelles.
- Windows requiert un processus d'activation afin de réduire les risques de malveillance et de garantir à nos clients toute la qualité qu'ils sont en droit d'attendre de leur logiciel. L'activation envoie à Microsoft des informations sur votre ordinateur.
- Si vous choisissez de vous connecter à Windows avec un compte Microsoft, Windows synchronise les paramètres entre les différents appareils et vous connecte automatiquement à certaines applications et à certains sites web. Windows ne requiert pas de connexion avec un compte Microsoft pour

accéder à des messageries ou à des réseaux sociaux tiers, mais si cette tierce partie offre une application via le Windows Store, vous devez vous connecter à ce dernier avec votre compte Microsoft pour installer l'application. Si vous créez un compte Microsoft, vous devrez fournir des informations personnelles, telles que votre région ou votre date de naissance.

- [Détails supplémentaires](#)

[Haut de la page](#)

Vos choix

- Windows met à votre disposition plusieurs moyens pour contrôler le mode de transfert des informations sur Internet via les fonctionnalités de Windows. Pour en savoir plus sur le contrôle de ces fonctionnalités, voir l' [Avenant aux fonctionnalités](#), l' [Avenant aux applications](#) et l' [Avenant à la version serveur](#).
- Pour améliorer votre expérience, certaines fonctionnalités qui utilisent Internet sont activées par défaut.
- [Détails supplémentaires](#)

[Haut de la page](#)

Utilisation des informations

- Nous utilisons les informations collectées pour activer les fonctionnalités que vous utilisez ou fournir les services demandés. Nous nous en servons également pour améliorer la qualité de nos produits et services. À cette fin, nous fournissons parfois des informations à des entreprises qui travaillent en notre nom. Seules celles ayant un intérêt professionnel à les utiliser y ont accès. Ces entreprises sont tenues de préserver la confidentialité de ces informations et ne doivent en aucun cas les utiliser à d'autres fins.
- [Détails supplémentaires](#)

[Haut de la page](#)

Comment nous contacter

Pour plus d'informations sur nos pratiques de confidentialité, consultez la version complète de la Déclaration de confidentialité de Windows 8.1. Vous pouvez également nous écrire en remplissant le [formulaire web](#).

[Haut de la page](#)

Pour obtenir des informations à jour sur les pratiques de traitement des données de Microsoft, passez en revue l'[Énoncé de confidentialité Microsoft](#). Vous pouvez également en savoir plus sur les derniers outils que nous proposons pour accéder à vos données et les contrôler, ainsi que sur la manière dont vous pouvez nous contacter si vous avez une demande en matière de confidentialité.

# Déclaration de confidentialité de Windows 8.1 et de Windows Server 2012 R2

Point essentiel **Déclaration** Fonctionnalités Applications Serveur

Dans cette page Dernière mise à jour : avril 2014

[Collecte et utilisation de vos informations personnelles](#) Cette déclaration concerne Windows 8.1 et Windows Server 2012 R2 (« Windows »). Certains composants Windows, également répertoriés dans cette page, disposent de leur propre déclaration de

[Collecte et utilisation d'informations sur votre ordinateur](#) confidentialité. Les déclarations de confidentialité de logiciels et services associés à Windows et de précédentes versions sont également répertoriés ici.

[Sécurité de vos informations personnelles](#) Pour plus d'informations sur les fonctionnalités spécifiques, consultez les sections [Avenant aux fonctionnalités](#), l' [Avenant aux applications](#), et [Avenant à la version serveur](#). Pour plus d'informations sur Windows Embedded Industry Pro et Windows Embedded Industry Enterprise, reportez-vous à [cette déclaration](#).

[Modifications apportées à cette déclaration de confidentialité](#) La présente déclaration divulgue des informations portant sur les fonctionnalités qui communiquent avec Internet et n'est nullement exhaustive.

[Pour plus](#)

## Collecte et utilisation de vos informations personnelles

Les informations personnelles que nous collectons auprès de vous sont utilisées par Microsoft, les filiales qu'elle contrôle et ses sociétés apparentées, dans le but d'activer les fonctionnalités que vous utilisez, de fournir les services ou de mener à bien les transactions que vous avez demandées ou autorisées. Elles peuvent également servir à analyser et améliorer les produits et services proposés par Microsoft.

Sauf mention contraire dans la présente déclaration, les informations personnelles que vous fournissez ne sont pas communiquées à des tiers sans votre autorisation. Nous faisons parfois appel à d'autres sociétés pour la prestation de certains services en notre nom, notamment pour réaliser des analyses statistiques de nos services. Nous ne fournissons à ces sociétés que les informations personnelles dont elles ont besoin pour assurer le service. Il leur est strictement interdit d'utiliser ces informations à d'autres fins.

Microsoft peut accéder à des informations vous concernant ou les divulguer, y compris le contenu de vos communications, afin de : (a) se conformer à la loi ou satisfaire à des demandes en vertu de la loi ou à une procédure judiciaire ; (b) protéger les droits ou la propriété de Microsoft ou de ses clients, notamment l'application des accords ou des politiques qui régissent l'utilisation du logiciel ; ou (c) agir en toute bonne foi lorsque cet accès ou cette divulgation est nécessaire pour préserver la sécurité personnelle des employés et des clients de Microsoft ou du public.

Toute information recueillie par ou transmise à Microsoft via Windows 8.1 peut être stockée et traitée aux États-Unis ou dans tout autre pays dans lequel Microsoft ou ses filiales, sociétés apparentées ou fournisseurs de services gèrent des infrastructures. Microsoft agit dans le cadre de la sphère de sécurité (« Safe Harbor ») définie par le ministère du commerce des États-Unis d'Amérique concernant la collecte, l'utilisation et la conservation des données provenant de l'Union européenne, de la zone économique européenne et de la Suisse.

[Haut de la page](#)

## Collecte et utilisation d'informations sur votre ordinateur

Lorsque vous utilisez des logiciels avec des fonctionnalités Internet, des informations concernant votre ordinateur (« informations standard de l'ordinateur ») sont envoyées aux sites Web que vous visitez et aux services en ligne que vous utilisez. Les informations standard de l'ordinateur incluent généralement diverses données, telles que votre adresse IP, la version du système d'exploitation, la version du navigateur, ainsi que vos paramètres régionaux et linguistiques. Dans certains cas, elles peuvent également comprendre l'ID du matériel qui indique le nom du fabricant, ainsi que le nom du périphérique et sa version. Si une fonctionnalité ou un service donné envoie des informations à Microsoft, les informations standard de l'ordinateur sont également transmises.

Les détails pour chaque fonctionnalité Windows qui sont inclus dans l'avenant aux fonctionnalités, l'avenant aux applications et l'avenant à la version serveur, ainsi que les fonctionnalités également répertoriées dans cette page décrivent les informations supplémentaires qui sont recueillies et leur utilisation.

Les administrateurs peuvent recourir à la stratégie de groupe afin de modifier un grand nombre de paramètres pour les fonctionnalités décrites ici. Pour plus d'informations, voir [ce livre blanc destiné aux administrateurs](#).

[Haut de la page](#)

## Sécurité de vos informations personnelles

Microsoft s'engage à assurer la protection de vos informations personnelles. Nous utilisons diverses technologies et procédures de sécurité afin de protéger au mieux vos informations personnelles contre tout accès, utilisation ou divulgation non autorisée.

Par exemple, nous stockons les informations personnelles que vous nous confiez sur des systèmes informatiques dont l'accès est limité et qui se trouvent dans des installations surveillées. Lorsque nous transmettons des informations hautement confidentielles (par exemple, un numéro de carte de crédit ou un mot de passe) sur Internet, nous les protégeons à l'aide de méthodes de chiffrement, telles que le protocole SSL (Secure Socket Layer).

[Haut de la page](#)

Modifications apportées à cette déclaration de confidentialité

Nous mettons occasionnellement à jour la présente déclaration de confidentialité afin de tenir compte des avis de nos clients et des modifications apportées à nos produits et à nos services. Au moment d'intégrer ces modifications, nous changeons la date de dernière mise à jour mentionnée en haut de cette déclaration. Si des modifications matérielles sont apportées à cette déclaration ou aux modalités selon lesquelles Microsoft utilise vos informations personnelles, nous publions un avis informant de ces changements avant leur mise en œuvre ou nous vous adressons directement un message de notification. Nous vous recommandons de consulter régulièrement cette déclaration de confidentialité afin de prendre connaissance des mesures prises par Microsoft pour protéger vos informations.

[Haut de la page](#)

Pour plus d'informations

Vos remarques à propos de cette déclaration de confidentialité sont précieuses pour Microsoft et sont les bienvenues. Si vous avez des questions concernant la présente déclaration ou pensez que Microsoft n'en respecte pas les principes, écrivez-nous en utilisant notre [formulaire web](#).

Microsoft Privacy  
Microsoft Corporation  
One Microsoft Way  
Redmond, Washington 98052  
USA

[Haut de la page](#)



Pour obtenir des informations à jour sur les pratiques de traitement des données de Microsoft, passez en revue l'[Énoncé de confidentialité Microsoft](#). Vous pouvez également en savoir plus sur les derniers outils que nous proposons pour accéder à vos données et les contrôler, ainsi que sur la manière dont vous pouvez nous contacter si vous avez une demande en matière de confidentialité.

# Déclaration de confidentialité de Windows 8.1 et de Windows Server 2012 R2

Point essentiel Déclaration **Fonctionnalités** Applications Serveur

Dans cette page Dernière mise à jour : avril 2014

[Activation](#)

Notez que cette page constitue un avenant à la Déclaration de confidentialité de Windows 8.1 et Windows Server 2012 R2

[Client AD RMS \(Active Directory Rights Management Services\)](#)

(« Déclaration de confidentialité de Windows ») qui comprend les sections suivantes :

[Identifiant de publicité](#)

- [Points clés](#)

[Audit](#)

- [Déclaration](#), qui constitue l'intégralité de la Déclaration de confidentialité de Windows 8.1, et qui inclut des liens vers les déclarations de confidentialité relatives aux fonctionnalités de Windows qui possèdent leur propre déclaration

[Biométrie](#)

[Chiffrement de lecteur](#)

[BitLocker](#)

- **Avenant aux fonctionnalités** (la présente page), qui décrit les fonctionnalités qui ont un impact sur les informations personnelles dans Windows 8.1 et Windows Server 2012 R2

[Contacts](#)

[Détection et](#)

[configuration des](#)

- [Avenant aux applications](#), qui décrit les applications qui ont un

périphériques	impact de confidentialité dans Windows 8.1
Chiffrement de l'appareil	<ul style="list-style-type: none"> <li>• <a href="#">Avenant à la version serveur</a>, qui décrit les fonctionnalités supplémentaires qui ont un impact sur les informations personnelles dans Windows Server 2012 R2</li> </ul>
DirectAccess	
Options d'ergonomie	Pour comprendre les méthodes de collecte et d'utilisation des données ayant trait à une fonctionnalité ou un service particulier de Windows, nous vous conseillons de lire l'intégralité de la Déclaration de confidentialité et tout avenant applicable ou toute déclaration individuelle.
Observateur d'événements	
Contrôle parental	
Télécopie	
Personnalisation de l'écriture manuscrite : apprentissage automatique	<p>Activation</p> <p><b>Quel est le rôle de cette fonctionnalité ?</b></p> <p>L'activation réduit la contrefaçon de logiciel, ce qui contribue à assurer aux clients de Microsoft toute la qualité qu'ils sont en droit d'attendre de leur logiciel. Une fois votre logiciel activé, une clé de produit spécifique est associée à l'ordinateur (ou au matériel) sur lequel ce premier est installé. Cette association empêche la clé de produit d'être utilisée pour activer la même copie du logiciel sur plusieurs ordinateurs. Des modifications apportées au matériel ou aux logiciels de votre ordinateur peuvent vous obliger à réactiver Windows.</p>
Groupe résidentiel	
IME (éditeur de méthode d'entrée)	
Partage de connexion Internet	
Impression Internet	L'activation peut détecter et désactiver les attaques du mécanisme d'activation (logiciel qui contourne l'activation du logiciel Microsoft). Si une telle attaque est présente, un éditeur de logiciel ou un fournisseur de matériel est susceptible d'avoir falsifié le logiciel Microsoft authentique afin de créer des copies de contrefaçon du logiciel. Les attaques du mécanisme d'activation peuvent interférer avec le fonctionnement normal de votre système.
Préférences linguistiques	
Services de localisation	
Gérer vos informations d'identification	
Nom et avatar de compte	<p><b>Informations collectées, traitées ou transmises</b></p> <p>Lors de l'activation, les informations suivantes sont envoyées à Microsoft :</p>
Reconnaissance du réseau	<ul style="list-style-type: none"> <li>• Le code de produit Microsoft (composé de cinq chiffres identifiant le produit Windows que vous activez).</li> </ul>
Notifications, applications de l'écran de verrouillage et	<ul style="list-style-type: none"> <li>• Un ID de canal ou un code de site, qui identifie où vous avez obtenu le produit Windows. Par exemple, un ID de canal ou un</li> </ul>

mises à jour de vignettes	code de site permet de déterminer si le produit a été acheté dans un magasin, reçu sous forme de copie d'évaluation, obtenu dans le cadre d'un programme de licence en volume ou préinstallé par un fabricant d'ordinateurs.
Commander des tirages	
Prérécupération et préléancement	<ul style="list-style-type: none"> <li>• La date de l'installation et si l'installation s'est effectuée correctement.</li> </ul>
Assistant Compatibilité des programmes	<ul style="list-style-type: none"> <li>• Des informations aidant à confirmer que la clé de votre produit Windows n'a pas été modifiée.</li> </ul>
Propriétés	<ul style="list-style-type: none"> <li>• La marque et le modèle de l'ordinateur.</li> </ul>
Proximité	<ul style="list-style-type: none"> <li>• Des renseignements qui indiquent la version du système d'exploitation et des logiciels.</li> </ul>
Connexions d'accès distant	<ul style="list-style-type: none"> <li>• Les paramètres régionaux et linguistiques.</li> </ul>
Connexions aux programmes RemoteApp et aux services Bureau à distance	<ul style="list-style-type: none"> <li>• Un numéro unique, appelé identificateur global unique (GUID, Globally Unique Identifier) attribué à votre ordinateur.</li> <li>• La clé du produit (avec hachage) et l'ID du produit.</li> <li>• Le nom, le numéro de révision et la date de révision du BIOS.</li> </ul>
Connexion Bureau à distance	<ul style="list-style-type: none"> <li>• Le numéro de série du disque dur (avec hachage).</li> </ul>
Se connecter à un compte Microsoft	<ul style="list-style-type: none"> <li>• Le résultat de la vérification de l'activation. Cela inclut les codes d'erreur et les informations relatives aux attaques du mécanisme d'activation et aux logiciels assimilés à des programmes malveillants ou non autorisés et détectés ou désactivés : <ul style="list-style-type: none"> <li>• l'identifiant de l'attaque du mécanisme d'activation ;</li> <li>• l'état de l'attaque, par exemple si elle est nettoyée ou mise en quarantaine ;</li> <li>• l'identification du fabricant de l'ordinateur ;</li> <li>• le nom de fichier de l'attaque du mécanisme d'activation et son hachage, ainsi qu'un hachage des composants logiciels connexes pouvant indiquer la présence d'une telle attaque.</li> </ul> </li> </ul>
Stockage nuage OneDrive	
Synchroniser les paramètres	
Technologie Tere do	
Services du module de plateforme sécurisée (TPM)	<ul style="list-style-type: none"> <li>• Le nom et un hachage du contenu du fichier d'instructions pour</li> </ul>
Certificats racine de mise à jour	

Update Services le démarrage de votre PC. Si votre licence Windows est associée à un abonnement, des renseignements sont également transmis pour indiquer les modalités de votre abonnement. Les informations standard de l'ordinateur sont également envoyées.

Réseau privé virtuel

Programme d'amélioration de l'expérience utilisateur Windows

- Si vous utilisez une copie sous licence en volume de Windows qui utilise un serveur d'activation, l'adresse IP de ce serveur peut être transmise à Microsoft.

Windows Defender

### **Utilisation des informations**

Service de rapport d'erreurs Windows

Microsoft utilise les informations collectées pour vérifier que vous disposez d'une copie sous licence du logiciel. Microsoft n'utilise pas ces informations pour contacter les clients. Les informations sur le serveur de licences sont utilisées pour garantir que les serveurs de licences sont en conformité avec leurs contrats de licence.

Association de fichier Windows

Aide de Windows

### **Choix et contrôle**

Assistance à distance

Windows Search

L'activation est obligatoire et se produit automatiquement lorsque vous installez Windows. Si vous ne possédez pas de licence valide pour le logiciel, vous n'êtes alors pas en mesure d'activer Windows.

Installation de Windows

[Haut de la page](#)

Partage Windows

Windows SmartScreen

Client AD RMS (Active Directory Rights Management Services)

Reconnaissance vocale de Windows

### **Quel est le rôle de cette fonctionnalité ?**

Windows Store

Le client AD RMS (Active Directory Rights Management Services) constitue une technologie de protection des informations fonctionnant avec les applications compatibles avec les services AD RMS dont le but est de sécuriser les informations numériques contre tout usage non autorisé. Les propriétaires des informations numériques peuvent définir ce que les destinataires sont en droit de faire avec les informations contenues dans un fichier, par exemple les utilisateurs autorisés à ouvrir, à modifier, à imprimer ou à réaliser des opérations sur le fichier. Afin de créer ou de visualiser un fichier auquel des autorisations restreintes s'appliquent, votre ordinateur doit exécuter une application AD RMS et disposer d'un accès à un serveur AD RMS.

Service de temps Windows

Résolution des problèmes Windows

Dossiers de travail

Espace de travail

### **Informations collectées, traitées ou transmises**

Le service AD RMS s'appuie sur votre adresse de messagerie pour vous identifier auprès d'un serveur AD RMS. En conséquence, votre adresse de messagerie est stockée sur le serveur, ainsi que sur votre ordinateur dans les licences et les certificats d'identité créés par le serveur. Les certificats d'identité et les licences sont transférés vers et depuis des serveurs AD RMS lorsque vous tentez d'ouvrir ou d'imprimer un document protégé par la gestion des droits, ou d'effectuer d'autres actions sur ce document. Si votre ordinateur est connecté au réseau d'une entreprise, le serveur AD RMS est généralement géré par cette dernière. Si vous utilisez les services AD RMS Windows Live, le serveur est géré par Microsoft. Pour préserver la confidentialité de vos informations personnelles, les informations envoyées aux serveurs Microsoft AD RMS sont chiffrées.

### **Utilisation des informations**

La licence vous permet d'accéder à des fichiers protégés. Les certificats d'identité servent à vous identifier auprès d'un serveur AD RMS, et vous permettent de protéger ces fichiers et d'y accéder.

### **Choix et contrôle**

Les fonctionnalités AD RMS doivent être activées par le biais d'une application compatible AD RMS. Par défaut, celles-ci ne sont pas activées. Il vous est possible de ne pas les activer ni de les utiliser. Toutefois, si vous ne les activez pas, vous n'êtes pas en mesure d'accéder aux fichiers protégés.

[Haut de la page](#)

Identifiant de publicité

### **Quel est le rôle de cette fonctionnalité ?**

Pour communiquer des publicités plus appropriées, Windows autorise les applications à accéder à un identifiant unique pour chaque utilisateur sur un appareil. Vous pouvez réinitialiser ou désactiver l'accès à cet identifiant à tout moment.

### **Informations collectées, traitées ou transmises**

Si vous autorisez les applications à accéder à l'identifiant de publicité, Windows le fournit à toutes les applications qui le demandent. Les

applications sont susceptibles de stocker ou de transmettre ces données.

### **Utilisation des informations**

Votre identifiant de publicité permet aux développeurs d'application et aux réseaux publicitaires de vous communiquer des publicités plus appropriées en fonction des applications que vous utilisez et de la façon dont vous les utilisez. Il permet également aux développeurs d'application d'améliorer la qualité de service en déterminant la fréquence et l'efficacité des publicités et en détectant les problèmes de fraude et de sécurité.

Si vous autorisez des applications à accéder à l'identifiant de publicité, son utilisation est soumise aux pratiques en matière de confidentialité de chaque application correspondante.

### **Choix et contrôle**

Si vous optez pour la configuration rapide de Windows, Windows autorise dans ce cas les applications à utiliser votre identifiant de publicité. Si vous choisissez de personnaliser les paramètres, vous pouvez contrôler l'accès à votre identifiant de publicité en sélectionnant **Autoriser les applications à utiliser mon identifiant de publicité pour de meilleures expériences dans les applications** sous **Partager des informations avec Microsoft** et d'autres services. Après avoir configuré Windows, vous pouvez modifier ce paramètre dans la section **Confidentialité** des paramètres de l'ordinateur. Si vous désactivez ce paramètre, l'identifiant de publicité n'est pas envoyé aux applications qui le demandent. Si vous choisissez de réactiver le paramètre, un nouvel identificateur est généré.

[Haut de la page](#)

### **Audit**

L'audit permet à un administrateur de configurer Windows afin d'enregistrer dans un journal de sécurité l'activité du système d'exploitation, accessible par le biais de l'observateur d'événements et d'autres applications. Ce journal peut s'avérer utile à un administrateur pour détecter les accès interdits à l'ordinateur ou aux ressources sur

l'ordinateur. Par exemple, le journal permet aux administrateurs de résoudre des problèmes et à déterminer si quelqu'un a ouvert une session sur l'ordinateur, a créé un compte d'utilisateur, a modifié une stratégie de sécurité ou a ouvert un document.

### **Informations collectées, traitées ou transmises**

Les administrateurs déterminent les informations à collecter, leur durée de conservation et si celles-ci sont transmises à des tierces parties. Ces informations peuvent comprendre des informations confidentielles, telles que des noms d'utilisateurs ou des noms de fichiers. Pour plus d'informations, contactez votre administrateur. Aucune information n'est envoyée à Microsoft.

### **Utilisation des informations**

Les administrateurs sont également en mesure de préciser l'usage qui est fait des informations d'audit. En règle générale, les auditeurs et les administrateurs utilisent le journal de sécurité pour effectuer le suivi de l'activité d'un ordinateur ou pour identifier les accès interdits à un ordinateur ou à des ressources sur ce dernier.

### **Choix et contrôle**

Les administrateurs indiquent si cette fonctionnalité doit être activée et la façon d'en notifier les utilisateurs. Les autres utilisateurs ne peuvent pas consulter le journal de sécurité à moins que l'administrateur ne les autorise à y accéder. Vous pouvez configurer l'audit sur votre ordinateur en ouvrant Stratégie de sécurité locale dans Outils d'administration.

[Haut de la page](#)

Biométrie

### **Quel est le rôle de cette fonctionnalité ?**

Si votre ordinateur dispose d'un lecteur d'empreintes digitales, vous pouvez utiliser votre empreinte digitale pour vous connecter à Windows et pour vous identifier auprès d'applications qui prennent en charge cette fonctionnalité.

### **Informations collectées, traitées ou transmises**

Lorsque vous configurez une nouvelle empreinte digitale, les lectures de votre empreinte digitale sont stockées localement sur votre ordinateur. Aucune information n'est envoyée à Microsoft. Lorsque vous utilisez votre empreinte digitale pour vous identifier auprès d'une application, Windows la compare avec celles enregistrées sur votre ordinateur, et indique à l'application si l'empreinte digitale numérisée correspond à une empreinte associée à votre compte. Windows ne fournit pas les données de l'empreinte digitale numérisée à l'application.

### **Utilisation des informations**

Windows utilise les informations relatives à l'empreinte digitale que vous avez choisi de stocker sur votre ordinateur pour vous connecter à Windows à l'aide de votre empreinte digitale.

### **Choix et contrôle**

Vous pouvez ajouter ou supprimer des empreintes digitales via **Options de connexion** dans la section **Comptes** disponible dans Paramètres du PC.

[Haut de la page](#)

Chiffrement de lecteur BitLocker

### **Quel est le rôle de cette fonctionnalité ?**

Le chiffrement de lecteur BitLocker contribue à protéger vos données en les chiffrant, ce qui permet d'empêcher un utilisateur non autorisé d'y accéder. Lorsque BitLocker est activé sur un lecteur pris en charge, Windows chiffre alors les données sur celui-ci.

### **Informations collectées, traitées ou transmises**

Lorsque BitLocker est activé par le biais de chiffrement logiciel, les clés de chiffrement stockées en mémoire chiffrent et déchiffrent les données de façon continue au fur et à mesure qu'elles sont lues ou écrites sur le lecteur protégé. Lorsque BitLocker est activé par le biais d'un chiffrement matériel, il incombe au lecteur d'effectuer le chiffrement et le déchiffrement des données.

Lors de la configuration de BitLocker, il vous est possible de choisir d'imprimer une clé de récupération ou de l'enregistrer sur le réseau. Si



vous configurez BitLocker sur un lecteur non amovible, vous pouvez également enregistrer votre clé de récupération sur un lecteur flash USB.

Si votre ordinateur ne fait pas partie d'un domaine, vous pouvez alors sauvegarder votre clé de récupération BitLocker, son ID et le nom de votre ordinateur sur MicrosoftOneDrive. Pour préserver la confidentialité de vos informations personnelles, les informations transmises sont chiffrées via SSL.

Vous pouvez configurer BitLocker pour chiffrer les données à l'aide d'un certificat stocké sur une carte à puce. Si vous protégez un lecteur de données par le biais d'une carte à puce, la clé publique et l'identifiant unique de cette dernière sont stockés sous une forme non chiffrée sur le lecteur. Ces informations vous permettent de retrouver le certificat ayant été utilisé à l'origine pour générer le certificat de chiffrement de la carte à puce.

Si votre ordinateur est doté de matériel de sécurité avec au minimum la version 1.2 du module de plateforme sécurisé (TPM, Trusted Platform Module), BitLocker fait appel à TPM pour assurer une protection matérielle améliorée des données sur le lecteur où Windows est installé. Pour plus d'informations, voir la section Services du module de plateforme sécurisée (TPM). Sur les ordinateurs équipés des services TPM, vous pouvez en outre configurer un numéro d'identification personnel (PIN, Personal Identification Number) pour ajouter un niveau supplémentaire de protection pour vos données chiffrées. BitLocker stocke ce code PIN TPM sous forme de hachage chiffré sur le lecteur.

Les informations que BitLocker recueille ne sont pas envoyées à Microsoft à moins que vous n'optiez pour la sauvegarde de votre clé de récupération sur OneDrive.

### **Utilisation des informations**

Les clés de chiffrement et les identifiants globaux uniques (GUID, Globally Unique IDentifiers) sont stockés dans la mémoire de l'ordinateur pour le bon déroulement des opérations de BitLocker. Les informations de récupération de BitLocker vous permettent d'accéder à vos données protégées en cas de panne matérielle ou d'autres problèmes. Elles permettent à BitLocker de faire la différence entre les

utilisateurs autorisés et les utilisateurs non autorisés.

Microsoft n'utilise en aucun cas vos clés de récupération personnelles. Lorsque les clés de récupération sont envoyées à OneDrive, Microsoft peut exploiter des données collectées sur ces clés pour analyser les tendances et contribuer à améliorer ses produits et services.

### **Choix et contrôle**

Par défaut, l'option BitLocker est désactivée. Sur un lecteur amovible, tout utilisateur peut activer ou désactiver BitLocker à tout moment en ouvrant Chiffrement de lecteur BitLocker dans le Panneau de configuration. Un administrateur peut activer ou désactiver BitLocker sur tous les lecteurs.

Vous pouvez afficher et gérer les [clés de récupération stockées sur votre compte OneDrive](#).

[Haut de la page](#)

Contacts

### **Quel est le rôle de cette fonctionnalité ?**

Si vous utilisez l'application Contacts ou une application tierce prise en charge pour gérer vos contacts, vous pouvez partager des contacts spécifiques avec d'autres applications de votre PC, afficher des coordonnées sur une carte de visite ou partager des coordonnées spécifiques avec d'autres applications de votre PC afin d'effectuer une action, par exemple passer un appel ou mapper une adresse.

### **Informations collectées, traitées, stockées et transmises**

Quand une application demande des coordonnées, Windows vous permet de choisir les contacts spécifiques à partager avec cette application. Les contacts peuvent provenir de l'application Contacts ou d'une application Contacts tierce prise en charge. Windows ne partage pas l'ensemble de votre liste de contacts avec l'application à l'origine de la demande.

Si une application a accès à une information relative à l'un de vos contacts, par exemple un numéro de téléphone ou une adresse e-mail, Windows peut afficher une carte de visite avec les informations

supplémentaires provenant de votre application Contacts pour ce contact. Windows ne partage pas les coordonnées supplémentaires avec l'application qui affiche la carte de visite.

Si vous appuyez ou cliquez sur une commande telle que **Appeler**, l' **E-Mail** ou **Mapper** dans la carte de visite, Windows ouvre l'application appropriée pour effectuer cette action et lui fournit les coordonnées nécessaires, par exemple le numéro de téléphone s'il s'agit d'un appel.

### **Utilisation des informations**

Windows utilise les coordonnées de votre application Contacts pour partager les contacts spécifiques de votre choix, afficher des cartes de visite, ouvrir des applications et partager des coordonnées afin d'effectuer les actions indiquées dans les cartes de visite, ainsi que pour afficher vos contacts dans Windows Search. L'utilisation par l'application Contacts des informations relatives à vos contacts est décrite dans la [déclaration de confidentialité des applications de communication](#).

Si vous partagez des coordonnées avec une application tierce, l'utilisation de ces informations est soumise aux pratiques de confidentialité de la tierce partie. Si vous partagez des coordonnées avec une application Microsoft, les pratiques de confidentialité de l'application sont expliquées dans la déclaration de confidentialité de cette application.

### **Choix et contrôle**

Windows affiche et partage uniquement les coordonnées quand vous choisissez de partager des contacts spécifiques avec une application, d'afficher une carte de visite ou de sélectionner une action à partir de la carte de visite.

### [Haut de la page](#)

### Détection et configuration des périphériques

Windows dispose de plusieurs fonctionnalités vous aidant à détecter et à configurer des périphériques sur votre ordinateur, notamment l'installation de périphériques, l'installation d'appareils haut débit mobiles, la découverte du réseau et le couplage de périphériques sans fil.

# Installation de périphérique

## Quel est le rôle de cette fonctionnalité ?

Lorsque vous installez un nouveau périphérique sur votre ordinateur, Windows peut rechercher, télécharger et installer automatiquement ses pilotes. Windows peut également télécharger des informations relatives au périphérique, telles que sa description, sa représentation graphique et le logo du fabricant. Certains périphériques, notamment les imprimantes, webcams, appareils à haut débit mobile et appareils mobiles qui effectuent une synchronisation avec Windows, disposent d'une application qui permet une totale activation des fonctionnalités du périphérique et une meilleure expérience utilisateur. Si le fabricant du périphérique a fourni une application pour le périphérique, Windows peut télécharger et installer automatiquement cette application à partir du Windows Store si vous y êtes connecté.

## Informations collectées, traitées ou transmises

Lorsque Windows recherche des pilotes, il contacte le service en ligne Windows Update pour rechercher et télécharger les pilotes du périphérique, si aucun pilote approprié n'est déjà installé sur l'ordinateur. Pour en savoir plus sur les informations recueillies par Windows Update et sur la manière dont elles sont utilisées, voir la [Déclaration de confidentialité de la fonctionnalité Update Services](#).

Pour récupérer des informations relatives à votre périphérique et déterminer si une application est disponible pour celui-ci, Windows envoie à Microsoft des données le concernant, parmi lesquelles son ID (par exemple, l'ID de matériel ou de modèle du périphérique que vous utilisez), votre région/pays et votre langue, ainsi que la date de dernière mise à jour des informations du périphérique. Si une application est proposée pour le périphérique, Windows la télécharge du Windows Store et l'installe automatiquement. L'application est alors disponible dans votre compte Windows Store, dans la liste des applications que vous possédez.

## Utilisation des informations

Les informations envoyées à Microsoft servent à déterminer et à télécharger le pilote, les informations et l'application qui conviennent pour votre périphérique. Microsoft n'utilise pas les informations

envoyées pour vous identifier ou vous contacter.

## **Choix et contrôle**

Si vous optez pour l'installation rapide de Windows, le téléchargement et l'installation automatiques des pilotes, informations et applications du périphérique sont activés. Si vous choisissez de personnaliser des paramètres, vous pouvez contrôler le téléchargement et l'installation automatiques des pilotes, applications et informations de périphérique en sélectionnant **Obtenir automatiquement les pilotes, applications et informations de périphérique pour les nouveaux périphériques** sous **Protéger et mettre à jour votre PC**. Après avoir configuré Windows, vous pouvez modifier ces paramètres dans le Panneau de configuration en sélectionnant Change device installation settings, puis **Non, je préfère choisir manuellement**.

Vous pouvez désinstaller une application pour périphérique à tout moment sans désinstaller le périphérique. Cependant, vous pouvez avoir besoin de l'application pour utiliser certaines fonctionnalités du périphérique. Vous pouvez réinstaller une application pour périphérique après l'avoir désinstallée en accédant à la liste des applications en votre possession dans le Windows Store.

## **Installation d'appareils haut débit mobiles**

### **Quel est le rôle de cette fonctionnalité ?**

Si votre ordinateur est doté de matériel haut débit mobile que certains opérateurs mobiles fournissent, Windows peut télécharger et installer automatiquement une application vous permettant de gérer votre compte et votre forfait données obtenus auprès de l'opérateur mobile vous ayant fourni le matériel haut débit mobile pour votre ordinateur. D'autres informations de périphérique sont également téléchargées pour permettre d'afficher votre connexion haut débit mobile dans les listes des réseaux.

### **Informations collectées, traitées ou transmises**

Pour déterminer les informations et l'application pour périphérique à télécharger, Windows envoie une partie des identificateurs du matériel à partir de votre matériel haut débit mobile, ce qui nous permet d'identifier votre opérateur mobile. Pour préserver la confidentialité de

vos informations personnelles, Windows n'envoie pas les identifiants complets du matériel haut débit mobile à Microsoft.

Si votre opérateur mobile a fourni une application à Microsoft, Windows la télécharge alors à partir du Windows Store et l'installe. Si vous ouvrez l'application après son installation, celle-ci a alors accès à votre matériel haut débit mobile, notamment aux identifiants du matériel que l'opérateur mobile peut utiliser pour identifier votre compte.

### **Utilisation des informations**

Microsoft utilise la partie de votre identifiant de matériel haut débit mobile que Windows transmet pour déterminer l'application de l'opérateur à installer sur votre ordinateur. Une fois cette dernière installée, elle peut alors exploiter les ID de votre matériel haut débit mobile. Par exemple, l'application d'un opérateur mobile est susceptible d'utiliser ces identifiants pour rechercher en ligne des informations sur les comptes et les forfaits. L'utilisation de ces informations par l'application est régie par les pratiques de votre opérateur mobile en matière de confidentialité.

### **Choix et contrôle**

Si vous optez pour la configuration rapide lors de la première installation de Windows, Windows recherche et télécharge automatiquement les applications de l'opérateur mobile. Vous avez la possibilité d'activer et de désactiver cette fonctionnalité depuis le Panneau de configuration. Pour plus d'informations, voir la section Installation de périphérique, ci-dessus.

Vous pouvez désinstaller à tout moment une application d'un opérateur mobile sans désinstaller pour autant votre matériel haut débit mobile.

## **Découverte du réseau**

### **Quel est le rôle de cette fonctionnalité ?**

Si vous connectez votre ordinateur à un petit réseau privé, par exemple à la maison, Windows peut détecter automatiquement les autres ordinateurs et les périphériques partagés du réseau, et rendre votre ordinateur visible aux autres dispositifs du réseau. Lorsque les périphériques partagés sont disponibles, Windows peut

automatiquement s'y connecter et les installer. Ces périphériques regroupent par exemple les imprimantes et les extendeurs de support mais ne comprennent pas les appareils personnels tels que les appareils photo et les téléphones portables.

### **Informations collectées, traitées ou transmises**

Si vous activez le partage et la connexion aux périphériques, les informations relatives à votre ordinateur, par exemple son nom et son adresse réseau, peuvent être diffusées sur le réseau local pour permettre aux autres ordinateurs de le détecter et de s'y connecter.

Afin de déterminer si les périphériques connectés à votre réseau doivent être automatiquement installés, des informations relatives au réseau sont collectées et envoyées à Microsoft. Ces informations comprennent le nombre de périphériques sur le réseau, le type de réseau (par exemple, un réseau privé) et les types et noms des modèles des périphériques. Aucune information confidentielle, telle que le nom du réseau ou un mot de passe, n'est collectée.

En fonction de vos paramètres d'installation des périphériques, lorsque Windows installe des périphériques partagés, Windows est susceptible d'envoyer des informations à Microsoft et d'installer le logiciel des périphériques en question sur votre ordinateur. Pour plus d'informations, voir la section Installation de périphérique.

### **Utilisation des informations**

Les informations envoyées à Microsoft concernant votre réseau servent à déterminer les périphériques du réseau devant être automatiquement installés. Microsoft n'utilise pas ces informations pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

### **Choix et contrôle**

Si vous activez le partage et la connexion aux périphériques au moment où vous vous connectez à un réseau, la découverte du réseau est alors activée pour le réseau en question. Vous pouvez modifier ce paramètre pour votre réseau en cliquant sur le type de réseau indiqué sous le nom du réseau dans le Centre Réseau et partage.

Il vous est possible d'activer entièrement la découverte du réseau et la

configuration automatique des périphériques réseau connectés en sélectionnant l'option **Modifier les paramètres de partage avancés** dans le Centre Réseau et partage.

## Couplage de périphériques sans fil

### Quel est le rôle de cette fonctionnalité ?

Windows vous permet de jumeler votre ordinateur et des périphériques sans fil utilisant Bluetooth ou Wi-Fi Direct. Wi-Fi Direct représente une technologie sans fil permettant aux périphériques de communiquer directement entre eux sans avoir besoin de se connecter à un réseau Wi-Fi.

### Informations collectées, traitées ou transmises

Si vous sélectionnez, dans les paramètres Bluetooth, l'option **Autoriser la découverte par les périphériques Bluetooth**, Windows diffuse alors le nom de votre ordinateur par Bluetooth pour permettre aux périphériques Bluetooth de le détecter et de l'identifier.

Si vous sélectionnez, dans les paramètres Bluetooth, l'option **Ajouter un périphérique**, Windows communique le nom de votre ordinateur par Wi-Fi pour permettre aux périphériques compatibles Wi-Fi Direct de le détecter et de l'identifier. Si vous fermez **Ajouter un périphérique**, Windows met fin à la diffusion par Wi-Fi du nom de votre ordinateur.

En fonction de vos paramètres d'installation des périphériques, lorsque Windows effectue le couplage avec des périphériques sans fil, Windows est susceptible d'envoyer des informations à Microsoft et d'installer le logiciel des périphériques en question sur votre ordinateur. Pour plus d'informations, voir la section Installation de périphérique, ci-dessus.

### Utilisation des informations

Windows diffuse le nom de votre ordinateur pour autoriser les autres périphériques à identifier votre ordinateur et à s'y connecter. Le nom de votre ordinateur n'est pas envoyé à Microsoft.

### Choix et contrôle

Pour modifier l'option indiquant à Windows de diffuser le nom de votre ordinateur par connexion Bluetooth, maintenez la touche enfoncée ou



cliquez avec le bouton droit sur votre ordinateur apparaissant dans l'option Périphériques et imprimantes du Panneau de configuration, sélectionnez **Paramètres Bluetooth**, puis sélectionnez **Autoriser la découverte par les périphériques Bluetooth**. Si vous ne voulez pas que Windows diffuse par Wi-Fi le nom de votre ordinateur lors de l'ajout de périphériques, désactivez temporairement la fonction Wi-Fi dans Paramètres du PC, puis Sans fil, avant d'ajouter un périphérique.

[Haut de la page](#)

Chiffrement de l'appareil

### **Quel est le rôle de cette fonctionnalité ?**

Le chiffrement de l'appareil permet de protéger vos données en les chiffrant à l'aide de la technologie Chiffrement de lecteur BitLocker, ce qui contribue à prévenir les attaques de logiciels hors connexion. Lorsque vous activez cette fonctionnalité, Windows chiffre les données sur le lecteur sur lequel Windows est installé.

### **Informations collectées, traitées ou transmises**

Lorsque vous utilisez le chiffrement logiciel, les clés de chiffrement stockées en mémoire chiffrent et déchiffrent les données de façon continue au fur et à mesure qu'elles sont lues ou écrites sur le lecteur protégé. Lorsque vous utilisez un chiffrement matériel, il incombe au lecteur d'effectuer le chiffrement et le déchiffrement des données.

Windows utilise le Module de plateforme sécurisée (TPM) sur votre ordinateur pour stocker et gérer les clés de chiffrement utilisées pour chiffrer votre lecteur. Lorsque le chiffrement de l'appareil est activé, Windows chiffre automatiquement le lecteur sur lequel Windows est installé et génère une clé de récupération. La clé de récupération vous permet d'accéder à vos données protégées en cas de panne matérielle ou d'autres problèmes.

La clé de récupération BitLocker pour votre ordinateur est automatiquement sauvegardée en ligne dans le compte MicrosoftOneDrive de chaque compte d'administrateur connecté à un compte Microsoft. Le nom de votre ordinateur et un identificateur pour la clé de récupération sont également sauvegardés dans le même compte OneDrive. Pour préserver la confidentialité de vos informations

personnelles, les informations transmises sont chiffrées via SSL.

## **Utilisation des informations**

Les clés de chiffrement et les identifiants globaux uniques (GUID, Globally Unique IDentifiers) sont stockés dans la mémoire de l'ordinateur pour prendre en charge les opérations BitLocker. Les informations de récupération vous permettent d'accéder à vos données protégées lors de certaines pannes matérielles ou autres problèmes, et permettent à BitLocker de distinguer les utilisateurs autorisés des utilisateurs non autorisés.

Microsoft sauvegarde vos informations de récupération sur votre compte OneDrive pour que vous puissiez y accéder en ligne. Nous n'utilisons pas les informations de clé de récupération à quelque fin que ce soit et elles sont stockées uniquement dans ce compte OneDrive. Nous sommes susceptibles d'exploiter des données collectées sur ces clés de récupération pour analyser les tendances et contribuer à améliorer nos produits et services. Par exemple, nous pouvons être amenés à utiliser ces informations pour déterminer la proportion de PC sur lesquels le chiffrement de l'appareil est activé.

## **Choix et contrôle**

Si vous choisissez d'utiliser un compte Microsoft lors de la configuration de votre PC et que celui-ci le prend en charge, le chiffrement de l'appareil est activé et votre clé de récupération est sauvegardée dans votre compte OneDrive. Si vous choisissez d'utiliser un compte local lors de la configuration de votre ordinateur, le chiffrement de l'appareil est désactivé.

Si vous associez ultérieurement un compte Microsoft à un compte d'administrateur sur votre ordinateur :

- Si le chiffrement de l'appareil n'est pas déjà activé, Windows l'active automatiquement et sauvegarde les informations de récupération dans le compte OneDrive de l'utilisateur.
- Si le chiffrement de l'appareil est déjà activé, les informations de récupération pour votre ordinateur sont sauvegardées dans le compte OneDrive de l'utilisateur.

Vous pouvez afficher et gérer les clés de récupération stockées sur

votre compte OneDrive [ici](#).

[Haut de la page](#)

DirectAccess

### **Quel est le rôle de cette fonctionnalité ?**

DirectAccess permet à votre ordinateur de se connecter à distance et de façon transparente au réseau de votre lieu de travail chaque fois que votre ordinateur est connecté à Internet, quelle que soit votre localisation.

### **Informations collectées, traitées ou transmises**

Chaque fois que vous démarrez votre ordinateur, DirectAccess tente de se connecter à votre réseau professionnel, que vous vous trouviez sur votre lieu de travail ou non. Une fois connecté, l'ordinateur télécharge la stratégie de votre entreprise pour que vous puissiez accéder aux ressources configurées sur le réseau professionnel. Votre administrateur est susceptible de réutiliser la connectivité DirectAccess pour gérer et surveiller à distance votre ordinateur, y compris les sites Web que vous visitez même si vous ne vous trouvez pas sur votre lieu de travail.

DirectAccess n'envoie pas d'information à Microsoft.

### **Utilisation des informations**

Les stratégies de votre entreprise déterminent l'usage des informations recueillies par votre administrateur.

### **Choix et contrôle**

L'administrateur de votre lieu de travail doit configurer DirectAccess par le biais de la stratégie de groupe. Si votre administrateur peut vous autoriser à désactiver temporairement certains éléments de DirectAccess, il reste cependant le seul à pouvoir empêcher Windows d'essayer de se connecter à votre lieu de travail pour des besoins de gestion. Si vous ou l'administrateur de votre lieu de travail supprimez votre ordinateur de votre domaine professionnel, DirectAccess n'est alors plus en mesure de se connecter.

[Haut de la page](#)

Options d'ergonomie

### **Quel est le rôle de cette fonctionnalité ?**

Les options d'ergonomie vous permettent d'activer les options et les paramètres d'accessibilité afin d'interagir plus facilement avec l'ordinateur.

### **Informations collectées, traitées ou transmises**

Si vous faites appel à cette fonctionnalité, vous êtes alors invité à sélectionner les affirmations qui s'appliquent à votre cas.

Parmi ces affirmations, l'on retrouve les suivantes :

- Je distingue difficilement les images et le texte à la télévision.
- En raison des conditions d'éclairage, j'ai du mal à distinguer les images à l'écran.
- Je n'utilise pas de clavier.
- Je suis non-voyant.
- Je suis sourd.
- Je souffre de troubles d'élocution.

Ces informations sont enregistrées dans un format non lisible par l'utilisateur et sont stockées sur votre ordinateur.

### **Utilisation des informations**

Un ensemble de recommandations de configuration vous est proposé en fonction des affirmations que vous choisissez. Ces informations ne sont pas envoyées à Microsoft et mises à disposition des autres utilisateurs hormis vous et les administrateurs de votre ordinateur.

### **Choix et contrôle**

Pour choisir les affirmations qui s'appliquent à votre cas, accédez au Panneau de configuration, puis Options d'ergonomie. Vous pouvez modifier vos choix à tout moment. Vous avez également la possibilité de sélectionner les recommandations à configurer sur votre ordinateur.

[Haut de la page](#)

Observateur d'événements

### **Quel est le rôle de cette fonctionnalité ?**

Les utilisateurs d'ordinateur, principalement les administrateurs, peuvent faire appel à l'observateur d'événements pour afficher et gérer les journaux des événements. Ces derniers contiennent des informations relatives aux événements liés au matériel, aux logiciels et à la sécurité sur votre ordinateur. Vous pouvez également obtenir des informations auprès de Microsoft sur les événements dans ces journaux en cliquant sur Aide sur le Journal.

### **Informations collectées, traitées ou transmises**

Les journaux des événements contiennent des informations sur les événements générées par tous les utilisateurs et applications sur l'ordinateur. Par défaut, tous les utilisateurs peuvent consulter les entrées du journal des événements ; cependant, les administrateurs peuvent choisir de restreindre l'accès à ces journaux. Vous pouvez y accéder pour votre ordinateur en ouvrant l'observateur d'événements. Pour savoir comment accéder à l'observateur d'événements, voir Aide et support Windows.

Si vous utilisez l'Aide en ligne du Journal d'événements pour rechercher des informations supplémentaires sur un événement spécifique, les informations relatives à cet événement sont transmises à Microsoft.

### **Utilisation des informations**

Lorsque vous utilisez l'Aide en ligne du Journal d'événements pour rechercher des informations sur un événement, les données de l'événement envoyées par votre ordinateur servent à rechercher des informations supplémentaires sur l'événement et à vous les fournir. Dans le cas des événements Microsoft, les détails de chacun d'entre eux sont envoyés à Microsoft. Microsoft n'utilise pas ces informations pour vous identifier, vous contacter ou vous envoyer des publicités ciblées. Dans le cas d'événements associés à des applications de tiers, les informations sont envoyées à l'emplacement indiqué par l'éditeur ou le fabricant tiers. Si vous transmettez des informations relatives aux événements à ces tiers, l'usage de celles-ci est alors régi par les

différentes pratiques en matière de confidentialité de ces tiers.

## **Choix et contrôle**

Les administrateurs peuvent choisir de restreindre l'accès aux journaux de l'observateur d'événements. Les utilisateurs bénéficiant d'un accès complet aux journaux de l'observateur d'événements sont en mesure de les effacer. À moins que vous n'ayez accepté au préalable l'envoi automatique des informations sur les événements après avoir cliqué sur Aide en ligne du Journal d'événements, un message vous demande de confirmer l'envoi sur Internet des informations qui vous sont présentées. Aucune information de journal d'événements n'est envoyée par Internet à moins que vous n'acceptiez de l'envoyer. Les administrateurs peuvent faire appel à la stratégie de groupe pour sélectionner ou changer le site auquel les informations sur les événements sont envoyées.

[Haut de la page](#)

Contrôle parental

## **Quel est le rôle de cette fonctionnalité ?**

Le Contrôle parental permet aux parents de protéger leurs enfants lorsqu'ils utilisent un ordinateur. Les parents peuvent contrôler les applications, jeux et sites Web que les enfants sont autorisés à utiliser. Ils peuvent également définir des limites de durée et recevoir régulièrement des rapports d'activité par courrier électronique. De plus, ils peuvent gérer des restrictions et afficher des rapports d'activité localement sur l'ordinateur ou en ligne à l'aide du site Web du Contrôle parental Microsoft.

## **Informations collectées, traitées ou transmises**

Les paramètres de Contrôle parental et les rapports d'activité des enfants sont stockés sur votre ordinateur. Les rapports d'activité peuvent inclure des informations sur le temps passé à utiliser l'ordinateur, le temps passé dans des applications et jeux individuels, ainsi que les sites Web visités (y compris les tentatives d'afficher des sites bloqués). Les administrateurs de l'ordinateur peuvent modifier les paramètres et afficher le rapport d'activité.

Si la gestion en ligne est activée pour un compte enfant, les parents peuvent afficher le rapport d'activité de l'enfant et modifier ses paramètres sur le site Web du Contrôle parental Microsoft. Un parent peut autoriser d'autres personnes à afficher des rapports d'activité et à modifier des paramètres en les ajoutant en tant que parents sur le site Web du Contrôle parental Microsoft. Si le parent qui configure le Contrôle parental est connecté à Windows avec un compte Microsoft, la gestion en ligne est automatiquement activée.

Lorsque le Contrôle parental est configuré pour un compte enfant avec la gestion en ligne activée, des rapports hebdomadaires de l'activité de l'enfant sont automatiquement envoyés par courrier électronique au parent.

### **Utilisation des informations**

Windows et le site Web du Contrôle parental Microsoft utilisent les informations recueillies pour fournir les fonctionnalités du Contrôle parental. Microsoft peut analyser de manière globale les informations du journal d'activité afin de garantir la qualité des données, mais nous n'utilisons pas ces informations pour identifier les utilisateurs, les contacter ou leur envoyer des publicités ciblées.

### **Choix et contrôle**

Le Contrôle parental est désactivé par défaut. Vous pouvez accéder au Contrôle parental en ouvrant l'application Contrôle parental dans le Panneau de configuration. Seuls les administrateurs peuvent activer le Contrôle parental, et seuls les utilisateurs sans privilèges d'administration peuvent être surveillés ou restreints. Les enfants peuvent voir leurs paramètres, mais ne peuvent pas les modifier. Si le Contrôle parental est activé, l'enfant reçoit une notification indiquant que le Contrôle parental surveille son compte chaque fois qu'il se connecte à Windows. Si vous indiquez qu'un compte est un compte enfant lors de la création du compte, vous pouvez choisir d'activer le Contrôle parental pour ce compte.

Si l'administrateur configurant un compte enfant est connecté à Windows avec un compte Microsoft, la gestion en ligne est automatiquement activée, et des rapports sur l'activité de l'enfant sont envoyés chaque semaine. Il est possible d'ajouter ou de supprimer des comptes parents sur le site Web du Contrôle parental Microsoft. Toute

personne ajoutée en tant que parent sur le site Web peut voir le rapport d'activité d'un enfant et modifier les paramètres de Contrôle parental de l'enfant, même si le parent n'est pas administrateur sur l'ordinateur que l'enfant utilise.

Pour exploiter correctement le Contrôle parental, seuls les parents doivent être définis comme administrateurs de leur ordinateur, et les enfants ne doivent pas se voir accorder de privilèges d'administration. Notez que l'utilisation de cette fonctionnalité pour surveiller d'autres utilisateurs (notamment des adultes) peut constituer une violation de la loi applicable.

[Haut de la page](#)

Télécopie

### **Quel est le rôle de cette fonctionnalité ?**

La fonctionnalité de télécopie vous permet de créer et d'enregistrer les pages de couverture de fax, et d'envoyer et recevoir des fax par le biais de votre ordinateur, d'un modem fax externe ou intégré ou encore d'un serveur de télécopie.

### **Informations collectées, traitées ou transmises**

Les informations recueillies comprennent toutes les informations confidentielles entrées sur la page de couverture d'un fax, ainsi que les identifiants repris dans les protocoles de télécopie standard tels que l'ID d'abonné transmetteur (TSID, Transmitting Subscriber ID) et l'ID d'abonné appelant (CSID, Call Subscriber ID). Par défaut, Windows utilise la valeur « Fax » pour chaque identifiant.

### **Utilisation des informations**

Les informations entrées dans la boîte de dialogue de l'expéditeur sont reprises sur la page de couverture du fax. Les identifiants, tels que le TSID et le CSID, peuvent contenir un texte arbitraire et sont généralement utilisés par le télécopieur ou l'ordinateur en réception pour identifier l'expéditeur. Aucune information n'est envoyée à Microsoft.

### **Choix et contrôle**

Les privilèges de votre compte d'utilisateur configuré sur votre



ordinateur déterminent l'accès à la fonction de télécopie. À moins qu'un administrateur de télécopie modifie les paramètres d'accès, tous les utilisateurs sont en mesure d'envoyer et de recevoir des fax. Par défaut, tous les utilisateurs peuvent consulter les documents qu'ils envoient et n'importe quel fax reçu sur l'ordinateur. Les administrateurs ont accès à l'intégralité des fax, qu'ils soient envoyés ou reçus, et peuvent configurer les paramètres de télécopie, parmi lesquels les individus bénéficiant des autorisations pour afficher ou gérer les fax, ainsi que les valeurs de TSID et de CSID.

[Haut de la page](#)

Personnalisation de l'écriture manuscrite : apprentissage automatique

### **Quel est le rôle de cette fonctionnalité ?**

L'apprentissage automatique correspond à un outil de personnalisation de la reconnaissance de l'écriture manuscrite disponible sur les ordinateurs dotés d'un écran tactile ou sur les tablettes. Cette fonctionnalité collecte des données sur les mots que vous utilisez et la façon dont vous les écrivez. Cela aide le logiciel de reconnaissance de l'écriture manuscrite à améliorer son interprétation de votre style d'écriture manuscrite et de votre vocabulaire, mais aussi à améliorer la correction automatique et les suggestions de texte pour les langues ne disposant pas d'éditeur de méthode d'entrée (IME, Input Method Editor).

### **Informations collectées, traitées ou transmises**

Les informations que l'apprentissage automatique recueille sont stockées dans le profil de chaque utilisateur de l'ordinateur. Les données sont stockées dans un format propriétaire non lisible à travers une application d'affichage de texte (par exemple, le Bloc-notes ou WordPad) et ne sont disponibles pour les autres utilisateurs que s'ils sont des administrateurs de votre ordinateur.

Les informations recueillies sont les suivantes :

- le texte des messages que vous composez et les entrées de calendrier que vous créez par le biais d'applications de messagerie électronique (par exemple, Office Outlook ou Windows Live Mail), y compris tous les messages déjà envoyés ;

- l'encre utilisée pour écrire dans le Panneau de saisie ;
- le texte reconnu à partir de l'encre que vous utilisez dans le Panneau de saisie ou que vous tapez sur un clavier tactile ;
- les caractères de remplacement que vous sélectionnez pour corriger le texte reconnu.

### **Utilisation des informations**

Les informations recueillies contribuent à améliorer la reconnaissance de l'écriture manuscrite en créant une version du logiciel de reconnaissance, personnalisée selon vos propres style et vocabulaire, et à activer la correction automatique et les suggestions de texte au cours de la frappe sur des claviers tactiles.

Les échantillons de texte permettent de créer un dictionnaire étendu. Les échantillons d'encre contribuent à améliorer la reconnaissance de l'écriture manuscrite pour chaque utilisateur d'un ordinateur. Aucune information n'est envoyée à Microsoft.

### **Choix et contrôle**

La fonctionnalité d'apprentissage automatique est activée par défaut. Vous pouvez à tout moment activer ou désactiver l'apprentissage automatique en accédant à l'option **Paramètres avancés** dans la section **Langues** du Panneau de configuration. Lorsque vous désactivez l'apprentissage automatique, toutes les données qui ont été collectées et stockées par cette fonctionnalité sont supprimées.

[Haut de la page](#)

Groupe résidentiel

### **Quel est le rôle de cette fonctionnalité ?**

Windows vous permet d'interconnecter facilement des ordinateurs sur votre réseau domestique pour vous permettre de partager des images, de la musique, des vidéos, des documents et des périphériques. Il permet également aux ordinateurs de diffuser des données multimédias en continu aux périphériques de votre réseau domestique, tels qu'un extenseur de support. Ces ordinateurs et périphériques

constituent votre groupe résidentiel. Vous avez la possibilité de protéger votre groupe résidentiel à l'aide d'un mot de passe et d'indiquer ce que vous comptez partager.

### **Informations collectées, traitées ou transmises**

Vous pouvez accéder à vos propres fichiers, par exemple des images, des vidéos, de la musique et des documents, depuis n'importe quel ordinateur du groupe résidentiel. Lorsque vous rejoignez un groupe résidentiel, les informations de compte (notamment l'adresse de messagerie, le nom complet et l'image) pour chacun des comptes Microsoft sur votre ordinateur sont alors partagées avec les autres utilisateurs du groupe résidentiel afin de permettre le partage avec ceux-ci.

### **Utilisation des informations**

Les informations recueillies permettent aux ordinateurs de votre groupe résidentiel de déterminer avec qui partager le contenu et comment le présenter. Aucune information n'est envoyée à Microsoft.

### **Choix et contrôle**

Vous avez la possibilité d'ajouter ou de retirer des ordinateurs de votre groupe résidentiel et de décider de ce qui doit être partagé avec les autres membres du groupe résidentiel. Vous pouvez créer un groupe résidentiel et gérer ses paramètres en accédant à l'option **Groupe résidentiel** sous **Réseau** disponible dans Paramètres du PC.

[Haut de la page](#)

IME (éditeur de méthode d'entrée)

Les éditeurs de méthode d'entrée (IME, Input Method Editors) de Microsoft sont utilisés avec les langues d'Asie orientale pour convertir les saisies au clavier en idéogrammes. Cette section traite de plusieurs fonctionnalités, notamment le réglage automatique et la prédiction de l'éditeur IME, les rapports d'erreur de conversion de l'éditeur IME et l'enregistrement de mots IME.

## Candidats de l'éditeur IME du nuage

### **Quel est le rôle de cette fonctionnalité ?**

Lorsque vous utilisez l'éditeur IME Pinyin Microsoft pour entrer des caractères chinois simplifiés, il peut utiliser un service en ligne pour rechercher des idéogrammes candidats pour une entrée tapée qui n'existe pas dans un dictionnaire local de votre ordinateur.

### **Informations collectées, traitées ou transmises**

À mesure que vous tapez des caractères chinois simplifiés à l'aide de l'éditeur IME Pinyin Microsoft, ce dernier suggère des idéogrammes que vous pouvez choisir d'utiliser. Si l'éditeur IME ne trouve aucune suggestion appropriée dans votre dictionnaire local, il envoie la saisie au clavier à Microsoft pour déterminer s'il existe de meilleurs idéogrammes candidats pour cette entrée. Si tel est le cas, ils s'affichent dans la liste de candidats et, s'ils sont sélectionnés, ils sont ajoutés au dictionnaire local. Un identificateur unique généré de manière aléatoire est également envoyé pour nous aider à analyser l'utilisation de cette fonctionnalité. Cet identificateur n'est pas associé à votre compte Microsoft, et il n'est pas utilisé pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

### **Utilisation des informations**

Microsoft utilise les informations collectées pour rechercher des idéogrammes du nuage et pour améliorer la qualité de nos produits et services. Nous ne les utilisons pas pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

### **Choix et contrôle**

Les candidats IME du nuage sont désactivés par défaut pour l'éditeur IME Pinyin Microsoft du chinois simplifié. Pour modifier ce paramètre, ouvrez Paramètres du PC, cliquez sur **Heure et langue**, cliquez sur **Région et langue**, choisissez votre langue, puis cliquez sur **Options**.

## **Réglage automatique et prédiction de l'éditeur IME**

### **Quel est le rôle de cette fonctionnalité ?**

En fonction de l'éditeur IME que vous utilisez et de vos paramètres, les fonctionnalités de réglage automatique et de suggestion de texte de l'éditeur IME peuvent enregistrer des mots ou des séquences de mots destinés à améliorer la sélection des idéogrammes affichés.

## **Informations collectées, traitées ou transmises**

Les fonctionnalités de réglage automatique de l'éditeur IME (auto-apprentissage) et de suggestion de texte enregistrent un mot ou une séquence de mots ainsi que la fréquence à laquelle vous l'utilisez. Les informations de réglage automatique (à l'exception de toute séquence de chiffres/symboles) sont stockées dans des fichiers distincts pour chaque utilisateur d'un ordinateur.

## **Utilisation des informations**

Les données d'apprentissage automatique et de suggestion de texte servent à l'éditeur IME sur votre ordinateur pour améliorer la sélection d'idéogrammes affichés pendant l'usage de l'éditeur IME. Si vous choisissez d'envoyer ces données à Microsoft, celles-ci sont alors utilisées pour améliorer l'éditeur IME et les produits et services correspondants.

## **Choix et contrôle**

Les fonctionnalités d'apprentissage automatique et de suggestion de texte sont activées par défaut dans les éditeurs IME les prenant en charge. Les données collectées ne sont pas automatiquement envoyées à Microsoft. Vous pouvez indiquer de recueillir ou d'envoyer ou non ces données dans le Panneau de configuration, puis dans la section Langue.

## **Rapports d'erreur de conversion par l'éditeur IME**

### **Quel est le rôle de cette fonctionnalité ?**

Si des erreurs se produisent lors de la présentation d'idéogrammes ou pendant la conversion de la saisie au clavier en idéogrammes, cette fonctionnalité peut collecter des informations sur les erreurs afin d'aider Microsoft à améliorer ses produits et services.

## **Informations collectées, traitées ou transmises**

La génération de rapports d'erreur de conversion d'éditeur IME recueille des informations sur les erreurs de conversion commises par l'éditeur IME, par exemple ce que vous tapez, le premier résultat de conversion ou de prédiction, la chaîne choisie en remplacement, des informations relatives à l'éditeur IME que vous utilisez ainsi que des

informations sur l'usage que vous en faites. De plus, si vous utilisez l'éditeur IME pour le japonais, il vous est possible d'inclure des informations sur l'apprentissage automatique dans les rapports d'erreur de conversion.

### **Utilisation des informations**

Microsoft s'appuie sur ces renseignements pour améliorer ses produits et services. Microsoft n'utilise pas ces informations pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

### **Choix et contrôle**

À l'issue d'un volume suffisant d'erreurs de conversion conservées, l'outil de rapport de mauvaise conversion vous demande si vous comptez envoyer un rapport d'erreur de conversion. Il vous est également possible d'envoyer à tout moment un tel rapport à partir de l'outil de rapport de mauvaise conversion de l'éditeur IME. Vous pouvez afficher les informations reprises dans chaque rapport avant d'indiquer de l'envoyer. Vous pouvez aussi activer l'envoi automatique des rapports d'erreur de conversion dans Paramètres IME.

## **Enregistrement de mot de l'éditeur IME**

### **Quel est le rôle de cette fonctionnalité ?**

En fonction de l'éditeur IME que vous utilisez, vous pouvez parfois exploiter l'enregistrement de mots pour faire état des mots non pris en charge (c'est-à-dire des mots saisis au clavier, susceptibles de ne pas être correctement convertis en idéogrammes).

### **Informations collectées, traitées ou transmises**

Les rapports d'enregistrement peuvent comprendre des informations que vous fournissez dans la boîte de dialogue Ajouter un mot, pour les mots à rapporter, et le numéro de version du logiciel correspondant à un éditeur IME. Ces rapports peuvent inclure des informations confidentielles, par exemple, si vous ajoutez des noms de personnes par le biais de l'enregistrement de mots. Vous avez la possibilité de passer en revue les données dans chaque rapport avant d'opter pour son envoi ou non.

### **Utilisation des informations**

Microsoft s'appuie sur ces renseignements pour contribuer à améliorer

ses produits et services. Microsoft n'utilise pas ces informations pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

## **Choix et contrôle**

Chaque fois que vous créez un rapport d'enregistrement de mots, il vous est demandé si vous comptez envoyer le rapport à Microsoft. Vous pouvez afficher les informations reprises dans le rapport avant d'indiquer de l'envoyer.

[Haut de la page](#)

Partage de connexion Internet

### **Quel est le rôle de cette fonctionnalité ?**

Le partage de connexion Internet vous permet de partager votre connexion Internet haut débit mobile avec d'autres appareils par Wi-Fi. Vous pouvez également démarrer à distance le partage de connexion Internet sur votre appareil haut débit mobile à partir de votre ordinateur si vous êtes connecté aux deux à l'aide du même compte Microsoft.

### **Informations collectées, traitées ou transmises**

Si vous partagez votre connexion Internet pour la première fois, Windows génère et stocke automatiquement un nom et un mot de passe réseau. Vous pouvez modifier ces éléments à tout moment.

Si votre ordinateur prend en charge cette opération, et si vous avez ajouté votre ordinateur à votre compte Microsoft en tant qu'appareil de confiance, Windows synchronise le nom et le mot de passe réseau sur votre compte Microsoft. Windows synchronise également d'autres informations pour vous permettre de démarrer à distance le partage de connexion Internet à partir de vos autres appareils de confiance. Ces informations comprennent notamment l'adresse matérielle de votre adaptateur Bluetooth et un numéro aléatoire utilisé pour renforcer la sécurité de la connexion.

### **Utilisation des informations**

Ces informations sont utilisées pour configurer le partage de connexion Internet. Microsoft n'utilise pas ces informations pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

## **Choix et contrôle**

Si vous vous connectez à un appareil qui prend en charge le partage de connexion Internet à l'aide de votre compte Microsoft, et que vous ajoutez cet appareil en tant qu'appareil de confiance, les informations nécessaires pour démarrer à distance le partage de connexion Internet sont synchronisées sur OneDrive. Vous pouvez arrêter la synchronisation des informations en choisissant de ne pas synchroniser les mots de passe. Pour plus d'informations, voir la section « Synchroniser les paramètres » dans cette page.

[Haut de la page](#)

Impression Internet

### **Quel est le rôle de cette fonctionnalité ?**

L'impression Internet vous permet d'imprimer en faisant transiter les données par Internet.

### **Informations collectées, traitées ou transmises**

Lorsque vous imprimez à l'aide de cette fonctionnalité, vous devez au préalable vous connecter et vous authentifier auprès d'un serveur d'impression Internet. Les informations que vous devez soumettre au serveur d'impression varient en fonction du niveau de sécurité que le serveur prend en charge (par exemple, il peut vous être demandé de fournir un nom et un mot de passe utilisateur). Une fois que vous êtes connecté, une liste répertoriant les imprimantes compatibles vous est présentée. Si votre ordinateur ne possède pas de pilote pour l'imprimante sélectionnée, vous pouvez télécharger un pilote depuis le serveur d'impression. Les travaux d'impression n'étant pas chiffrés, il est possible que d'autres utilisateurs puissent consulter le contenu envoyé.

### **Utilisation des informations**

Les informations recueillies vous permettent d'imprimer par le biais d'imprimantes distantes. Si vous choisissez de faire appel à un serveur d'impression hébergé par Microsoft, nous n'utilisons pas les informations que vous fournissez pour vous identifier, vous contacter ou vous envoyer des publicités ciblées. Si vous transmettez des



informations à un serveur d'impression tiers, l'utilisation de celles-ci est alors régie par les différentes pratiques de ce tiers en matière de confidentialité.

## **Choix et contrôle**

Vous pouvez activer ou désactiver l'impression Internet en ouvrant, dans le Panneau de configuration, l'option **Programmes et fonctionnalités**, puis en sélectionnant **Activer ou désactiver des fonctionnalités Windows**.

[Haut de la page](#)

Préférences linguistiques

## **Quel est le rôle de ces fonctionnalités ?**

Vous pouvez ajouter les langues que vous utilisez le plus souvent dans votre liste de langues dans Windows 8.1. Les applications et les sites Web s'affichent dans la première langue disponible dans cette liste.

## **Informations collectées, traitées ou transmises**

Lorsque vous visitez des sites Web ou que vous installez des applications sur votre ordinateur, votre liste de langues préférées est transmise aux sites et mise à la disposition des applications pour que ces derniers affichent le contenu dans vos langues préférées.

## **Utilisation des informations**

Votre liste de langues préférées est utilisée par les applications et sites Web de Microsoft pour afficher le contenu dans vos langues préférées. Microsoft n'utilise pas ces informations de langue pour vous identifier ou vous contacter. Les informations de langue envoyées ou utilisées par des sites Web ou applications tiers sont soumises aux règles de confidentialité appliquées par les éditeurs de ces sites Web ou applications.

## **Choix et contrôle**

Votre liste de langues préférées peut être utilisée par les applications que vous installez et par les sites Web que vous visitez. Vous pouvez ajouter ou supprimer des langues dans cette liste via l'option Langues du Panneau de configuration. Si vous n'avez défini aucune langue dans

cette liste, c'est la langue que vous avez choisie dans l'onglet Formats du Panneau de configuration Région qui est transmise aux sites Web visités.

[Haut de la page](#)

## Services de localisation

Les services de localisation Windows vous permettent de déterminer les applications, sites Web et fonctionnalités Windows que vous voulez autoriser à déterminer la localisation de votre ordinateur. Les services de localisation Windows se composent de deux composants. Le Service de localisation Windows se connecte à un service en ligne Microsoft pour déterminer votre localisation. La plateforme de localisation Windows détermine l'emplacement de votre ordinateur par le biais d'un matériel, tel qu'un capteur GPS, ou d'un logiciel, par exemple le Service de localisation Windows.

## Plateforme de localisation Windows

### **Quel est le rôle de cette fonctionnalité ?**

Si vous choisissez d'activer la plateforme de localisation Windows, les applications que vous installez à partir du Windows Store, ainsi que certaines fonctionnalités Windows, peuvent demander l'autorisation de déterminer la localisation de votre ordinateur. Si vous laissez une application utiliser votre localisation, en plus de fournir votre localisation pendant que vous utilisez l'application, la plateforme de localisation Windows peut indiquer à l'application quand votre ordinateur se déplace à l'intérieur ou à l'extérieur de limites géographiques définies par l'application. Par exemple, une application peut vous permettre de définir un rappel indiquant que vous devez passer à l'épicerie en sortant du travail. En fonction de la configuration de votre système, il se peut que la plateforme de localisation Windows détermine l'emplacement de votre ordinateur par le biais d'un matériel, tel qu'un capteur GPS, ou d'un logiciel, par exemple le Service de localisation Windows.

La plateforme de localisation Windows n'empêche pas les applications de déterminer l'emplacement de votre ordinateur par le biais d'autres méthodes. Par exemple, vous pouvez installer des appareils (tel qu'un récepteur GPS) pouvant envoyer des informations de localisation

directement à une application et contourner ainsi la plateforme. Indépendamment de vos paramètres de plateforme de localisation Windows, les services en ligne peuvent utiliser votre adresse IP pour déterminer son emplacement approximatif, généralement la ville où votre ordinateur se trouve.

### **Informations collectées, traitées ou transmises**

La plateforme de localisation Windows ne transmet pas en soi d'informations à partir de votre ordinateur, mais chaque service de localisation (par exemple le Service de localisation Windows) est en mesure de transférer des informations lorsque la plateforme de localisation Windows leur demande de déterminer la localisation de votre ordinateur. Les applications, sites Web et fonctionnalités autorisés à exploiter la plateforme de localisation pour déterminer le lieu où se trouve votre ordinateur peuvent en outre transmettre ou stocker ces informations. Si une application configure des limites géographiques à surveiller, ces limites sont stockées sur votre ordinateur. Les informations stockées concernant ces limites sont notamment un nom, un emplacement, ainsi que la présence de votre ordinateur à l'intérieur ou à l'extérieur de la limite la dernière fois que sa localisation a été déterminée. Les applications qui configurent des limites géographiques sont susceptibles de transmettre ces informations.

### **Utilisation des informations**

Si vous activez la plateforme de localisation Windows, les applications, sites Web et fonctionnalités Windows autorisés sont alors en mesure de connaître la localisation de votre ordinateur et de s'appuyer sur cette dernière pour vous présenter du contenu personnalisé. Si vous faites appel à un service de localisation ou une application d'un tiers, l'utilisation de la localisation de votre ordinateur est soumise aux pratiques de ce tiers en matière de confidentialité. Avant de télécharger une application du Windows Store, vous pouvez savoir, dans sa description, si elle exploite des technologies de localisation.

### **Choix et contrôle**

Si vous optez pour la configuration rapide de Windows, la plateforme de localisation Windows est alors activée. Si vous choisissez de personnaliser les paramètres, vous pouvez contrôler la plateforme de

localisation Windows en sélectionnant Permettre à Windows et aux applications de demander mon emplacement à partir de la plateforme de localisation Windows sous Partager des informations avec Microsoft et d'autres services. La première fois où une application du Windows Store demande la localisation de votre ordinateur, Windows vous demande si vous souhaitez autoriser l'application à utiliser ces données. Vous pouvez consulter et modifier ce paramètre dans les options Autorisations accessibles depuis les paramètres de chaque application du Windows Store.

Si vous utilisez une application de bureau qui utilise la plateforme de localisation Windows, elle doit vous demander l'autorisation d'utiliser les données de localisation de votre ordinateur. Lorsqu'elle y accède, une icône apparaît dans la zone de notification pour vous informer que les données de localisation de votre ordinateur ont fait l'objet d'un accès. Chaque utilisateur peut contrôler ses propres paramètres de localisation pour les applications dans la section **Confidentialité** de Paramètres du PC. En outre, les administrateurs sont en mesure de désactiver la plateforme de localisation pour tous les utilisateurs dans la section **Paramètres de localisation** du Panneau de configuration. Pour empêcher l'envoi de notification aux applications lorsque les limites géographiques qu'elles ont définies sont franchies, un utilisateur administratif peut désactiver le Service d'infrastructure de localisation Windows dans le Panneau de configuration.

## Service de localisation Windows

### **Quel est le rôle de cette fonctionnalité ?**

Le service de localisation Windows se connecte au service de localisation Microsoft en ligne chargé de déterminer la localisation approximative de votre ordinateur en s'appuyant sur son adresse IP et celle des réseaux Wi-Fi avoisinants.

### **Informations collectées, traitées ou transmises**

Quand une application, que vous avez autorisée à accéder à vos données de localisation, demande votre emplacement géographique, la plateforme de localisation Windows interroge tous les services de localisation installés (y compris le service de localisation Windows) afin de déterminer la localisation actuelle de votre ordinateur. Le service de localisation Windows vérifie d'abord s'il dispose d'une liste des points

d'accès Wi-Fi avoisinants en mémoire établie lors d'une demande précédente par une application de géolocalisation. Si une telle liste n'existe pas ou si celle-ci n'est pas à jour, le service envoie des informations relatives aux points d'accès Wi-Fi les plus proches, ainsi que les détails GPS, le cas échéant, au service de localisation Microsoft. Ce dernier retourne ensuite l'emplacement approximatif de votre ordinateur au service de localisation, lequel le transmet à son tour à la plateforme de localisation Windows afin qu'elle puisse la fournir à l'application l'ayant demandée. Le service de localisation Windows met éventuellement à jour sa liste des points d'accès Wi-Fi établie. Le service de localisation Windows conserve cette liste afin de pouvoir déterminer l'emplacement approximatif de votre ordinateur sans avoir à se connecter systématiquement à Internet. Cette liste des points d'accès est chiffrée lorsqu'elle est stockée sur le disque afin que les applications ne puissent pas y accéder directement.

Les informations sur les points d'accès Wi-Fi à proximité qui sont envoyées comprennent le BSSID (à savoir l'adresse MAC du point d'accès Wi-Fi) et la puissance du signal. Les renseignements GPS, pour leur part, incluent la latitude, la longitude, la direction, la vitesse et l'altitude observées. Pour préserver la confidentialité de vos informations personnelles, le service de localisation Windows n'envoie aucune information permettant d'identifier de manière unique votre ordinateur autre que les informations standard sur l'ordinateur envoyées lors de toute connexion à Internet. Pour préserver la confidentialité des informations personnelles des propriétaires des réseaux Wi-Fi, Windows ne transmet pas d'informations sur les SSID (nom des points d'accès Wi-Fi) ou réseaux Wi-Fi masqués. À des fins de confidentialité et de sécurité, les informations envoyées relatives aux réseaux Wi-Fi transmises sont chiffrées via SSL.

Si vous choisissez de contribuer à l'amélioration du Service de localisation Microsoft, Windows peut renvoyer des informations relatives aux points d'accès Wi-Fi à Microsoft lorsqu'une application demande l'emplacement de votre PC. Si vous utilisez une connexion Internet limitée, Windows limite le nombre de transmissions quotidiennes de ce type d'informations afin de limiter l'usage de votre connexion Internet.

## **Utilisation des informations**

Le service de localisation Windows utilise ces informations pour fournir la localisation approximative de votre ordinateur à la plateforme de localisation Windows lorsqu'une application autorisée la demande.

Si vous décidez de contribuer à améliorer le service de localisation Microsoft, les renseignements Wi-Fi et GPS envoyés à Microsoft sont exploités pour améliorer les services de localisation de Microsoft et, par conséquent, la pertinence des applications qui en dépendent. Microsoft ne conserve aucune donnée collectée par ce service qui pourrait permettre de vous identifier, vous contacter, vous envoyer de la publicité, suivre l'emplacement de votre ordinateur ou créer un historique de ses emplacements.

### **Choix et contrôle**

Le service de localisation Windows n'est sollicité que si une application autorisée demande la localisation de votre ordinateur. Pour plus d'informations sur la manière de contrôler l'autorisation ou le refus aux applications de demander la localisation de votre ordinateur, voir la section Plateforme de localisation Windows. Si vous autorisez des applications à demander le lieu où se trouve votre ordinateur, la liste mise en cache des emplacements des points d'accès Wi-Fi à proximité, chiffrés et stockés par le service de localisation Windows est supprimée et remplacée régulièrement.

Si vous optez pour la configuration rapide de Windows, l'option de contribution à l'amélioration du service de localisation Microsoft est activée. Si vous choisissez de personnaliser les paramètres, vous pouvez indiquer si vous comptez contribuer à améliorer les services de localisation Microsoft en sélectionnant **Envoyer des données d'emplacement à Microsoft quand des applications de géolocalisation sont utilisées** sous **Participer à l'amélioration des produits et services Microsoft**. Après avoir configuré Windows, vous pouvez modifier ce paramètre dans la section Paramètres de localisation du Panneau de configuration. Si vous choisissez de ne pas aider à améliorer le service, vous avez toujours la possibilité d'exploiter le service de localisation Windows pour déterminer la localisation approximative de votre ordinateur.

Vous pouvez activer et désactiver le service de localisation Windows par le biais de la section **Activer ou désactiver des fonctionnalités**

**Windows** du Panneau de configuration. Si vous désactivez le service de localisation Windows, vous pouvez néanmoins utiliser d'autres services de localisation (par exemple, le GPS) par le biais de la plateforme de localisation Windows.

[Haut de la page](#)

Gérer vos informations d'identification

### **Quel est le rôle de cette fonctionnalité ?**

Windows vous permet de connecter des applications du Windows Store à des comptes que vous utilisez pour des sites Web. Si vous avez précédemment enregistré un mot de passe pour un site Web dans Internet Explorer, Windows peut utiliser ce mot de passe enregistré lorsque vous connectez une application à ce site Web.

### **Informations collectées, traitées ou transmises**

Lorsqu'une application demande des informations d'identification pour se connecter à un site Web, vous pouvez choisir d'enregistrer ces informations d'identification. Si vous vous êtes déjà connecté au site Web dans Internet Explorer et que vous avez choisi d'enregistrer vos informations d'identification, Windows remplit automatiquement les informations d'identification enregistrées. Ces informations d'identification sont stockées sur votre ordinateur. Pour plus d'informations sur la façon dont ces informations d'identification et d'autres informations peuvent être synchronisées avec OneDrive, voir la section « Synchroniser les paramètres » dans cette page.

### **Utilisation des informations**

Windows utilise uniquement les informations d'identification enregistrées pour vous aider à vous connecter aux sites Web que vous avez sélectionnés. Si vous enregistrez des informations d'identification lors de la connexion d'une application à un site Web, ces informations d'identification enregistrées ne sont pas utilisées dans Internet Explorer ou d'autres applications.

### **Choix et contrôle**

Vous pouvez gérer les informations d'identification enregistrées dans le Gestionnaire d'informations d'identification du Panneau de

configuration. Pour plus d'informations sur la façon dont ces informations d'identification et d'autres informations peuvent être synchronisées avec OneDrive, voir la section « Synchroniser les paramètres » dans cette page.

[Haut de la page](#)

Nom et avatar de compte

### **Quel est le rôle de cette fonctionnalité ?**

Pour vous proposer du contenu personnalisé, les applications peuvent demander à Windows votre nom et l'avatar de votre compte. Votre nom et l'avatar de votre compte s'affichent sous Paramètres du PC, dans la zone **Votre compte** dans la section **Comptes** . Si vous vous connectez à Windows à l'aide d'un compte Microsoft, Windows utilise le nom et l'avatar associés au compte en question. Si vous n'avez pas choisi d'avatar pour votre compte, Windows vous en fournit un par défaut.

### **Informations collectées, traitées ou transmises**

Si vous autorisez des applications à accéder à votre nom et à l'avatar de votre compte, Windows fournit ces informations à toutes les applications qui les demandent. Les applications sont susceptibles de stocker ou de transmettre ces données.

Si vous vous connectez à Windows à l'aide d'un compte de domaine et que vous autorisez les applications à utiliser votre nom et l'avatar de votre compte, celles capables d'exploiter vos informations d'identification Windows sont alors en mesure d'accéder à d'autres formes d'informations particulières relatives à votre compte de domaine. Ces informations comprennent, entre autres, votre nom d'utilisateur principal (par exemple, jacques@contoso.com) et le nom de domaine DNS (par exemple, corp.contoso.com\jacques).

Si vous vous connectez à Windows à l'aide d'un compte Microsoft, ou si vous vous connectez à Windows à l'aide d'un compte de domaine associé au compte Microsoft, Windows peut synchroniser automatiquement l'avatar de votre compte sur votre ordinateur et celui du compte Microsoft.

### **Utilisation des informations**



Si vous faites appel à une application tierce, l'utilisation de votre nom et de l'avatar de votre compte est soumise aux pratiques de confidentialité de la tierce partie. Si vous utilisez une application Microsoft, les pratiques en matière de confidentialité inhérentes à l'application sont expliquées dans sa déclaration de confidentialité.

### **Choix et contrôle**

Si vous optez pour la configuration rapide de Windows, Windows autorise dans ce cas les applications à accéder à votre nom et à l'image de votre compte. Si vous choisissez de personnaliser les paramètres, vous pouvez contrôler l'accès à votre nom et à l'avatar de votre compte en sélectionnant **Permettre aux applications d'utiliser mon nom et l'avatar de mon compte** sous **Partager des informations avec Microsoft**. Après avoir configuré Windows, vous pouvez modifier ce paramètre dans la section **Confidentialité** des paramètres de l'ordinateur. Vous pouvez changer l'avatar de votre compte dans la section **Comptes** des paramètres de l'ordinateur. Il vous est également possible d'autoriser certaines applications à changer l'avatar de votre compte.

[Haut de la page](#)

Reconnaissance du réseau

### **Quel est le rôle de cette fonctionnalité ?**

Si vous disposez d'un abonnement à un accès réseau (par exemple, à travers une connexion haut débit mobile), cette fonctionnalité fournit aux applications et aux fonctionnalités de Windows installées sur votre ordinateur, des informations relatives à votre abonnement. Les fonctionnalités de Windows et les applications peuvent exploiter ces informations pour optimiser leur fonctionnement. Par exemple, si vous possédez un plan de facturation à l'usage, Windows Update attend avant de distribuer les mises à jour de priorité plus faible à votre ordinateur jusqu'à ce que vous vous connectiez à un autre type de réseau. Cette fonctionnalité offre également des informations sur votre connexion réseau, telles que la puissance du signal et l'état de connexion de votre ordinateur à Internet.

### **Informations collectées, traitées ou transmises**

Cette fonctionnalité recueille des renseignements de connectivité réseau Internet et intranet, tels que le suffixe DNS (Domain Name Service) de votre ordinateur, le nom du réseau et l'adresse de la passerelle des réseaux auxquels votre ordinateur se connecte. Cette fonctionnalité reçoit en outre des détails sur l'abonnement, comme le volume de données restant autorisé par l'abonnement.

Les profils de connectivité réseau peuvent inclure un historique de tous les réseaux visités et la date et l'heure de la dernière connexion. Cette fonctionnalité peut tenter de se connecter à un serveur Microsoft pour déterminer si vous êtes connecté à Internet. Les seules données envoyées à Microsoft lors des vérifications de connectivité réseau correspondent à des informations standard sur l'ordinateur.

### **Utilisation des informations**

Si des données sont envoyées à Microsoft, celles-ci ne sont utilisées que pour fournir l'état de la connectivité réseau. Ce dernier est communiqué aux applications et aux fonctionnalités installées sur votre ordinateur, demandant des informations sur la connectivité réseau. Si vous faites appel à une application tierce, l'utilisation des informations recueillies est soumise aux pratiques de confidentialité de la tierce partie.

### **Choix et contrôle**

La reconnaissance du réseau est activée par défaut. Un administrateur peut désactiver cette fonctionnalité par le biais du Panneau de configuration, dans Outils d'administration, puis dans les options Services. La désactivation de cette fonctionnalité n'est pas recommandée car cela empêche certaines fonctionnalités de Windows de fonctionner correctement.

[Haut de la page](#)

Notifications, applications de l'écran de verrouillage et mises à jour de vignettes

Les applications du Windows Store peuvent recevoir automatiquement du contenu et afficher des notifications de différentes manières. Elles peuvent, par exemple, recevoir des notifications qui s'affichent brièvement dans l'angle de l'écran ou sur des vignettes d'application si

ces vignettes sont épinglées à l'écran d'accueil. Vous pouvez également, si vous le souhaitez, recevoir ces notifications sur l'écran de verrouillage. L'écran de verrouillage peut également afficher un état détaillé ou bref de certaines applications. Les éditeurs d'applications peuvent envoyer du contenu à vos applications du Windows Store via les Services de notifications Push Windows (WNS) s'exécutant sur les serveurs Microsoft, ou les applications peuvent télécharger des informations directement à partir de serveurs tiers.

## Notifications

### **Quel est le rôle de cette fonctionnalité ?**

Les applications du Windows Store peuvent vous fournir des informations périodiques ou en temps réel sous forme de notifications brèves dans le coin de l'écran.

### **Informations collectées, traitées ou transmises**

Les applications peuvent afficher du texte, des images ou les deux dans des notifications. Le contenu de notifications peut être fourni localement par l'application (par exemple, une alarme provenant d'une application horloge). Les notifications peuvent également être envoyées à partir du service en ligne d'une application via les Services de notifications Push Windows (WNS) (par exemple, une notification de réseau social). Les images affichées dans les notifications peuvent être téléchargées directement à partir d'un serveur spécifié par l'éditeur de l'application ; dans ce cas, les informations standard de l'ordinateur sont envoyées à ce serveur.

### **Utilisation des informations**

Microsoft utilise les informations des notifications uniquement pour permettre aux applications de vous les livrer. La notification peut être stockée temporairement par les Services de notifications Push Windows (WNS) avant d'être livrée à votre ordinateur. Si une notification ne peut pas être délivrée immédiatement, elle est alors conservée pendant quelques minutes uniquement avant d'être supprimée.

### **Choix et contrôle**

Vous pouvez désactiver les notifications pour toutes les applications ou pour des applications précises, en accédant à **Notifications** sous

**Rechercher des applications** dans Paramètres du PC. Si vous désactivez les notifications pour une application ou que vous désinstallez cette dernière, son éditeur est néanmoins en mesure d'envoyer les mises à jour aux Services de notifications Push Windows (WNS), mais ces notifications ne s'affichent pas sur votre ordinateur.

## Applications de l'écran de verrouillage

### Quel est le rôle de cette fonctionnalité ?

Certaines applications du Windows Store peuvent afficher l'état et les notifications sur l'écran lorsque votre ordinateur est verrouillé. Les applications de l'écran de verrouillage peuvent également effectuer des tâches pendant que l'ordinateur est verrouillé, comme synchroniser le courrier électronique en arrière-plan ou vous laisser répondre aux appels téléphoniques entrants. Vous pouvez également utiliser la caméra de votre ordinateur directement à partir de l'écran de verrouillage.

### Informations collectées, traitées ou transmises

Les applications de l'écran de verrouillage peuvent recevoir des mises à jour d'état de leur éditeur via les Services de notifications Push Windows (WNS), ou directement des serveurs de leurs éditeurs ou d'un tiers. Les applications de l'écran de verrouillage peuvent également transmettre ou traiter d'autres informations non liées à des notifications et mises à jour.

### Utilisation des informations

Windows utilise les informations d'état et de notification fournies par les applications de l'écran de verrouillage pour mettre à jour l'écran de verrouillage.

### Choix et contrôle

Une fois Windows installé, les applications Courrier, Calendrier et Skype sont automatiquement définies en tant qu'applications de l'écran de verrouillage. Vous pouvez ajouter ou supprimer ces applications, ou d'autres, dans l'écran de verrouillage, et désactiver l'utilisation de la Caméra dans **Écran de verrouillage** sous **PC et périphériques** dans Paramètres du PC. Vous pouvez également choisir une application pour afficher de manière persistante un état détaillé (par exemple, les détails du prochain rendez-vous de votre

calendrier) sur l'écran de verrouillage.

Vous pouvez déterminer si les applications de l'écran de verrouillage peuvent afficher des notifications sur l'écran de verrouillage dans la section **Notifications** sous **Rechercher des applications** disponible dans Paramètres du PC.

## Mises à jour de vignettes

### Quel est le rôle de cette fonctionnalité ?

Les applications du Windows Store peuvent vous fournir des informations régulièrement ou en temps réel qui entraînent la mise à jour des vignettes de vos applications dans l'écran d'accueil.

### Informations collectées, traitées ou transmises

Les applications du Windows Store épinglées à l'écran d'accueil peuvent mettre à jour leur vignette avec du texte, des images, ou les deux. Le contenu affiché sur la vignette d'une application peut être fourni par l'application, téléchargé régulièrement à partir d'un serveur spécifié par l'éditeur de l'application ou envoyé à partir d'un service en ligne de l'application via les Services de notifications Push Windows (WNS). Si le contenu de la vignette est téléchargé directement à partir d'un serveur spécifié par l'éditeur de l'application, les informations standard de l'ordinateur sont envoyées à ce serveur.

### Utilisation des informations

Microsoft utilise uniquement les informations de vignette pour vous remettre les mises à jour de vignettes de vos applications. Ces informations peuvent être stockées temporairement par le Service de notification Push Windows (WNS) avant d'être remises à votre ordinateur. Si une mise à jour de vignette ne peut pas être délivrée immédiatement, elle est conservée quelques jours avant d'être supprimée.

### Choix et contrôle

Dès lors qu'une application a commencé à recevoir des mises à jour de vignette, vous pouvez les désactiver en sélectionnant la vignette de l'application dans l'écran d'accueil et en sélectionnant **Vignette désactivée** dans les commandes disponibles pour l'application. Si vous détachez la vignette d'une application de l'écran d'accueil, ses

mises à jour de vignette ne s'affichent pas. Si vous désinstallez une application, son éditeur est néanmoins en mesure d'envoyer les mises à jour aux Services de notifications Push Windows (WNS), mais elles ne s'affichent pas sur votre ordinateur.

Pour effacer les mises à jour actuellement affichées dans vos vignettes de l'écran d'accueil, balayez de droite à gauche ou pointez dans la partie supérieure droite de l'écran d'accueil, appuyez ou cliquez sur **Paramètres**, puis sur **Vignettes**. Appuyez ou cliquez sur le bouton **Effacer** sous **Effacer les informations personnelles de mes vignettes**. Les mises à jour de vignettes remises après que vous avez effacé les mises à jour actuelles continuent à s'afficher.

[Haut de la page](#)

Commander des tirages

### **Quel est le rôle de cette fonctionnalité ?**

La fonction Commander des tirages vous permet d'envoyer des images numériques stockées sur votre ordinateur ou sur un lecteur réseau au service de développement de photos en ligne de votre choix. Selon le service choisi, vous pouvez obtenir l'impression de vos images pour qu'elles vous soient livrées par courrier postal ou que vous pouvez passer prendre à un magasin proche.

### **Informations collectées, traitées ou transmises**

Si vous choisissez de passer une commande auprès d'un service d'impression de photographies en ligne, vos photos numériques sont alors envoyées par Internet au service que vous avez sélectionné. Le chemin d'accès aux photos numériques que vous sélectionnez (lequel est susceptible d'inclure votre nom d'utilisateur) peut être envoyé au service afin de permettre à ce dernier d'afficher et de télécharger les images. Les fichiers des images numériques sont à même de contenir des données sur les images stockées par l'appareil photo avec le fichier, par exemple la date et l'heure de prise de chaque image ou son lieu si votre appareil possède des fonctionnalités GPS. Les fichiers peuvent en outre renfermer des informations confidentielles (telles que des légendes) pouvant être associées au fichier lors de l'usage d'applications de gestion d'images numériques et de l'Explorateur de

fichiers. Pour plus d'informations, voir la section « Propriétés », ci-dessous.

Après avoir sélectionné un service d'impression de photographies en ligne dans la section Commander des tirages, vous êtes alors redirigé vers le site Web du service dans la fenêtre Commander des tirages. Les informations que vous entrez sur le site Web des services d'impression photographique en ligne sont fournies au service choisi.

### **Utilisation des informations**

Les informations stockées dans les fichiers d'image numérique par l'appareil photo peuvent être utilisées par le service d'impression photographique en ligne au cours du processus d'impression, par exemple, pour régler la couleur ou la netteté de l'image avant son tirage. Les informations que les applications de gestion d'images numériques stockent sont susceptibles d'être exploitées par le service d'impression de photographies en ligne pour les imprimer sous forme de légendes au recto ou au verso de la copie imprimée. L'usage de ces informations par les services d'impression de photographies en ligne, ainsi que des autres informations que vous fournissez à ces services comme celles que vous entrez sur leur site Web, est soumis à leurs pratiques en matière de confidentialité.

### **Choix et contrôle**

Vous pouvez passer par la fonctionnalité Commander des tirages pour choisir les images à envoyer et à quel service faire appel pour développer vos photographies. Certaines applications de gestion d'images peuvent vous proposer de supprimer les informations confidentielles stockées avant l'envoi des images à l'impression. Vous pouvez également bénéficier de la modification des propriétés du fichier pour supprimer ces informations confidentielles.

[Haut de la page](#)

Prérécupération et prélançement

### **Quel est le rôle de cette fonctionnalité ?**

Les applications d'aide de Windows et les fonctionnalités Windows se lancent plus rapidement grâce au suivi des éléments suivants : quand et à quelle fréquence ces applications et fonctionnalités sont utilisées,

quels sont les fichiers système qui les chargent.

### **Informations collectées, traitées ou transmises**

Quand vous utilisez une application ou fonctionnalité Windows, Windows enregistre certaines informations sur votre ordinateur relatives aux fichiers système utilisés et à la date et la fréquence d'utilisation de cette application ou fonctionnalité.

### **Utilisation des informations**

Windows utilise ces informations sur l'utilisation des applications et fonctionnalités pour accélérer leur lancement. Dans certains cas, les applications peuvent se lancer automatiquement dans un état interrompu.

### **Choix et contrôle**

Les applications automatiquement lancées et interrompues apparaissent dans le Gestionnaire des tâches et peuvent être arrêtées. Quand elles sont interrompues, ces applications ne peuvent pas accéder à votre webcam ou microphone tant que vous ne les avez pas lancées, même si vous avez auparavant activé cette fonctionnalité.

[Haut de la page](#)

Assistant Compatibilité des programmes

### **Quel est le rôle de cette fonctionnalité ?**

Si un problème d'incompatibilité est détecté sur une application de bureau que vous essayez d'exécuter, l'Assistant Compatibilité des programmes vous aide alors à le résoudre.

### **Informations collectées, traitées ou transmises**

Si un problème d'incompatibilité est trouvé sur une application que vous tentez d'exécuter, un rapport généré reprend alors des renseignements tels que le nom de l'application, sa version, les paramètres de compatibilité nécessaires et vos opérations ayant pu être réalisées avec l'application jusqu'au problème. Les problèmes relatifs aux applications incompatibles sont signalés à Microsoft par l'intermédiaire du Rapport d'erreurs Windows ou du Programme d'amélioration de l'expérience utilisateur Windows.



## **Utilisation des informations**

Les rapports d'erreur proposent des réponses aux problèmes avec vos applications dont vous faites part. Ces réponses contiennent des liens (le cas échéant) vers le site Web de l'éditeur de l'application de façon à pouvoir en savoir plus sur les solutions possibles. Les rapports d'erreur créés suite à des échecs d'application contribuent à déterminer le paramètre à ajuster lorsque vous rencontrez des problèmes de compatibilité pour l'application que vous exécutez sur cette version de Windows. Les renseignements émis à travers le Programme d'amélioration du produit servent à identifier les problèmes de compatibilité d'applications.

Microsoft n'utilise aucune des informations recueillies pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

## **Choix et contrôle**

Dans le cas de problèmes rapportés par le biais du Rapport d'erreurs Windows, un rapport d'erreurs est créé uniquement si vous sélectionnez l'option permettant de vérifier en ligne l'existence d'une solution. À moins que vous n'acceptiez au préalable de faire automatiquement état des problèmes pour vérifier la présence de solutions connues, il vous est demandé si vous voulez envoyer le rapport d'erreurs. Pour plus d'informations, voir la section « Rapport d'erreurs Windows ».

Certains problèmes sont automatiquement signalés via le Programme d'amélioration de l'expérience utilisateur Windows si vous choisissez de l'activer. Pour plus d'informations, voir la section Programme d'amélioration de l'expérience utilisateur Windows.

[Haut de la page](#)

Propriétés

### **Quel est le rôle de cette fonctionnalité ?**

Les propriétés sont des informations sur les fichiers qui vous permettent d'organiser vos fichiers et de les trouver rapidement. Certaines propriétés sont intrinsèques au fichier, comme la taille du fichier. D'autres peuvent être spécifiques à une application ou un

appareil, comme les paramètres de votre appareil photo au moment où vous avez pris un cliché ou les données d'emplacement de l'image enregistrées par l'appareil photo.

### **Informations collectées, traitées ou transmises**

Le type des informations stockées dépend du type de fichier et des applications qui les utilisent. Le nom de fichier, la date de modification, la taille de fichier, l'auteur, les mots clés et les commentaires sont autant d'exemples de propriétés. Elles sont stockées dans le fichier et suivent ce dernier s'il est déplacé ou copié à un autre emplacement (partage de fichiers ou envoi sous forme de pièce jointe à un message électronique, par exemple).

### **Utilisation des informations**

Les propriétés peuvent vous aider à organiser vos fichiers et à les trouver plus rapidement. Des applications peuvent également les utiliser pour effectuer des tâches spécifiques. Aucune information n'est envoyée à Microsoft.

### **Choix et contrôle**

Vous pouvez modifier ou supprimer certaines propriétés d'un fichier en sélectionnant ce dernier dans l'Explorateur de fichiers et en cliquant sur **Propriétés**. Certaines propriétés intrinsèques, telles que la date de modification, la taille et le nom du fichier, ainsi que certaines propriétés spécifiques à des applications, ne peuvent être supprimées de cette façon. Vous avez la possibilité de modifier ou de supprimer les propriétés spécifiques aux applications uniquement si l'application utilisée pour générer le fichier prend en charge ces fonctionnalités.

[Haut de la page](#)

Proximité

## **Service de proximité en champ proche**

### **Quel est le rôle de cette fonctionnalité ?**

Si votre ordinateur est équipé d'un matériel de communication en champ proche (ou NFC, Near-Field Communication), vous pouvez le mettre en contact physique avec un autre appareil ou accessoire doté d'un matériel NFC pour partager des liens, des fichiers et d'autres

informations. Il existe deux types de connexions de proximité : Approcher pour activer et Approcher pour conserver la connexion. Avec Approcher pour activer, vous pouvez créer une connexion temporaire ou durable entre des appareils par Wi-Fi, Wi-Fi Direct ou Bluetooth. Avec Approcher pour conserver la connexion, la connexion reste active aussi longtemps que les appareils se trouvent proches l'un de l'autre.

### **Informations collectées, traitées ou transmises**

Lorsque vous mettez en contact des appareils dont la fonctionnalité de proximité est activée, ils échangent des informations pour établir une connexion entre eux. Selon la configuration des appareils, ces données peuvent inclure des informations de couplage Bluetooth, des adresses réseau Wi-Fi, ainsi que le nom de votre ordinateur.

Une fois la connexion établie, d'autres informations peuvent être échangées entre les appareils, selon les spécificités de la fonctionnalité de proximité ou de l'application que vous utilisez. Windows peut envoyer fichiers, liens et autres informations entre des appareils utilisant une connexion de proximité. Les applications qui utilisent la proximité peuvent envoyer et recevoir n'importe quelles informations auxquelles elles ont accès. Ces informations peuvent transiter par votre connexion réseau ou Internet ou directement par le biais d'une connexion sans fil d'appareil à appareil.

### **Utilisation des informations**

Les informations du réseau et du PC échangées dans le cadre d'une connexion de proximité servent à établir une connexion réseau et à identifier les appareils qui se connectent entre eux. Les données transférées dans le cadre d'une connexion de proximité initiée dans une application peuvent être utilisées par cette même application de quelque manière que ce soit. Aucune information n'est envoyée à Microsoft.

### **Choix et contrôle**

Le service de proximité en champ proche est activé par défaut. Un administrateur peut désactiver cette fonctionnalité par le biais des options proposées dans Périphériques et imprimantes, accessible à partir du Panneau de configuration.

## Approcher pour envoyer

### **Quel est le rôle de cette fonctionnalité ?**

La fonctionnalité Approcher pour envoyer de Windows facilite le partage d'informations sélectionnées avec un ami qui se trouve près de vous ou avec un de vos autres appareils, tel qu'un téléphone mobile. Par exemple, lorsque vous êtes dans un navigateur, vous pouvez démarrer la fonctionnalité Approcher pour envoyer dans le volet Périphériques. Le prochain appareil sur lequel vous appuyez reçoit un lien vers la page Web actuellement affichée. Cela vaut également pour les applications qui prennent en charge le partage d'informations (images, texte ou fichiers, par exemple).

### **Informations collectées, traitées ou transmises**

La fonctionnalité Approcher pour envoyer utilise les informations que vous partagez, ainsi que les informations décrites dans la section Service de proximité en champ proche, ci-dessus.

### **Utilisation des informations**

Ces informations servent uniquement à créer la connexion entre les deux appareils. Les informations partagées ne sont pas stockées par la fonctionnalité Approcher pour envoyer. Aucune information n'est envoyée à Microsoft.

### **Choix et contrôle**

Si le service de proximité en champ proche est activé, la fonctionnalité Approcher pour envoyer est également activée. Pour plus d'informations, voir la section « Service de proximité en champ proche ».

[Haut de la page](#)

Connexions d'accès distant

### **Quel est le rôle de cette fonctionnalité ?**

Les connexions d'accès distant vous permettent de vous connecter aux réseaux privés au moyen d'une connexion de réseau privé virtuel (ou VPN, Virtual Private Network) et du service d'accès à distance (ou RAS, Remote Access Service). Le service RAS est un composant qui permet

de connecter un PC client (généralement, votre PC) à un PC hôte (également appelé serveur d'accès distant) en utilisant des protocoles standard. Les technologies VPN permettent aux utilisateurs de se connecter à un réseau privé, tel qu'un réseau d'entreprise, via Internet.

Partie intégrante des connexions d'accès distant, le composant Accès réseau à distance vous permet d'accéder à Internet à l'aide d'un modem d'accès à distance ou d'une technologie haut débit, telle qu'un modem câble ou une ligne DSL (Digital Subscriber Line). L'accès réseau à distance intègre des composants de numérotation, tels qu'un client RAS, le Gestionnaire des connexions et un téléphone RAS, ainsi que des numéroteurs en ligne de commande, comme rasdial.

### **Informations collectées, traitées ou transmises**

Les composants de numérotation recueillent des informations auprès de votre PC, telles que le nom d'utilisateur, le mot de passe et le nom de domaine. Ces informations sont envoyées au système auquel vous essayez de vous connecter. Pour préserver la confidentialité de vos données et la sécurité de votre PC, les informations liées à la sécurité (nom d'utilisateur et mot de passe) sont chiffrées et stockées sur votre PC.

### **Utilisation des informations**

Les informations du numéroteur sont utilisées pour permettre à votre PC de se connecter à Internet. Un serveur d'accès distant peut conserver le nom d'utilisateur et les informations d'adresse IP à des fins de comptabilité et de conformité, mais aucune information n'est envoyée à Microsoft.

### **Choix et contrôle**

Pour les numéroteurs non basés sur la ligne de commande, vous pouvez choisir d'enregistrer votre mot de passe en sélectionnant **Enregistrer ce nom d'utilisateur et ce mot de passe**. Vous pouvez à tout moment désactiver cette option pour supprimer le mot de passe enregistré dans le numéroteur. Cette option étant désactivée par défaut, vous pouvez être invité à fournir votre mot de passe pour vous connecter à Internet ou à un réseau. Les numéroteurs en ligne de commande, tels que rasdial, ne vous permettent pas d'enregistrer

votre mot de passe.

[Haut de la page](#)

Connexions aux programmes RemoteApp et aux services Bureau à distance

### **Quel est le rôle de cette fonctionnalité ?**

La fonctionnalité Connexions RemoteApp et Bureau à distance vous permet d'accéder aux applications et aux Bureaux d'ordinateurs distants qui ont été placés en ligne pour permettre d'y accéder à distance.

### **Informations collectées, traitées ou transmises**

Lorsque vous activez une connexion, les fichiers de configuration sont téléchargés sur votre PC à partir de l'URL distante que vous spécifiez. Ces fichiers de configuration lient les applications et les Bureaux des PC distants pour vous permettre de les exécuter à partir de votre PC. Votre PC vérifie de manière automatique et périodique s'il existe des mises à jour pour ces fichiers de configuration et les télécharge, le cas échéant. Ces applications s'exécutent sur des PC distants, et les informations que vous entrez dans les applications sont transmises via le réseau aux PC distants auxquels vous choisissez de vous connecter.

Si Microsoft héberge l'ordinateur ou l'application auquel vous vous connectez, il se peut que des informations supplémentaires relatives à votre connexion soient envoyées à Microsoft à des fins de support technique.

### **Utilisation des informations**

Les mises à jour des fichiers de configuration peuvent inclure des modifications de paramètres qui peuvent, par exemple, vous donner accès à de nouvelles applications ; toutefois, les nouvelles applications s'exécutent uniquement si vous le décidez. De même, cette fonctionnalité envoie des informations aux ordinateurs distants sur lesquels les applications distantes s'exécutent. L'utilisation de ces données par les applications distantes est soumise à la politique des fournisseurs d'applications et des administrateurs des ordinateurs distants en matière de confidentialité. Aucune information n'est envoyée à Microsoft sauf si la connexion à distance est hébergée par

Microsoft.

## **Choix et contrôle**

Vous êtes libre d'utiliser ou non la fonctionnalité Connexions aux programmes RemoteApp et aux services Bureau à distance. Vous pouvez ajouter ou supprimer des Connexions aux programmes RemoteApp et aux services Bureau à distance en accédant à Connexions aux programmes RemoteApp et aux services Bureau à distance dans le Panneau de configuration. Vous pouvez ajouter une nouvelle connexion en cliquant sur **Accéder aux programmes RemoteApp et aux services Bureau à distance**, puis en entrant une URL de connexion dans la boîte de dialogue. Vous pouvez également utiliser votre adresse de messagerie pour récupérer l'URL de connexion. Vous pouvez supprimer une connexion et les fichiers de connexion associés en cliquant sur **Supprimer** dans la boîte de dialogue de description de la connexion. Si vous déconnectez une connexion sans fermer toutes les applications ouvertes, ces applications restent ouvertes sur le PC distant. La fonctionnalité Connexions aux programmes RemoteApp et aux services Bureau à distance ne figure pas dans la liste Ajouter ou supprimer des programmes du Panneau de configuration.

[Haut de la page](#)

Connexion Bureau à distance

### **Quel est le rôle de cette fonctionnalité ?**

La fonctionnalité Connexion Bureau à distance vous permet d'établir une connexion distante avec un ordinateur hôte exécutant les services Bureau à distance.

### **Informations collectées, traitées ou transmises**

Les paramètres de la fonctionnalité Connexion Bureau à distance sont stockés dans un espace de stockage local de l'application ou dans un fichier de protocole RDP (Remote Desktop Protocol) sur votre ordinateur. Parmi ces paramètres figurent le nom de votre domaine et les paramètres de configuration de la connexion, tels que le nom de l'ordinateur distant, le nom d'utilisateur, les informations sur l'affichage, le périphérique local et le dispositif audio, le Presse-

papiers, les paramètres de connexion, les noms des applications distantes, ainsi que l'icône ou la miniature de la session.

Les informations d'identification de ces connexions, celles de la passerelle des services Bureau à distance et la liste des noms de serveurs de passerelle Bureau à distance approuvés sont stockées en local sur votre ordinateur. La liste est stockée dans le Registre. Cette liste est stockée de façon permanente, sauf si l'administrateur décide de la supprimer. Aucune information n'est envoyée à Microsoft sauf si la connexion à distance est hébergée par Microsoft.

### **Utilisation des informations**

Les informations collectées par la fonctionnalité Connexion Bureau à distance vous permettent de vous connecter à des ordinateurs hôtes exécutant les services Bureau à distance en utilisant les paramètres de votre choix. Le nom d'utilisateur, le mot de passe et les informations de domaine sont collectés pour vous permettre d'enregistrer vos paramètres de connexion et de lancer une connexion en double-cliquant sur un fichier de protocole RDP ou en cliquant sur un favori, sans qu'il soit nécessaire d'entrer à nouveau ces informations.

### **Choix et contrôle**

Vous êtes libre d'utiliser ou non la fonctionnalité Connexion Bureau à distance. Si vous l'utilisez, vos fichiers de protocole RDP et les favoris de la connexion Bureau à distance contiennent les informations nécessaires pour se connecter à un PC distant, y compris les options et les paramètres qui ont été configurés lors de l'enregistrement automatique de la connexion. Vous pouvez personnaliser les fichiers de protocole RDP et les favoris, y compris les fichiers permettant de se connecter à un même PC avec des paramètres différents. Pour modifier les informations d'identification enregistrées, ouvrez le Gestionnaire d'informations d'identification dans Comptes d'utilisateurs, accessible à partir du Panneau de configuration.

[Haut de la page](#)

Se connecter à un compte Microsoft

### **Quel est le rôle de cette fonctionnalité ?**

Un compte Microsoft (anciennement connu sous le nom d'identifiant



Windows Live ID) se compose d'une adresse de messagerie et son mot de passe uniques que vous pouvez utiliser pour vous connecter à des applications, à des sites et à des services de Microsoft et de certains partenaires Microsoft. Vous pouvez vous inscrire à un compte Microsoft dans Windows ou sur des sites Web Microsoft qui nécessitent que vous vous connectiez avec un compte Microsoft.

Vous pouvez vous connecter à Windows avec un compte Microsoft ou, sur les produits qui le permettent, choisir de connecter votre compte local ou de domaine à un compte Microsoft. Dans ce dernier cas, Windows peut adapter l'environnement de l'ordinateur que vous utilisez en synchronisant automatiquement les paramètres et informations dans Windows et dans les applications Microsoft. Si vous visitez un site Web auquel vous vous connectez à l'aide d'un compte Microsoft, Windows vous connecte également automatiquement à ce site Web.

### **Informations collectées, traitées ou transmises**

Lorsque vous entrez une adresse de messagerie comme compte Microsoft lors de la configuration de votre ordinateur ou dans la section **Comptes** de Paramètres du PC, Windows envoie l'adresse de messagerie à Microsoft pour déterminer si un compte Microsoft lui est associé. Si vous utilisez déjà cette adresse de messagerie comme compte Microsoft, vous pouvez l'utiliser avec le mot de passe du compte Microsoft pour vous connecter à Windows. Si les informations de sécurité sont insuffisantes pour votre compte Microsoft, d'autres informations de sécurité peuvent vous être demandées, telles qu'un numéro de téléphone portable, pour vérifier que le compte est bien le vôtre. Si vous ne possédez pas de compte Microsoft, vous pouvez en créer un en utilisant l'adresse de messagerie de votre choix.

Lorsque vous vous connectez avec un compte Microsoft, Windows envoie également les informations standard sur l'ordinateur à Microsoft, notamment le fabricant, le nom de modèle et la version du périphérique.

Chaque fois que vous vous connectez à Windows à l'aide d'un compte Microsoft et que votre ordinateur est connecté à Internet, Windows vérifie votre adresse de messagerie et votre mot de passe auprès des serveurs de Microsoft. Lorsque vous vous connectez à Windows

à l'aide d'un compte Microsoft ou d'un compte de domaine connecté à votre compte Microsoft :

- Certains paramètres de Windows se synchronisent entre les ordinateurs que vous utilisez pour vous connecter à votre compte Microsoft. Pour plus d'informations sur les paramètres qui se synchronisent et comment les contrôler, voir la section « Synchroniser les paramètres » dans cette page.
- Les applications Microsoft qui utilisent un compte Microsoft pour l'authentification (comme Courrier, Calendrier, Contacts, Microsoft Office et d'autres applications) peuvent automatiquement lancer le téléchargement de vos informations. Par exemple, l'application Courrier télécharge automatiquement les messages de la boîte de réception de votre adresse Outlook.com ou Hotmail.com si vous en possédez une). Les navigateurs Web peuvent automatiquement vous connecter à des sites Web sur lesquels vous ouvrez des sessions à l'aide de votre compte Microsoft (par exemple, si vous visitez le site Bing.com, vous pouvez vous y connecter automatiquement sans avoir à entrer le mot de passe de votre compte Microsoft).

Windows vous demande l'autorisation avant de permettre à des applications tierces d'utiliser les informations de profil ou personnelles d'autre nature associées à votre compte Microsoft. Si vous vous connectez à Windows par le biais d'un compte de domaine lié à un compte Microsoft, les paramètres et informations choisis sont alors synchronisés avec votre compte de domaine, et vous êtes automatiquement connecté à des applications et des sites Web tel que décrit ci-dessus. Étant donné que les administrateurs de domaine peuvent accéder à toutes les informations sur votre ordinateur, ils peuvent également accéder à l'ensemble des paramètres et informations que vous avez choisi de synchroniser avec d'autres ordinateurs via votre compte Microsoft. Cela peut inclure des paramètres tels que le nom, l'avatar du compte et l'historique du navigateur. Pour plus d'informations sur les paramètres qui se synchronisent et comment les contrôler, voir la section « Synchroniser les paramètres » dans cette page.

### **Utilisation des informations**

Lorsque vous créez un compte Microsoft dans Windows, les informations que vous fournissez servent à créer le compte et contribuent à le sécuriser. Par exemple, les informations de sécurité que vous fournissez (telles que votre numéro de téléphone ou votre adresse de messagerie de secours) ne sont utilisées que si vous ne pouvez pas vous connecter à votre compte. Lorsque vous vous connectez à Windows à l'aide d'un compte Microsoft, Windows utilise les informations de votre compte Microsoft pour vous connecter automatiquement à des applications et sites Web. Pour en savoir plus sur l'impact d'un compte Microsoft sur la confidentialité, lisez la [Déclaration de confidentialité du compte Microsoft](#). Pour obtenir des informations sur la façon dont chaque application Microsoft utilise les informations associées à votre compte Microsoft, voir la déclaration de confidentialité de chaque application. La déclaration de confidentialité d'une application Microsoft est disponible en ouvrant Paramètres à partir de l'application, ou dans la boîte de dialogue À propos de.

Les informations standard sur l'ordinateur peuvent être utilisées pour personnaliser certaines communications qui vous sont envoyées, telles que des messages électroniques de prise en main de votre périphérique.

### **Choix et contrôle**

Si vous vous connectez à Windows par le biais d'un compte Microsoft, certains paramètres se synchronisent automatiquement. Pour savoir comment changer les paramètres de Windows à synchroniser ou comment arrêter la synchronisation, voir la section « Synchroniser les paramètres » dans cette page. Pour en savoir plus sur les données collectées par les applications Microsoft qui utilisent un compte Microsoft pour l'authentification, lisez leur déclaration de confidentialité respective.

Sur les produits qui le permettent, vous pouvez créer un compte local ou un compte Microsoft à tout moment dans **Comptes** dans Paramètres du PC. Si vous ouvrez une session Windows à l'aide d'un compte de domaine, vous pouvez connecter ou déconnecter votre compte Microsoft à loisir dans la section **Comptes** disponible dans Paramètres du PC.

Lorsque vous utilisez la navigation InPrivate dans Internet Explorer,

vous n'êtes pas connecté automatiquement aux sites Web qui utilisent des comptes Microsoft.

[Haut de la page](#)

Stockage nuage OneDrive

### **Quel est le rôle de cette fonctionnalité ?**

Lorsque vous vous connectez avec un compte Microsoft sur votre appareil, vous pouvez choisir d'enregistrer automatiquement certains paramètres et informations sur les serveurs Microsoft afin de disposer d'une sauvegarde si votre appareil est confronté à un problème.

### **Informations collectées, traitées ou transmises**

Pendant la configuration, si vous choisissez d'utiliser OneDrive pour le stockage nuage, Windows transmet automatiquement le contenu aux serveurs de Microsoft, notamment les éléments suivants :

- les photos et les vidéos enregistrées dans le dossier **Pellicule** sur votre appareil ;
- les paramètres spécifiques à votre appareil et qui ne sont pas partagés sur vos autres appareils ;
- des informations descriptives sur l'appareil, telles que le nom et le type de l'appareil.

Vous pouvez également choisir d'enregistrer du contenu sur les serveurs Microsoft, et les applications peuvent choisir de sélectionner les serveurs Microsoft comme emplacement par défaut pour l'enregistrement de vos fichiers.

### **Utilisation des informations**

Windows utilise ce contenu pour assurer le service de stockage nuage. Microsoft n'utilise pas votre contenu ou vos informations personnelles pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

### **Choix et contrôle**

Si vous choisissez « Utiliser OneDrive » lors de la configuration de votre ordinateur, Windows enregistre le contenu décrit dans cette

section sur OneDrive. Vous pouvez modifier à tout moment ces paramètres dans la section OneDrive de Paramètres du PC.

[Haut de la page](#)

Synchroniser les paramètres

### **Quel est le rôle de cette fonctionnalité ?**

Lorsque vous vous connectez à Windows à l'aide d'un compte Microsoft, Windows synchronise certains de vos paramètres et certaines de vos informations avec les serveurs Microsoft pour faciliter la personnalisation des expériences sur plusieurs ordinateurs. Une fois que vous vous êtes connecté sur un ou plusieurs ordinateurs avec un compte Microsoft, lorsque vous vous connectez à un autre ordinateur avec le même compte Microsoft pour la première fois, Windows télécharge et applique les paramètres et informations que vous avez choisi de synchroniser à partir des autres ordinateurs. Les paramètres que vous avez choisi de synchroniser sont automatiquement mis à jour sur les serveurs Microsoft et vos autres ordinateurs lorsque vous les utilisez.

### **Informations collectées, traitées ou transmises**

Si vous choisissez d'ouvrir une session Windows avec un compte Microsoft, Windows synchronise certains paramètres avec les serveurs Microsoft. Ces paramètres sont les suivants :

- la disposition de votre écran d'accueil ;
- les applications que vous avez installées à partir du Windows Store ;
- Préférences linguistiques
- les préférences concernant les options d'ergonomie ;
- les paramètres de personnalisation, tels que l'avatar de votre compte, l'image de l'écran de verrouillage, l'arrière-plan et les paramètres de souris ;
- les paramètres des applications du Windows Store ;

les dictionnaires des vérificateurs orthographiques, les dictionnaires IME et les dictionnaires personnels ;

- l'historique et les favoris du navigateur Web, ainsi que les sites Web que vous avez ouverts ;
- les mots de passe réseau, d'applications et de sites Web enregistrés ;
- les adresses d'imprimantes réseau partagées auxquelles vous êtes connecté.

Pour préserver la confidentialité de vos informations personnelles, tous les paramètres synchronisés sont chiffrés via SSL. Certains de ces paramètres ne se synchronisent pas sur votre ordinateur tant que vous n'avez pas ajouté ce dernier à votre compte Microsoft en tant qu'ordinateur approuvé.

Si vous vous connectez à Windows à l'aide d'un compte de domaine connecté à un compte Microsoft, les paramètres et informations choisis sont synchronisés dans le compte de domaine. Les mots de passe que vous enregistrez lorsque vous êtes connecté à Windows à l'aide d'un compte de domaine connecté à un compte Microsoft ne sont jamais synchronisés. Étant donné que les administrateurs de domaine peuvent accéder à toutes les informations sur votre ordinateur, ils peuvent également accéder à l'ensemble des paramètres et informations que vous avez choisi de synchroniser avec d'autres ordinateurs via votre compte Microsoft.

### **Utilisation des informations**

Windows utilise ces paramètres et informations pour assurer les fonctions du service de synchronisation. Microsoft n'utilise pas vos paramètres et informations synchronisés pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

### **Choix et contrôle**

Lorsque vous vous connectez à Windows par le biais d'un compte Microsoft, vos paramètres se synchronisent par défaut. Vous pouvez choisir de synchroniser vos paramètres et de contrôler quels paramètres sont synchronisés en accédant à **Synchroniser les paramètres** dans la section OneDrive des paramètres de l'ordinateur.

Si vous vous connectez à Windows à l'aide d'un compte de domaine et que vous décidez de le connecter à un compte Microsoft, Windows vous demande quels paramètres synchroniser avant d'établir la connexion avec votre compte Microsoft.

[Haut de la page](#)

Technologie Teredo

### **Quel est le rôle de cette fonctionnalité ?**

La technologie Teredo (Teredo) permet aux PC et réseaux de communiquer par le biais de plusieurs protocoles réseau.

### **Informations collectées, traitées ou transmises**

À chaque démarrage de votre PC, Teredo essaie de trouver un service IPv6 (Internet Protocol version 6) public sur Internet. Cette opération se produit automatiquement lorsque votre PC est connecté à un réseau public ou privé (mais pas à des réseaux gérés, tels que des domaines d'entreprise). Si vous utilisez une application qui impose à Teredo d'utiliser la connectivité IPv6, ou si vous configurez votre pare-feu de façon à toujours autoriser la connectivité IPv6, Teredo contacte régulièrement le service Microsoft Teredo sur Internet. Les seules informations envoyées à Microsoft sont des informations standard sur le PC, ainsi que le nom du service demandé (par exemple, `teredo.ipv6.microsoft.com`).

### **Utilisation des informations**

Les informations envoyées par votre PC via Teredo servent à déterminer si votre PC est connecté à Internet et s'il peut trouver un service IPv6 public. Une fois le service localisé, des informations sont envoyées pour maintenir la connexion avec le service IPv6.

### **Choix et contrôle**

À l'aide de l'outil en ligne de commande netsh, vous pouvez modifier la requête envoyée par le service sur Internet afin d'utiliser des serveurs non-Microsoft ou de désactiver cette fonctionnalité. Pour obtenir des instructions détaillées, voir la section « Internet Protocol Version 6, Teredo et technologies connexes » de [ce livre blanc technique](#).

[Haut de la page](#)

Services du module de plateforme sécurisée (TPM)

### **Quel est le rôle de cette fonctionnalité ?**

Le module de plateforme sécurisée (TPM) est un équipement de sécurité intégré à certains ordinateurs. Si vous en disposez d'un et qu'il est en service, il permet à votre ordinateur de tirer pleinement parti des fonctionnalités de sécurité avancées. Les fonctionnalités Windows qui utilisent le module TPM sont les suivantes : Chiffrement de l'appareil, Carte à puce virtuelle, Démarrage sécurisé, Windows Defender et Stockage de certificats TPM.

### **Informations collectées, traitées ou transmises**

Par défaut, Windows s'approprié le module TPM et stocke les informations d'autorisation complète du propriétaire du module TPM afin que seuls les administrateurs Windows puissent y accéder. Des valeurs d'autorisation limitée sont créées pour effectuer les actions d'administration classiques et les actions utilisateur standard. Ces valeurs sont gérées par Windows.

La console de gestion du module TPM vous permet de mettre en service le module TPM de façon interactive et d'enregistrer la valeur d'autorisation du propriétaire du module TPM sur un support externe, tel qu'un disque mémoire flash USB, après la mise en service du module TPM. Un fichier enregistré contient les informations d'autorisation du propriétaire du module TPM. Le fichier contient également le nom du PC, la version du système d'exploitation, le nom de l'auteur et la date de création pour vous aider à reconnaître le fichier.

Dans un environnement de domaine, le mot de passe du propriétaire exclusif du module TPM peut être configuré par l'administrateur du domaine pour être stocké dans Active Directory sous un objet TPM lorsque le module TPM est mis en service.

Chaque module TPM dispose d'une paire de clés de chiffrement unique de type EK (Endorsement Key) dont il se sert pour prouver son authenticité. La paire de clés de type EK peut être créée et stockée dans le module TPM par le fabricant de votre PC. Pour les PC plus anciens, Windows peut être amené à occasionner la création de la



paire de clés de type EK à l'intérieur du module TPM. La partie privée de la paire de clés de type EK n'est jamais exposée à l'extérieur du module TPM, et une fois créée, elle ne peut généralement pas être réinitialisée. Un certificat de paire de clés de type EK est stocké dans le module TPM de la plupart des ordinateurs Windows. Ce certificat indique que la paire de clés de type EK existe dans un module TPM matériel. Le certificat s'avère utile aux vérificateurs distants pour s'assurer que le module TPM est conforme aux spécifications TPM. Le certificat d'une paire de clés de type EK est généralement signé par le fabricant du module TPM ou par le fabricant de la plateforme.

### **Utilisation des informations**

Une fois le module TPM initialisé, les applications peuvent l'utiliser pour créer et sécuriser d'autres clés de chiffrement uniques. Par exemple, la fonctionnalité Chiffrement de l'appareil utilise le module TPM pour protéger la clé qui chiffre le lecteur.

Si vous décidez d'enregistrer le mot de passe du propriétaire du module TPM dans un fichier, les informations supplémentaires enregistrées dans ce fichier à propos du PC et de l'utilisateur vous permettront d'identifier le PC et le module TPM correspondants. Windows se sert de la paire de clés de type EK du module TPM pendant l'initialisation du module TPM pour chiffrer votre valeur d'autorisation du propriétaire du module TPM avant de l'envoyer au module TPM. Windows ne transmet pas les clés de chiffrement hors de votre PC. Windows n'offre pas d'interface permettant à des applications tierces, telles que des logiciels anti-programme malveillant, d'utiliser la paire de clés de type EK dans certains scénarios de module TPM, comme le démarrage mesuré avec attestation. Dans le cas des logiciels anti-programme malveillant, la paire de clés de type EK (Endorsement Key) et le certificat qui l'accompagne permettent également de s'assurer que les mesures de démarrage sont fournies par le module TPM d'un fabricant spécifique. Par défaut, seuls les administrateurs ou les applications bénéficiant de droits d'administration peuvent utiliser la paire de clés de type EK (Endorsement Key) du module TPM.

### **Choix et contrôle**

Les utilisateurs ou les administrateurs peuvent opter pour l'utilisation

du module TPM en activant une fonctionnalité Windows ou en exécutant une application qui fait appel au module TPM.

Vous pouvez choisir d'effacer le module TPM et de rétablir ses valeurs par défaut. Dans ce cas, les informations sur le propriétaire sont supprimées, tout comme l'ensemble des clés TPM (à l'exception de la paire de clés de type EK) ou des informations de chiffrement que les applications ont pu créer pendant que le module TPM était utilisé.

[Haut de la page](#)

Certificats racine de mise à jour

### **Quel est le rôle de cette fonctionnalité ?**

Les certificats servent principalement à vérifier l'identité d'une personne ou d'un appareil, à authentifier un service ou à chiffrer des fichiers. Les autorités de certification racines de confiance sont des organismes qui émettent des certificats. La fonctionnalité Certificats racines de mise à jour contacte le service en ligne Windows Update pour déterminer si Microsoft a ajouté une autorité de certification à sa liste d'autorités de confiance. Cette opération n'intervient cependant que lorsqu'une application reçoit un certificat émis par une autorité de certification qui n'est pas directement approuvée (le certificat n'est pas stocké dans la liste des certificats autorisés de votre PC). Si l'autorité de certification a été ajoutée à la liste Microsoft des autorités de confiance, son certificat est automatiquement ajouté à la liste des certificats autorisés sur votre PC.

### **Informations collectées, traitées ou transmises**

La fonctionnalité Certificats racines de mise à jour s'adresse au service en ligne Windows Update pour lui demander la liste actuelle des autorités de certification racines du programme de certificat racine Microsoft. Si le certificat non autorisé figure dans la liste, la fonctionnalité Certificats racines de mise à jour obtient ce certificat auprès de Windows Update et le place dans le magasin de certificats autorisés de votre PC. Parmi les informations transférées figurent les noms et les hachages de chiffrement des certificats racines.

### **Utilisation des informations**

Les informations sont utilisées par Microsoft pour mettre à jour la liste

des certificats autorisés sur votre PC. Microsoft n'utilise pas ces informations pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

## **Choix et contrôle**

La fonctionnalité Certificats racines de mise à jour est activée par défaut. Les administrateurs peuvent configurer la stratégie de groupe afin de désactiver la fonctionnalité Certificats racines de mise à jour sur un ordinateur.

[Haut de la page](#)

Update Services

## **Quel est le rôle de cette fonctionnalité ?**

La fonctionnalité Update Services pour Windows englobe Windows Update et Microsoft Update :

- **Windows Update** est un service qui met à votre disposition les mises à jour des logiciels Windows et d'autres logiciels de prise en charge, tels que les pilotes fournis par les fabricants de périphériques.
- **Microsoft Update** est un service qui met à votre disposition les mises à jour des logiciels Windows et d'autres logiciels Microsoft, tels que Microsoft Office.

## **Informations collectées, traitées ou transmises**

La fonctionnalité Update Services collecte des informations sur votre ordinateur qui permettent à Microsoft de faire fonctionner des services et de les améliorer, par exemple :

- Les logiciels Microsoft et autres logiciels associés (pilotes et microprogrammes fournis par les fabricants de périphériques, par exemple) installés sur votre ordinateur pour lesquels la fonctionnalité Update Services dispose de mises à jour. Cela nous permet de déterminer quelles mises à jour sont appropriées.
- Les paramètres de configuration de Windows Update et/ou de Microsoft Update, stipulant par exemple si vous souhaitez, ou

non, que les mises à jour soient automatiquement téléchargées ou installées.

- Les réussites, échecs et erreurs que vous rencontrez lors de l'accès aux services de mise à jour et de leur utilisation.
- Le numéro d'ID Plug-and-Play des périphériques matériels : code affecté par le fabricant de périphériques qui identifie chaque périphérique (par exemple, un type spécifique de clavier).
- L'identificateur global unique (GUID) : nombre généré de façon aléatoire qui ne contient aucune information personnelle. Les GUID sont utilisés pour différencier des PC sans identifier l'utilisateur.
- Les nom, numéro de révision, fournisseur et date de révision du BIOS : informations sur l'ensemble des routines logicielles de base qui testent votre matériel, démarrent le système d'exploitation sur votre ordinateur et transfèrent les données entre les périphériques connectés à votre ordinateur.
- Les fabricant, modèle, rôle de plateforme et numéro de référence (SKU) : informations sur le PC utilisées pour activer les études de diagnostic dans les installations de pilotes.

Pour utiliser Update Services, accédez à Windows Update dans le Panneau de configuration et recherchez des mises à jour, ou changez vos paramètres pour autoriser Windows à installer automatiquement les mises à jour lorsqu'elles sont disponibles (recommandé). Dans la fonctionnalité Windows Update, vous pouvez choisir d'activer ou non Microsoft Update.

Si vous choisissez d'effectuer les mises à jour logicielles importantes sur votre ordinateur, il se peut que l'outil de suppression de logiciels malveillants Microsoft Windows (MSRT) soit inclus avec ces mises à jour. Cet outil analyse les PC à la recherche d'infections causées par certains logiciels malveillants répandus et aide à les supprimer. Si le logiciel s'exécute, il supprime les [programmes malveillants répertoriés](#) sur le site Web de Support technique Microsoft. Durant une recherche de programme malveillant, un rapport est envoyé à Microsoft avec des informations spécifiques sur les programmes malveillants détectés, les

erreurs et d'autres informations sur votre ordinateur. Pour plus d'informations, lisez la [Déclaration de confidentialité de l'outil de suppression de logiciels malveillants Windows](#) .

## **Utilisation des informations**

Les données envoyées à Microsoft sont utilisées dans le cadre du fonctionnement et de la maintenance de la fonctionnalité Update Services. Elles permettent également de générer des statistiques globales que nous utilisons pour analyser les tendances et améliorer nos produits et services, dont la fonctionnalité Update Services.

Pour générer les statistiques globales, Update Services utilise le GUID collecté pour suivre et enregistrer le nombre d'ordinateurs qui utilisent ces services et pour savoir si le téléchargement et l'installation de mises à jour spécifiques ont réussi ou échoué. Update Services enregistre le GUID de l'ordinateur qui a tenté le téléchargement et l'installation, l'ID de l'élément demandé, si des mises à jour étaient disponibles, ainsi que les informations standard sur l'ordinateur.

Les informations MSRT décrites ci-dessus nous servent à améliorer nos logiciels anti-programme malveillant, ainsi que d'autres produits et services de sécurité. Les informations contenues dans les rapports MSRT ne sont pas utilisées pour vous identifier ou vous contacter.

## **Mises à jour requises**

Si vous activez Update Services, certains composants logiciels de votre système qui font partie de cette fonctionnalité ou qui y sont directement liés devront être mis à jour de temps en temps pour son bon fonctionnement. Ces mises à jour doivent être effectuées avant que le service puisse rechercher, télécharger ou installer d'autres mises à jour. Ces mises à jour requises corrigent des erreurs, fournissent des améliorations et maintiennent la compatibilité avec les serveurs Microsoft qui prennent en charge le service.

Si la fonctionnalité Update Services est désactivée, vous ne recevez pas ces mises à jour.

Les mises à jour logicielles requises pour installer ou mettre à jour les applications du Windows Store seront téléchargées et installées automatiquement. Ces mises à jour sont indispensables au bon fonctionnement des applications.

## **Cookies et jetons**

Un jeton est semblable à un cookie. Il stocke des informations dans un petit fichier placé sur votre disque dur par le serveur Update Services, et est utilisé lorsque votre ordinateur se connecte à ce serveur pour conserver une connexion valide. Il est stocké uniquement sur l'ordinateur, pas sur le serveur. Ce cookie ou jeton contient des informations (notamment l'heure de la dernière analyse) qui lui permettent de trouver les mises à jour disponibles les plus récentes. Il contient des informations qui permettent de gérer le contenu à télécharger sur votre ordinateur, à quel moment le téléchargement doit avoir lieu, ainsi que le GUID pour identifier votre ordinateur sur le serveur.

Les informations incluses dans le contenu du cookie ou du jeton sont chiffrées par le serveur (à l'exception de l'heure d'expiration du cookie ou jeton). Ce cookie ou jeton est différent d'un cookie de navigateur et ne peut pas être contrôlé par les paramètres du navigateur. Le cookie ou jeton ne peut pas être supprimé. Cependant, si vous n'utilisez pas Update Services, il n'est pas utilisé.

## **Choix et contrôle**

Si vous optez pour la configuration rapide de Windows, le service Windows Update est activé et est paramétré de sorte à installer automatiquement les mises à jour.

Si vous activez la fonctionnalité Update Services, quels que soient les paramètres choisis, les mises à jour requises de certains composants du service sont téléchargées et installées automatiquement sans vous en informer. Si vous préférez ne pas recevoir les mises à jour requises, désactivez Update Services.

Vous pouvez également choisir de rechercher ou d'installer automatiquement les mises à jour importantes et recommandées pour votre ordinateur, ou uniquement les mises à jour importantes. Les mises à jour facultatives ne sont jamais installées automatiquement. Après avoir configuré Windows, vous pouvez modifier les paramètres de Windows Update dans le Panneau de configuration ou dans les paramètres du PC.

Si vous avez indiqué vouloir rechercher et installer les mises à jour

importantes, et recevoir l'outil MSRT dans le cadre de ces mises à jour pour votre ordinateur, vous pouvez [désactiver la fonctionnalité de création de rapports du logiciel](#).

[Haut de la page](#)

Réseau privé virtuel

### **Quel est le rôle de cette fonctionnalité ?**

Un réseau privé virtuel (VPN) vous permet de vous connecter à un réseau privé, tel qu'un réseau d'entreprise, via Internet. Une connexion VPN peut être fournie par le client VPN Windows, ou par une application VPN tierce.

### **Informations collectées, traitées ou transmises**

Lorsque vous vous connectez à un réseau privé virtuel (VPN), les informations d'identification que vous entrez dans le client VPN sont envoyées au réseau distant. Vous pouvez stocker ces informations d'identification sur votre ordinateur. Une fois que vous êtes connecté, en fonction de la façon dont le VPN est configuré, une partie ou toute l'activité réseau est acheminée via le réseau distant. Les administrateurs peuvent configurer des applications spécifiques pour qu'elles acheminent toujours leur trafic via le VPN ou pour qu'elles se connectent automatiquement au VPN au démarrage. Aucune information n'est envoyée à Microsoft.

Des logiciels de VPN tiers peuvent collecter des informations supplémentaires ; la collecte et l'utilisation de ces informations sont soumises aux pratiques du tiers en matière de confidentialité.

### **Utilisation des informations**

Les clients VPN utilisent les informations d'identification que vous fournissez pour authentifier le réseau distant, ainsi que pour acheminer le trafic réseau vers et à partir du réseau distant. Si un client VPN tiers collecte des informations supplémentaires, l'utilisation de ces informations par ce tiers est soumise à ses pratiques en matière de confidentialité.

### **Choix et contrôle**

Vous pouvez ajouter ou supprimer une connexion VPN, et consulter

l'état de connexions existantes, dans la section **Réseau** de Paramètres du PC. Une fois qu'une connexion VPN a été configurée, vous pouvez la connecter ou la déconnecter en sélectionnant le réseau dans la liste figurant dans Paramètres.

[Haut de la page](#)

Programme d'amélioration de l'expérience utilisateur Windows

### **Quel est le rôle de cette fonctionnalité ?**

Le Programme d'amélioration de l'expérience utilisateur Windows collecte des informations relatives à l'utilisation que vous faites de vos applications, de vos ordinateurs, de vos périphériques connectés et de Windows. Il peut également collecter des informations relatives à d'éventuels problèmes de performances et de fiabilité. Si vous choisissez de participer au Programme d'amélioration de l'expérience utilisateur Windows, Windows envoie ces données à Microsoft, et télécharge de régulièrement un fichier pour collecter d'autres informations pertinentes sur votre utilisation de Windows et de vos applications. Les rapports du Programme d'amélioration de l'expérience utilisateur sont envoyés à Microsoft, et servent à améliorer les fonctionnalités les plus utilisées et à trouver des solutions aux problèmes les plus courants.

### **Informations collectées, traitées ou transmises**

Les rapports du CEIP peuvent contenir des informations concernant :

- des données de configuration, notamment le nombre de processeurs dont est équipé votre ordinateur, le nombre de connexions réseau utilisées, les résolutions d'écran des périphériques d'affichage et la version de Windows installée sur votre ordinateur ;
- des informations sur les performances et la fiabilité, notamment les temps de réponse d'une application lorsque vous cliquez sur un bouton, le nombre de problèmes rencontrés avec une application ou un périphérique et le délai nécessaire à l'envoi ou à la réception d'informations sur une connexion réseau ;
- des informations relatives à l'utilisation des applications :



notamment la fréquence d'utilisation des applications et de la fonctionnalité Aide et support Windows, les services que vous utilisez pour vous connecter dans des applications et le nombre de dossiers que vous créez généralement sur votre Bureau.

Les rapports du Programme d'amélioration de l'expérience utilisateur contiennent également des informations sur les événements (données du journal des événements) de votre ordinateur, remontant jusqu'à 7 jours avant le début de votre participation à ce programme. Étant donné que la plupart des utilisateurs décident de participer au Programme d'amélioration de l'expérience utilisateur peu de temps après l'installation de Windows, Microsoft utilise ces informations pour analyser et améliorer l'installation de Windows.

Ces informations sont envoyées à Microsoft lorsque vous êtes connecté à Internet. Les rapports du Programme d'amélioration de l'expérience utilisateur ne contiennent pas intentionnellement d'informations personnelles, telles que vos nom, adresse ou numéro de téléphone. Toutefois, certains rapports peuvent involontairement contenir des identificateurs uniques, tels que le numéro de série d'un périphérique connecté à votre ordinateur. Microsoft filtre les informations contenues dans les rapports du Programme d'amélioration de l'expérience utilisateur pour tenter de supprimer les identificateurs individuels susceptibles d'y figurer. Si des éléments d'identification personnel sont reçus, Microsoft ne les utilise pas dans le but de vous identifier ou de vous contacter.

Le Programme d'amélioration de l'expérience utilisateur génère de façon aléatoire un numéro appelé GUID (Globally Unique Identifier, identificateur global unique), qui est envoyé à Microsoft avec chaque rapport du programme. Le GUID permet de déterminer les données qui sont envoyées au fil du temps à partir d'un ordinateur particulier. Certains rapports du Programme d'amélioration de l'expérience utilisateur sont également susceptibles de contenir des GUID issus de votre compte Microsoft.

Le Programme d'amélioration de l'expérience utilisateur peut également télécharger régulièrement un fichier permettant de collecter davantage d'informations pertinentes sur votre utilisation de Windows et de vos applications. Ce fichier permet à Windows de collecter des informations supplémentaires afin que Microsoft trouve des solutions

aux problèmes les plus courants et comprend mieux les habitudes d'utilisation de Windows et des applications.

## **Utilisation des informations**

Microsoft exploite les informations du Programme d'amélioration de l'expérience utilisateur pour améliorer ses produits et services, ainsi que les logiciels et matériels tiers conçus pour une utilisation avec ces produits et services. Nous pouvons en outre partager les informations globales du Programme d'amélioration de l'expérience utilisateur avec les partenaires Microsoft pour leur donner la possibilité d'améliorer leurs produits et services, mais ces informations ne peuvent pas être exploitées dans le but de vous identifier, vous contacter ou vous envoyer des publicités ciblées.

Le GUID permet de déterminer l'ampleur des problèmes, grâce aux commentaires reçus, et d'établir des priorités. Par exemple, le GUID permet à Microsoft d'établir s'il s'agit d'un client qui a été confronté à un problème une centaine de fois ou de centaines de clients confrontés une seule fois au même problème. Microsoft n'utilise pas les informations collectées par le Programme d'amélioration de l'expérience utilisateur dans le but de vous identifier ou de vous contacter.

## **Choix et contrôle**

Si vous optez pour la configuration rapide de Windows, vous activez le Programme d'amélioration de l'expérience utilisateur Windows : Windows et les applications Microsoft issues du Windows Store peuvent envoyer des rapports du Programme d'amélioration de l'expérience utilisateur pour tous les utilisateurs de l'ordinateur. Si vous choisissez de personnaliser les paramètres, vous pouvez contrôler le Programme d'amélioration de l'expérience utilisateur en sélectionnant **Envoyer à Microsoft des informations sur la façon dont j'utilise mon PC, dans le cadre du programme d'amélioration de l'expérience utilisateur (un fichier se téléchargera régulièrement pour collecter de meilleures informations)** sous **Participer à l'amélioration des produits et services Microsoft**. Après avoir configuré Windows, les administrateurs peuvent modifier ce paramètre dans la section **Centre de maintenance** du Panneau de configuration.

Pour plus d'informations, voir le [Forum Aux Questions du Programme d'amélioration de l'expérience utilisateur](#).

[Haut de la page](#)

Windows Defender

Windows Defender recherche sur votre PC la présence de programmes malveillants et autres logiciels potentiellement indésirables. Il inclut les fonctionnalités Microsoft Active Protection Service et Historique.

## Microsoft Active Protection Service

Si vous utilisez Windows Defender, Microsoft Active Protection Service (MAPS) peut contribuer à la protection de votre ordinateur en téléchargeant automatiquement de nouvelles signatures pour les programmes malveillants récemment détectés et en surveillant l'état de sécurité de votre ordinateur. Le service MAPS envoie à Microsoft des informations sur les programmes malveillants et autres formes de logiciels potentiellement indésirables ; il peut également envoyer des fichiers qui pourraient contenir des programmes malveillants. Si MAPS détecte que votre ordinateur est infecté par certains types de programmes malveillants, il vous contacte automatiquement via votre compte Microsoft pour vous aider à résoudre le problème.

### **Informations collectées, traitées ou transmises**

Les rapports MAPS contiennent des informations sur les fichiers de programmes malveillants potentiels, telles que les noms des fichiers, le hachage de chiffrement, l'éditeur du logiciel, la taille et les horodatages. En outre, MAPS peut collecter des URL complètes pour indiquer l'origine des fichiers, ainsi que les adresses IP auxquelles les fichiers potentiellement malveillants se connectent. Ces URL peuvent parfois contenir des informations personnelles, telles que des termes recherchés ou des données entrées dans des formulaires. Les rapports peuvent aussi mentionner les actions que vous avez appliquées lorsque Windows Defender vous aura notifié la détection d'un logiciel potentiellement indésirable. Le service MAPS reprend ces informations pour permettre à Microsoft d'évaluer l'efficacité de la détection et de la suppression des programmes malveillants et des logiciels potentiellement indésirables par Windows Defender, et pour tenter d'identifier tout nouveau programme malveillant.

Ces rapports sont automatiquement envoyés à Microsoft lorsque :

- Windows Defender détecte des logiciels dont les risques n'ont pas encore été évalués ;
- Windows Defender détecte des modifications apportées à votre ordinateur par un logiciel dont les risques n'ont pas encore été évalués ;
- Windows Defender entreprend des actions sur tout programme malveillant détecté (dans le cadre de son action corrective automatique) ;
- Windows Defender effectue une analyse planifiée complète et des opérations automatiques sur les logiciels qu'il détecte, en fonction de vos paramètres.
- Windows Defender analyse un contrôle ActiveX dans Internet Explorer.

Si vous décidez de participer au service MAPS lors de l'installation de Windows, vous pouvez souscrire un abonnement de base. Les rapports des membres pour l'abonnement de base contiennent les informations décrites dans cette section. Les rapports des membres de l'abonnement avancé sont plus complets et peuvent parfois contenir des informations personnelles, telles que des chemins d'accès de fichiers et des vidages de mémoire partiels. Ces rapports et les rapports des autres utilisateurs de Windows Defender participant à MAPS aident nos chercheurs à découvrir plus rapidement les nouvelles menaces. Des définitions de programmes malveillants sont ensuite créées, et ces définitions mises à jour sont mises à disposition de tous les utilisateurs à travers Windows Update.

Si vous rejoignez MAPS, il se peut que Windows Defender envoie, à partir de votre ordinateur, des fichiers ou du contenu Web spécifiques que Microsoft soupçonne d'être des logiciels potentiellement indésirables. Cet exemple de rapport est ensuite utilisé pour une analyse détaillée. Si un fichier est susceptible de contenir des informations personnelles, le système vous demande confirmation avant de l'envoyer. Si Windows Update n'a pas pu obtenir les signatures mises à jour pour Windows Defender pendant un certain

laps de temps, Windows Defender essaie d'utiliser le service MAPS pour télécharger les signatures à partir d'un autre emplacement de téléchargement.

Pour préserver la confidentialité de vos informations personnelles, toutes les informations transmises au service MAPS sont chiffrées via SSL.

Pour détecter et résoudre certains types d'infections de programmes malveillants, Windows Defender envoie régulièrement au service MAPS des informations sur l'état de sécurité de votre ordinateur. Ces données comprennent des informations sur les paramètres de sécurité de votre ordinateur et des fichiers journaux décrivant les pilotes et autres logiciels qui se chargent au démarrage de votre ordinateur. Un nombre qui identifie de façon unique votre ordinateur est également envoyé.

### **Utilisation des informations**

Les rapports envoyés au service MAPS permettent d'améliorer les logiciels et services de Microsoft. Ces rapports peuvent également être utilisés à des fins statistiques ou pour des tests et des études, ainsi que pour générer des définitions. MAPS ne collecte pas intentionnellement des informations personnelles. Si le service MAPS devait involontairement collecter ce type d'informations, Microsoft ne les utilise pas pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

Les informations relatives à l'état de sécurité de votre ordinateur que le service MAPS collecte sont utilisées pour déterminer si certains types de programmes malveillants ont infecté votre ordinateur. Si tel est le cas, Microsoft utilise les informations de contact mentionnées dans votre compte Microsoft pour vous contacter et vous transmettre des détails sur le problème et la façon de le résoudre.

### **Choix et contrôle**

Si vous optez pour la configuration rapide de Windows, le service MAPS est alors activé. Si vous choisissez de personnaliser les paramètres, vous pouvez contrôler le service MAPS en sélectionnant **Renforcer la protection contre les logiciels malveillants en envoyant des informations et des fichiers à Microsoft Active**

**Protection Service quand Windows Defender est activé** sous **Partager des informations avec Microsoft**. Après avoir configuré Windows, vous pouvez modifier votre abonnement ou vos paramètres MAPS, y compris désactiver MAPS, à partir du menu **Paramètres** de Windows Defender.

Si vous recevez l'outil de suppression des programmes malveillants via Windows Update, il est possible qu'il envoie des informations similaires au service MAPS même si Windows Defender est désactivé. Pour plus d'informations, lisez la [Déclaration de confidentialité de l'outil de suppression des logiciels malveillants Windows](#) .

## Fonctionnalité Historique

### **Quel est le rôle de cette fonctionnalité ?**

La fonctionnalité Historique fournit la liste de toutes les applications que Windows Defender a détectées sur votre ordinateur et indique les mesures qu'il a prises à ces occasions.

De plus, vous pouvez consulter la liste des applications que Windows Defender ne surveille pas lorsqu'elles sont exécutées sur votre ordinateur (Éléments autorisés). Vous pouvez également examiner les applications dont Windows Defender empêche l'exécution jusqu'à ce vous décidiez de les supprimer ou d'autoriser leur exécution (Éléments en quarantaine).

### **Informations collectées, traitées ou transmises**

La liste des logiciels détectés par Windows Defender, les mesures que vous et les autres utilisateurs avez prises et les actions effectuées automatiquement par Windows Defender sont stockées sur votre PC. Tous les utilisateurs peuvent consulter l'historique de Windows Defender pour identifier les programmes malveillants et les autres logiciels potentiellement indésirables qui ont essayé de s'installer ou de s'exécuter sur le PC, ou dont l'exécution a été autorisée par un autre utilisateur. Si, par exemple, vous apprenez l'existence d'une nouvelle menace causée par un programme malveillant, vous pouvez consulter l'Historique pour savoir si Windows Defender l'a empêché d'infecter votre ordinateur. Aucune information n'est envoyée à Microsoft.

### **Choix et contrôle**

Les listes d'historique peuvent être supprimées par un administrateur.

Service de rapport d'erreurs Windows

### **Quel est le rôle de cette fonctionnalité ?**

Le Rapport d'erreurs Windows aide Microsoft et les partenaires Microsoft à diagnostiquer certains problèmes concernant les logiciels que vous utilisez, ainsi qu'à proposer des solutions. À chaque problème ne correspondant pas toujours une solution, mais lorsqu'elles existent, ces solutions sont fournies sous la forme de procédures de résolution ou de mises à jour à installer. Pour éviter les problèmes et accroître la fiabilité du logiciel, certaines solutions sont également incluses dans des Service Packs et dans les futures versions du logiciel.

### **Informations collectées, traitées ou transmises**

De nombreux logiciels sont conçus pour fonctionner avec le Rapport d'erreurs Windows. Si un problème survient dans l'un de ces produits, il est probable que vous soyez invité à le signaler.

Le Rapport d'erreurs Windows collecte des informations qui s'avèrent utiles pour diagnostiquer et résoudre un problème. Des fichiers aidant à décrire le problème et les informations de base sur le matériel et le logiciel permettent d'identifier l'endroit où est survenu le problème dans le logiciel ou le matériel, le type ou la gravité du problème et les problèmes éventuels de compatibilité et de performances du logiciel. Si vous hébergez des ordinateurs virtuels à l'aide de Windows, les rapports d'erreurs envoyés à Microsoft peuvent contenir des informations concernant ces ordinateurs virtuels.

Le Rapport d'erreurs Windows collecte également des informations sur les applications, pilotes et périphériques pour aider Microsoft à comprendre et améliorer la compatibilité des applications et des périphériques. Les informations relatives à une application peuvent inclure le nom des fichiers exécutables de l'application. Les informations sur les périphériques et les pilotes peuvent inclure les noms des périphériques que vous avez installés sur votre PC, ainsi que les fichiers exécutables associés à ces pilotes de périphériques. Les informations relatives à la société qui a publié une application ou un pilote sont susceptibles d'être collectées.

Si vous décidez d'activer la génération de rapports automatique lors de la configuration de Windows, le service de rapport envoie automatiquement des informations de base sur l'emplacement des problèmes. Dans certains cas, le service de rapport transmet automatiquement des informations supplémentaires pour mieux diagnostiquer le problème (par exemple, une capture instantanée partielle de la mémoire de l'ordinateur). Certains rapports d'erreurs peuvent recueillir involontairement des informations personnelles. Par exemple, un rapport qui contient une capture instantanée de la mémoire de l'ordinateur peut inclure votre nom, une partie du document sur lequel vous étiez en train de travailler ou encore des données que vous avez récemment envoyées à un site Web.

Pour faciliter le diagnostic de certains types de problèmes, la fonctionnalité Rapport d'erreurs Windows peut créer un rapport contenant des informations supplémentaires, notamment des fichiers journaux. Avant de transmettre un rapport contenant ces données supplémentaires, Windows vous demande de confirmer que vous souhaitez l'envoyer, même si vous avez activé la génération de rapports automatique.

Après l'envoi du rapport, le service de rapport peut éventuellement vous demander de plus amples informations sur le problème que vous avez rencontré. Si vous choisissez de communiquer votre numéro de téléphone ou votre adresse de messagerie avec ces informations, votre rapport d'erreurs est identifiable personnellement. Microsoft peut alors vous contacter pour vous demander des informations supplémentaires afin de résoudre le problème signalé.

Le Rapport d'erreurs Windows génère de façon aléatoire un numéro appelé GUID (Globally Unique Identifier, identificateur global unique), qui est envoyé à Microsoft avec chaque rapport d'erreurs. Le GUID permet de déterminer les données qui sont envoyées au fil du temps à partir d'un ordinateur particulier. Il ne contient aucune information personnelle.

Pour préserver la confidentialité de vos informations personnelles, les informations transmises sont chiffrées via SSL.

## **Utilisation des informations**

Microsoft exploite les informations relatives aux erreurs et aux



problèmes signalés par les utilisateurs de Windows pour améliorer les produits et services de Microsoft, ainsi que les logiciels et matériels tiers conçus pour une utilisation avec ces produits et services. Nous utilisons le GUID pour déterminer l'étendue des commentaires que nous recevons et les classer par ordre de priorité. Par exemple, le GUID permet à Microsoft d'établir s'il s'agit d'un client qui a été confronté à un problème une centaine de fois ou de centaines de clients confrontés une seule fois au même problème.

Les employés, fournisseurs, distributeurs et partenaires de Microsoft peuvent être autorisés à accéder aux informations collectées, mais ils ne peuvent utiliser ces informations que dans le cadre d'une réparation ou d'une amélioration des produits et services de Microsoft, ou des logiciels et matériels tiers conçus pour une utilisation avec des produits et services Microsoft. Si un rapport d'erreurs contient des informations confidentielles, Microsoft ne les exploite pas pour vous identifier, vous contacter ou vous envoyer des publicités ciblées. Toutefois, si vous acceptez de fournir vos coordonnées tel que décrit ci-dessus, nous pouvons utiliser ces informations pour vous contacter.

### **Choix et contrôle**

Si vous optez pour la configuration rapide de Windows pendant son installation, le Rapport d'erreurs Windows transmet alors des rapports de base pour vérifier si des solutions aux problèmes sont proposées en ligne. Si vous choisissez de personnaliser les paramètres, vous pouvez contrôler le Rapport d'erreurs Windows en sélectionnant **Utiliser le rapport d'erreurs Windows pour rechercher en ligne des solutions** sous **Rechercher en ligne des solutions**. Après avoir configuré Windows, vous pouvez modifier ce paramètre dans la section Centre de maintenance du Panneau de configuration.

Pour plus d'informations, voir la [Microsoft Déclaration de confidentialité du service de rapport d'erreurs](#).

[Haut de la page](#)

Association de fichier Windows

### **Quel est le rôle de cette fonctionnalité ?**

L'association de fichier Windows aide les utilisateurs à associer des

types de fichiers à des applications spécifiques. Si vous essayez d'ouvrir un type de fichier qui n'est associé à aucune application, Windows vous invite à utiliser la fonctionnalité Association de fichier Windows pour chercher une application appropriée, ce qui suppose notamment de rechercher une application compatible dans Windows Store. Les applications généralement associées à l'extension du nom de fichier sont affichées à l'écran.

### **Informations collectées, traitées ou transmises**

Si vous décidez d'utiliser l'association de fichier Windows, l'extension du nom de fichier (par exemple, docx ou pdf) et la langue d'affichage de votre PC sont transmises à Microsoft. L'autre partie du nom de fichier n'est pas communiquée à Microsoft. Lorsqu'une association de fichier est établie avec une application déterminée, un identificateur unique de l'application est envoyé pour identifier l'application par défaut. Cela se produit pour chaque type de fichier.

### **Utilisation des informations**

Lorsque vous envoyez une extension de nom de fichier, le service renvoie la liste des applications connues par Microsoft comme étant en mesure d'ouvrir les fichiers de cette extension. Aucune association de type de fichier ne change, sauf si vous choisissez de télécharger et d'installer une application.

### **Choix et contrôle**

Lorsque vous essayez d'ouvrir un type de fichier qui n'est associé à aucune application, vous pouvez choisir d'utiliser la fonctionnalité Association de fichier Windows. Aucune information sur le fichier n'est transmise à Microsoft, sauf si vous décidez d'utiliser le service.

[Haut de la page](#)

Aide de Windows

## **Aide et support en ligne Windows**

### **Quel est le rôle de cette fonctionnalité ?**

La fonctionnalité Aide et support Windows en ligne (si elle est activée) vous permet d'accéder aux rubriques d'aide et au contenu à jour du support lorsque vous êtes connecté à Internet.

## **Informations collectées, traitées ou transmises**

Lorsque vous utilisez la fonctionnalité Aide et support Windows en ligne, vos requêtes de recherche d'aide sont envoyées à Microsoft, tout comme vos demandes de contenu d'aide formulées en cliquant sur un lien. Windows envoie des informations sur la configuration de votre ordinateur pour permettre de trouver du contenu d'aide plus pertinent. L'aide et le support en ligne de Windows utilisent également des technologies Web standard telles que les cookies.

## **Utilisation des informations**

Microsoft utilise les informations pour retourner des rubriques d'aide en réponse à vos requêtes de recherche, fournir des résultats pertinents, développer de nouveaux contenus et améliorer ceux existants. Nous utilisons les informations sur la configuration de votre ordinateur pour afficher le contenu d'aide approprié pour cette configuration. Nous utilisons les cookies et d'autres technologies Web pour faciliter la navigation dans le contenu de l'aide et nous permettre de mieux comprendre le comportement des utilisateurs dans l'aide en ligne de Windows.

## **Choix et contrôle**

L'aide et le support en ligne sont désactivés par défaut. Pour modifier ce paramètre, appuyez ou cliquez sur l'icône **Paramètres** dans la partie supérieure de la fenêtre Aide et support, puis activez ou désactivez l'option **Obtenir de l'aide en ligne**. Pour effacer les cookies utilisés par l'aide de Windows, ouvrez Options Internet dans le Panneau de configuration, appuyez ou cliquez sur le bouton **Supprimer** sous **Historique de navigation**, sélectionnez **Cookies et données de sites Web**, puis appuyez ou cliquez sur **Supprimer**. Si vous choisissez de bloquer tous les cookies (dans la section Confidentialité de l'onglet Options Internet), l'aide de Windows ne définit aucun cookie.

## **Programme d'amélioration de l'aide**

### **Quel est le rôle de cette fonctionnalité ?**

Le Programme d'amélioration de l'aide permet à Microsoft d'identifier les tendances d'utilisation par les clients de la fonctionnalité Aide et support en ligne de Windows et d'améliorer les résultats de recherche,

ainsi que la pertinence du contenu proposé.

### **Informations collectées, traitées ou transmises**

Le Programme d'amélioration de l'aide transmet à Microsoft des informations sur la version de Windows exécutée sur votre ordinateur et sur la façon dont vous utilisez la fonctionnalité Aide et support Windows. Ainsi, les requêtes de recherche que vous formulez dans Aide et support Windows et les évaluations ou les commentaires que vous faites au sujet des rubriques d'aide qui vous sont présentées comptent parmi les informations transmises. Dès lors que vous effectuez une recherche, que vous parcourez l'aide ou que vous faites des évaluations ou des commentaires sur les rubriques d'aide qui vous sont présentées, ces informations sont transmises à Microsoft.

Le Programme d'amélioration de l'aide génère de façon aléatoire un numéro appelé GUID (Globally Unique IDentifier, identificateur global unique) qui est communiqué à Microsoft avec chaque rapport du programme. Ce GUID nous permet de déterminer quelles données sont envoyées à partir d'un ordinateur précis au fil du temps. Il ne contient aucune information personnelle. Il est différent des autres GUID utilisés par le Rapport d'erreurs Windows et le Programme d'amélioration de l'expérience utilisateur Windows.

### **Utilisation des informations**

Les données recueillies servent à identifier les tendances et les habitudes d'utilisation et permettre à Microsoft d'améliorer la qualité du contenu proposé et la pertinence des résultats de recherche. Nous faisons appel au GUID pour déterminer le degré d'importance des problèmes qui nous sont communiqués afin d'établir leur priorité. Par exemple, le GUID permet à Microsoft d'établir s'il s'agit d'un client qui a été confronté à un problème une centaine de fois ou de centaines de clients confrontés une seule fois au même problème.

Le programme d'amélioration de l'aide ne collecte pas intentionnellement d'informations qui pourraient permettre de vous identifier personnellement. Si vous tapez des informations personnelles dans les champs de recherche ou de commentaires, celles-ci sont alors envoyées mais Microsoft ne les exploite pas pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

## Choix et contrôle

Si vous optez pour la configuration rapide de Windows, vous êtes inscrit au Programme d'amélioration de l'aide. Si vous choisissez de personnaliser les paramètres, vous pouvez contrôler les paramètres du programme d'amélioration de l'aide en sélectionnant **Envoyer à Microsoft des informations sur la façon dont j'utilise l'aide, dans le cadre du programme d'amélioration de l'aide** sous **Participer à l'amélioration des produits et services Microsoft**. Après avoir configuré Windows, vous pouvez modifier ce paramètre dans Aide et support Windows.

[Haut de la page](#)

Assistance à distance

### Quel est le rôle de cette fonctionnalité ?

Vous pouvez utiliser la fonctionnalité Assistance à distance pour inviter un individu à se connecter à votre ordinateur et vous aider à résoudre un problème, même si cette personne ne se trouve pas à proximité. Une fois connectée, cette personne peut consulter l'écran de votre PC. Avec votre autorisation, elle peut utiliser sa souris et son clavier pour contrôler votre PC et vous montrer comment résoudre un problème.

### Informations collectées, traitées ou transmises

L'Assistance à distance crée une connexion chiffrée entre les deux ordinateurs via Internet ou le réseau local. Lorsqu'une personne utilise l'Assistance à distance pour se connecter à votre ordinateur, elle peut voir votre Bureau, tous les documents ouverts, ainsi que les informations privées visibles à l'écran. De plus, si vous autorisez cette personne à contrôler votre PC avec sa souris et son clavier, elle pourra y effectuer des opérations, notamment supprimer des fichiers ou modifier des paramètres. Une fois la connexion établie, l'Assistance à distance échange certaines informations de contact, telles que le nom d'utilisateur, le nom de l'ordinateur et l'avatar du compte. Un fichier journal de la session conserve une trace de toutes les connexions établies via l'Assistance à distance.

### Utilisation des informations

Ces informations sont utilisées pour établir une connexion chiffrée et

permettre à l'autre personne d'accéder à votre Bureau. Aucune information n'est envoyée à Microsoft.

## **Choix et contrôle**

Avant d'autoriser une personne à se connecter à votre PC, fermez les applications ou les documents ouverts que vous ne souhaitez pas qu'elle voie. Si, à un quelconque moment de la connexion, vous préférez que cette personne arrête de voir votre écran ou d'agir sur votre ordinateur, appuyez sur la touche Échap pour mettre fin à la session. Vous pouvez désactiver la journalisation de la session et l'échange d'informations de contact en désactivant ces options dans les paramètres de l'Assistance à distance.

[Haut de la page](#)

Windows Search

## **Quel est le rôle de cette fonctionnalité ?**

Windows Search vous permet de rechercher votre périphérique et Internet depuis un endroit unique. Pour offrir de meilleurs résultats de recherche, Windows Search peut faire appel à Bing et à la plateforme de localisation Windows. Notez qu'il existe sur votre appareil d'autres fonctionnalités de recherche fournies par Microsoft, telles que la recherche dans le Windows Store, Internet Explorer et autres produits Microsoft.

## **Informations collectées, traitées ou transmises**

Si vous souhaitez effectuer des recherches sur le Web, Windows envoie le contenu de votre saisie dans Windows Search à Microsoft. Pour affiner les résultats de la recherche, Windows Search envoie également à Microsoft des informations sur la manière dont vous interagissez avec la fonctionnalité. Windows Search envoie également un identificateur pour produire des résultats de recherche personnalisés basés sur vos interactions avec Bing et d'autres produits et services Microsoft. Si vous vous connectez à Windows avec un compte Microsoft l'identificateur est associé à votre compte Microsoft. Vous pouvez choisir de ne pas produire de résultats personnalisés dans Windows Search, auquel cas cet identificateur ne sera pas transmis.

Si vous autorisez Windows Search à utiliser votre emplacement, l'emplacement physique de votre périphérique tel que fourni par la plateforme de localisation Windows sera envoyé à Microsoft dans le cadre de chaque demande de recherche. Nous pouvons également être amenés à tirer votre emplacement physique approximatif de votre adresse IP.

Lorsque vous utilisez Windows Search pour effectuer une recherche dans une application, vos termes de recherche sont fournis à l'application.

### **Utilisation des informations**

Si vous choisissez d'utiliser Windows Search pour effectuer des recherches sur le Web, nous utilisons le terme à rechercher que vous avez précisé, votre historique de recherche local et en ligne, les informations associées à votre compte Microsoft et l'emplacement de votre périphérique pour émettre des suggestions de recherche pertinentes, des résultats de recherche personnalisés et des expériences personnalisées dans d'autres produits et services Microsoft. Pour en savoir plus sur les modalités d'utilisation de vos données, lisez la [Déclaration de confidentialité de Bing](#).

Lorsque vous utilisez Windows Search pour effectuer une recherche dans une application tierce, l'utilisation des informations recueillies est soumise aux pratiques de ce tiers en matière de confidentialité. Si vous effectuez une recherche dans une application Microsoft, la politique de confidentialité de l'application est expliquée dans sa déclaration de confidentialité.

### **Choix et contrôle**

Si vous optez pour la configuration rapide de Windows au cours de son installation, vous autorisez Windows Search à obtenir des suggestions de recherche et des résultats sur le Web, et vous autorisez Microsoft à utiliser les données issues de Windows Search (notamment l'emplacement) pour personnaliser Windows Search et les autres expériences Microsoft. Si vous choisissez de personnaliser les paramètres, vous pouvez décider, ou non, de modifier ces paramètres pour Windows Search. Après avoir configuré Windows, vous pouvez modifier ces paramètres dans la section **Rechercher** disponible dans

## Paramètres du PC.

Vous pouvez effacer votre historique de recherche local et une partie de l'historique de recherche Bing utilisé pour personnaliser votre expérience de recherche Windows dans la section **Rechercher** dans la section **Rechercher des applications** dans les paramètres de l'ordinateur. Le fait d'effacer votre historique de recherche indique à Microsoft de ne pas utiliser l'historique de recherche précédemment collecté pour personnaliser les suggestions de recherche ou organiser les résultats de la recherche. Il ne permet pas d'effacer les publicités ou autres informations de personnalisation (notamment les informations dérivées de votre historique de recherche), ni de supprimer les informations utilisées globalement par Microsoft pour améliorer les résultats de recherche et d'autres expériences Microsoft. Ces informations sont conservées et rendues anonymes comme décrit dans la [Déclaration de confidentialité de Bing](#). Vous pouvez gérer la publicité Microsoft et d'autres informations de personnalisation en ligne.

[Haut de la page](#)

## Installation de Windows

Cette section décrit les fonctionnalités disponibles dans le cadre du processus d'installation de Windows.

### Mise à jour dynamique

#### **Quel est le rôle de cette fonctionnalité ?**

La fonction de mise à jour dynamique permet à Windows d'effectuer une recherche unique des mises à jour les plus récentes pour votre ordinateur via Windows Update pendant l'installation de Windows. Si des mises à jour sont détectées, la mise à jour dynamique les télécharge et les installe automatiquement afin que votre ordinateur soit à jour lorsque vous ouvrez une session ou que vous l'utilisez pour la première fois.

#### **Informations collectées, traitées ou transmises**

Pour installer des pilotes compatibles, la mise à jour dynamique envoie des informations sur la configuration matérielle de votre ordinateur à Microsoft. Parmi les mises à jour que la fonctionnalité est en mesure



de télécharger sur votre ordinateur figurent les suivantes :

- **Mises à jour d'installation.** Mises à jour importantes des fichiers d'installation de logiciel garantissant le bon déroulement de votre installation.
- **Mises à jour des pilotes fournis.** Mises à jour importantes de pilotes pour la version de Windows que vous installez.

De plus, si vous installez Windows à partir du Windows Store, la mise à jour dynamique télécharge et installe les mises à jour les plus récentes sur Windows, ainsi que certains pilotes matériels requis par votre ordinateur.

### **Utilisation des informations**

La mise à jour dynamique transmet des informations à Microsoft au sujet de la configuration matérielle de votre ordinateur pour aider à identifier les pilotes adaptés à votre système.

### **Choix et contrôle**

Si vous installez Windows à partir du Windows Store, le programme d'installation télécharge et installe automatiquement les mises à jour. Si vous installez Windows à partir d'un média physique, vous êtes invité à vous connecter à Internet pour installer les mises à jour.

## **Programme d'amélioration de l'installation**

### **Quel est le rôle de cette fonctionnalité ?**

Cette fonctionnalité envoie à Microsoft un rapport unique reprenant les informations de base relatives à votre ordinateur et aux caractéristiques de votre installation de Windows. Microsoft exploite ces informations pour contribuer à améliorer l'environnement d'installation et apporter des solutions aux problèmes d'installation courants.

### **Informations collectées, traitées ou transmises**

Ce rapport inclut en règle générale des informations sur le déroulement de votre installation, telles que la date d'installation, la durée d'exécution de chaque phase d'installation, si l'installation consiste en une mise à niveau ou en une nouvelle installation du produit, les détails de sa version, la langue du système d'exploitation,

le type de support employé, la configuration de l'ordinateur, la réussite ou l'échec des opérations, ainsi que tous les codes d'erreur.

Si vous choisissez de participer au Programme d'amélioration de l'installation, le rapport est alors envoyé à Microsoft une fois que vous êtes connecté à Internet. Le Programme d'amélioration de l'installation génère de façon aléatoire un numéro appelé GUID (Globally Unique Identifier, identificateur global unique) transmis à Microsoft avec le rapport. Le GUID permet de déterminer les données qui sont envoyées au fil du temps à partir d'un ordinateur particulier. Le GUID ne contient aucune information personnelle et n'est pas utilisé dans le but de vous identifier.

### **Utilisation des informations**

Microsoft et ses partenaires utilisent le rapport pour contribuer à améliorer ses produits et services. Le GUID nous sert à mettre en corrélation ces données et celles recueillies par le Programme d'amélioration de l'expérience utilisateur Windows auquel vous pouvez participer dans le cadre de votre utilisation de Windows.

### **Choix et contrôle**

Vous avez le choix de participer à ce programme au moment où vous installez Windows en sélectionnant **Je veux aider à améliorer l'installation de Windows**.

Pour plus d'informations, voir la section « Programme d'amélioration de l'expérience utilisateur de Windows ».

## **Vérificateur de compatibilité Windows**

### **Quel est le rôle de cette fonctionnalité ?**

Lorsque vous installez Windows, le programme d'installation vous permet de déterminer si votre ordinateur actuel peut prendre en charge une mise à niveau vers Windows 8.1, et fournit des informations sur la compatibilité de vos programmes et périphériques.

### **Informations collectées, traitées ou transmises**

Lorsque nous évaluons la compatibilité de votre système, nous collectons certaines informations relatives à sa configuration avant la mise à jour, telles que les capacités du matériel, les périphériques connectés et les programmes installés. Parfois, les informations

concernant l'éditeur de logiciels peuvent contenir des données telles que le nom ou l'adresse de messagerie de l'éditeur.

## **Utilisation des informations**

Nous utilisons les informations collectées pour déterminer les pilotes appropriés pour votre ordinateur, ainsi que la compatibilité de votre ordinateur, de vos programmes et de vos périphériques avec Windows 8.1. Nous pouvons aussi nous en servir pour améliorer la qualité de nos produits et services. Nous n'utilisons pas ces informations pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

## **Choix et contrôle**

Si vous installez Windows à partir du Windows Store ou à partir d'un média physique à l'intérieur d'une installation de Windows existante, les informations décrites dans cette section sont envoyées à Microsoft. Si vous démarrez à partir d'un média d'installation physique pour installer Windows, le programme d'installation ne vérifie pas en ligne s'il existe des informations sur la compatibilité.

[Haut de la page](#)

Partage Windows

## **Quel est le rôle de cette fonctionnalité ?**

La fonctionnalité de partage Windows vous permet de partager du contenu entre les applications du Windows Store qui prennent en charge le partage. Elle vous permet également de partager du contenu avec vos amis.

## **Informations collectées, traitées ou transmises**

Lors du partage, l'application source transmet du contenu à l'application cible seulement à partir du moment où vous sélectionnez la cible dans le volet de partage. Si l'application source n'a pas implémenté le partage, vous avez la possibilité de partager une image de l'écran. Les applications cibles et les personnes avec lesquelles vous êtes habitué à partager du contenu sont affichées dans une liste du volet de partage pour vous permettre d'y accéder plus facilement. Aucune information n'est envoyée à Microsoft.

## Utilisation des informations

Les informations stockées à propos de votre fréquence de partage avec les applications cibles et les personnes avec lesquelles vous partagez régulièrement du contenu sont utilisées pour trier la liste du volet de partage par ordre de fréquence. Si vous partagez des informations avec une application tierce, l'utilisation des informations recueillies est soumise à la politique de confidentialité de l'éditeur tiers. Si vous partagez avec une application Microsoft, les pratiques de confidentialité inhérentes à l'application sont expliquées dans sa déclaration de confidentialité.

## Choix et contrôle

Par défaut, Windows stocke les informations sur votre utilisation du partage Windows. Vous pouvez désactiver le stockage de ces informations ou supprimer toutes les cibles stockées dans la section **Partage** sous **Rechercher des applications** disponible dans Paramètres du PC.

[Haut de la page](#)

Windows SmartScreen

## Quel est le rôle de cette fonctionnalité ?

Windows SmartScreen vérifie les fichiers et le contenu Web téléchargés dans des applications pour vous protéger contre les programmes malveillants et le contenu Web potentiellement dangereux, et préserver ainsi l'intégrité de votre ordinateur. Avant d'ouvrir un fichier téléchargé inconnu ou potentiellement dangereux, Windows affiche un avertissement. Si SmartScreen détecte du contenu Web potentiellement dangereux dans une application, Windows affiche un avertissement à la place du contenu.

## Informations collectées, traitées ou transmises

Si vous choisissez d'utiliser Windows SmartScreen pour vérifier des fichiers téléchargés, Windows envoie des informations au service en ligne SmartScreen. Celles-ci peuvent inclure un nom de fichier, un identificateur de fichier (appelé « hachage ») et des informations de certificat numérique assorties d'informations standard sur votre

ordinateur et du numéro de version du filtre Windows SmartScreen. Pour préserver la confidentialité de vos informations personnelles, les informations transmises à Microsoft sont chiffrées via SSL.

Si vous choisissez d'utiliser Windows SmartScreen pour bloquer du contenu potentiellement dangereux dans des applications, Windows envoie au service en ligne SmartScreen des informations, notamment les adresses et les types du contenu auquel certaines applications du Windows Store accèdent lorsque vous les utilisez. En réponse, le service en ligne indique à votre ordinateur si le contenu a été signalé à Microsoft comme étant non sécurisé ou suspect. Les rapports envoyés à Microsoft comprennent des informations telles que le nom ou l'identificateur de l'application et les adresses complètes du contenu Web auquel accède l'application.

Pour préserver la confidentialité de vos informations personnelles, les informations transmises à Microsoft sont chiffrées. Les informations associées à une page Web faisant l'objet d'un accès à l'intérieur d'une application, comme les termes de recherche, peuvent être incluses dans l'adresse envoyée à Microsoft. Par exemple, si vous recherchez un mot dans une application de dictionnaire, le mot que vous recherchez peut être envoyé à Microsoft en tant que partie de l'adresse complète à laquelle accède l'application. Dans la mesure du possible, Microsoft filtre ces adresses pour tenter de supprimer toute information personnelle.

Windows génère un identificateur global unique (GUID) qui est envoyé à Microsoft avec chaque rapport. Le GUID permet de déterminer les données qui sont envoyées au fil du temps à partir d'un ordinateur particulier. Il ne contient aucune information personnelle.

### **Utilisation des informations**

Microsoft utilise les informations décrites ci-dessus pour vous avertir du caractère potentiellement dangereux de fichiers et de contenu téléchargés dans des applications. Par exemple, si SmartScreen détecte une menace potentielle dans une application qui prend en charge SmartScreen, Windows affiche un avertissement à la place du contenu. Nous utilisons également ces informations pour améliorer SmartScreen, ainsi que d'autres produits et services. Microsoft n'utilise pas ces informations pour vous envoyer des publicités ciblées.

## Choix et contrôle

Si vous optez pour la configuration rapide pendant l'installation de Windows, vous activez de fait Windows SmartScreen. Si vous choisissez de personnaliser les paramètres, vous pouvez contrôler Windows SmartScreen en sélectionnant **Utiliser les services en ligne SmartScreen pour protéger le PC contre les contenus malveillants des sites chargés par des applications du Windows Store et par Internet Explorer, ainsi que les téléchargements malveillants** sous **Participer à l'amélioration des produits et services**. Après avoir configuré Windows, vous pouvez modifier ce paramètre dans la section Centre de maintenance du Panneau de configuration. Pour plus d'informations sur Internet Explorer SmartScreen, voir la section « Filtre SmartScreen » de la [Déclaration de confidentialité d'Internet Explorer](#).

[Haut de la page](#)

Reconnaissance vocale de Windows

### Quel est le rôle de cette fonctionnalité ?

La fonctionnalité Reconnaissance vocale Windows assure la reconnaissance vocale aussi bien dans Windows que dans les applications qui choisissent de l'utiliser. La reconnaissance vocale de Windows augmente sa précision en apprenant comment vous utilisez la langue, y compris les sons et les mots que vous aimez employer.

### Informations collectées, traitées ou transmises

La reconnaissance vocale de Windows stocke une liste de mots et leur(s) prononciation(s) sur votre PC. Pour ajouter des mots et leur(s) prononciation(s) à cette liste, vous pouvez soit utiliser le dictionnaire vocal, soit utiliser la reconnaissance vocale de Windows pour dicter et corriger les mots.

Lorsque la fonctionnalité d'analyse de document de la reconnaissance vocale de Windows est activée, le texte des documents Microsoft Office Word (portant l'extension de nom de fichier .doc ou .docx) et des messages électroniques (dans les dossiers de courrier électronique, à l'exception des dossiers Éléments supprimés et Courrier indésirable) sur votre ordinateur et sur tout partage de fichiers

connecté figurant dans les emplacements de l'index de recherche Windows est collecté et stocké sous forme de fragments comprenant un, deux ou trois mots. Les fragments d'un mot contiennent uniquement les mots que vous avez ajoutés à des dictionnaires personnels, tandis que les fragments de deux ou trois mots contiennent uniquement les mots trouvés dans les dictionnaires standard.

Toutes les informations collectées sont stockées dans votre profil de voix personnel sur votre PC. Un profil de voix est stocké pour chaque utilisateur. Toutefois, un utilisateur n'a pas accès aux profils des autres utilisateurs de votre PC. Les administrateurs, eux, ont accès à tous les profils se trouvant sur votre PC. Les informations relatives aux profils ne sont pas envoyées à Microsoft, sauf si vous indiquez le contraire lorsque la reconnaissance vocale de Windows vous le demande. Vous avez la possibilité d'examiner les données avant de les envoyer. Si vous choisissez d'envoyer ces informations, les données d'adaptation acoustique appliquées à vos caractéristiques audio sont également envoyées.

Au terme d'une session d'apprentissage de la voix, la reconnaissance vocale de Windows vous demande si vous souhaitez envoyer des informations sur votre profil de voix à Microsoft. Vous pouvez passer en revue les informations avant de les envoyer. Ces informations peuvent contenir des enregistrements de votre voix réalisés au cours de la session d'apprentissage, ainsi que d'autres informations issues de votre profil de voix personnel.

### **Utilisation des informations**

La reconnaissance vocale de Windows utilise des mots du profil de voix pour convertir votre voix en texte. Microsoft utilise les informations de votre profil de voix personnel dans le but d'améliorer ses produits et ses services. Nous n'utilisons pas ces informations pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

### **Choix et contrôle**

Vous êtes libre d'exécuter ou non la reconnaissance vocale de Windows. Si vous exécutez la reconnaissance vocale de Windows, la fonctionnalité d'analyse de document est activée par défaut. Vous avez la possibilité de modifier les paramètres d'analyse de document

lorsque vous exécutez la reconnaissance vocale de Windows pour la première fois. Pour modifier les paramètres d'analyse de document ou supprimer des profils de voix personnels (et la plupart des informations d'analyse de document), ouvrez Reconnaissance vocale dans le Panneau de configuration, puis cliquez sur **Options vocales avancées**. Vous pouvez également utiliser l'option Modifier des mots dans le dictionnaire vocal pour supprimer des mots que vous avez ajoutés à votre profil de voix. Toutefois, le fait de supprimer votre profil de voix personnel n'entraîne pas la suppression des mots qui ont été ajoutés par le biais du dictionnaire vocal.

Vous pouvez contrôler les emplacements à partir desquels l'analyse de document collecte des fragments de mots en modifiant les emplacements définis dans l'index de recherche Windows. Pour afficher ou modifier les emplacements définis dans l'index de recherche Windows, ouvrez Options d'indexation dans le Panneau de configuration.

À la fin d'une session d'apprentissage, vous êtes invité à envoyer des données relatives à votre apprentissage ainsi que d'autres informations sur votre profil à Microsoft. Vous pouvez également envoyer des informations lorsque la reconnaissance vocale de Windows est en cours d'exécution. Pour cela, cliquez avec le bouton droit sur **Microphone**, puis cliquez sur **Participer à l'amélioration de la Reconnaissance vocale**. Dans les deux cas, vous avez toujours la possibilité d'afficher les fichiers de données avant de les envoyer, puis de décider de leur envoi.

[Haut de la page](#)

Windows Store

Le Windows Store vous permet de rechercher des applications pour votre PC, de les gérer et de les installer. Les sections ci-dessous décrivent l'impact que peuvent avoir les fonctionnalités du Windows Store et les applications que vous téléchargez depuis le Windows Store sur vos informations personnelles, et ce que vous pouvez faire pour contrôler cela.

## Applications et services du Windows Store

### Quel est le rôle de cette fonctionnalité ?



Le Windows Store vous permet de rechercher des applications pour votre PC et de les installer. Il fait également le suivi des applications que vous installez. Ainsi, vous pouvez obtenir des mises à jour pour vos applications et installer celles-ci sur plusieurs PC.

### **Informations collectées, traitées ou transmises**

Pour rechercher et installer des applications, vous devez vous connecter au Windows Store à l'aide d'un compte Microsoft. De cette façon, le Windows Store peut accéder aux informations de contact stockées dans votre profil de compte Microsoft, en particulier vos nom, adresse de messagerie et avatar de compte. Le Windows Store collecte d'autres informations qu'il associe à votre compte Windows Store. Ces informations sont les suivantes :

- Paiements effectués dans le Windows Store. Informations sur vos achats, le montant payé et le mode de paiement utilisé pour acheter des applications ou réaliser des achats dans des applications avec votre compte Windows Store.
- Applications installées. Liste des applications que vous avez installées à partir du Windows Store, stratégie de licence pour chaque application (licence permanente ou version d'évaluation sur une durée déterminée) et liste des achats que vous avez effectués avec votre compte Windows Store dans chaque application. Outre le stockage en ligne de ces informations avec votre compte, le Windows Store stocke les informations de licence sur votre PC pour chaque application installée. Ces informations vous identifient comme le propriétaire de la licence.
- PC sur lesquels vous avez installé des applications. Marque, modèle, nom d'ordinateur de chaque PC sur lequel vous installez des applications, et nombre qui identifie de façon unique le PC. Ce nombre, qui est généré d'après la configuration matérielle du PC, ne contient aucune information vous concernant.
- Notations, évaluations et rapports de problèmes. Après avoir installé une application, vous avez la possibilité de l'évaluer ou de la noter dans le Windows Store. Votre compte Microsoft est associé à ces notations. Si vous rédigez une évaluation, le nom et l'avatar de votre compte Microsoft sont publiés avec votre

évaluation.

- Préférences du Windows Store. Préférences relatives à l'affichage des applications dans le Windows Store. Vous pouvez, par exemple, spécifier d'afficher uniquement les applications qui sont disponibles dans votre langue maternelle.

Vous avez aussi la possibilité de stocker vos informations de paiement, comme un numéro de carte de crédit, avec votre compte Windows Store. À des fins de sécurité, ces informations sont transmises sur SSL et le numéro de votre carte de crédit (à l'exception des quatre derniers chiffres) est stocké de manière chiffrée.

Le Windows Store collecte des informations sur votre copie de Windows pour déterminer si vous l'avez achetée dans le commerce, s'il s'agit d'une version d'évaluation, si elle entre dans le cadre d'un programme de licence en volume ou bien si elle a été préinstallée par le fabricant de votre PC. Lors de la première connexion au Windows Store, la liste de toutes les applications préinstallées sur votre ordinateur est envoyée au Windows Store, qui associe alors les licences de ces applications à votre compte Windows Store.

Lorsque vous parcourez le Store et que vous utilisez des applications, Microsoft collecte des informations pour mieux comprendre vos habitudes et tendances d'utilisation, au même titre que de nombreux sites Web analysent les données de navigation de leurs visiteurs.

### **Utilisation des informations**

Microsoft utilise vos informations de contact pour vous envoyer des messages électroniques relatifs aux services du Windows Store, par exemple les reçus des applications que vous avez achetées. Le Windows Store utilise vos informations de paiement pour vous permettre de régler vos achats ; si vous optez pour le stockage de ces informations, vous n'êtes pas obligé de les entrer chaque fois. Microsoft utilise les informations sur vos achats pour gérer le Windows Store et assurer le support technique.

Le Windows Store fait le suivi de toutes les applications que vous installez. Pour gérer la liste des périphériques sur lesquels vous avez installé des applications, vous pouvez passer par le Windows Store ou bien contacter le support technique pour obtenir de l'aide. Une fois

que vous avez installé une application, celle-ci est répertoriée dans votre historique des achats du Windows Store, et ce même si vous décidez de la désinstaller. Le Windows Store a également recours à cette liste pour limiter le nombre de PC sur lesquels vous pouvez installer des applications, conformément aux conditions d'utilisation du Windows Store. Lorsque vous évaluez une application, le nom et l'avatar du compte associés à votre compte Windows sont publiés dans le Windows Store en regard de votre évaluation. Si vous signalez un problème rencontré avec une application, le rapport de problème est mis à la disposition des responsables du Windows Store afin qu'ils puissent évaluer la situation et prendre les actions nécessaires. En cas de besoin, votre nom et l'adresse de messagerie associés à votre compte Windows Store peuvent être utilisés pour vous contacter.

Si des mises à jour sont publiées pour des applications que vous avez installées, une notification s'affiche dans le Windows Store. En outre, la vignette du Windows Store indique le nombre de mises à jour disponibles. Vous pouvez alors afficher la liste des mises à jour disponibles et sélectionner celles que vous voulez installer. Il est possible que des applications mises à jour utilisent des fonctionnalités de Windows différentes de celles des versions précédentes, leur donnant ainsi accès à d'autres ressources sur votre PC. Vous pouvez consulter les listes de fonctionnalités mises à jour dans les pages Description de l'application. Pour y accéder, cliquez sur les liens situés dans la page répertoriant les mises à jour disponibles.

Le Windows Store utilise les informations collectées sur votre copie de Windows pour déterminer comment Windows a été installé sur votre PC (par exemple, si le fabricant de votre PC l'a préinstallé). Ces informations permettent au Windows Store de vous donner accès aux applications proposées en exclusivité par le fabricant à ses clients. Elles sont également utilisées pour fournir des informations à Microsoft (et de manière globale au fabricant, dans certains cas) sur les habitudes d'utilisation de Windows.

Microsoft utilise de manière globale les données d'achat et d'utilisation relatives à certaines applications pour comprendre le comportement des utilisateurs dans le Windows Store (par exemple, comment ils trouvent les applications qu'ils l'installent). Microsoft peut être amené à partager certaines de ces statistiques globales avec des

développeurs d'applications. Microsoft ne transmet pas vos informations personnelles aux développeurs d'applications. Nous utilisons les données relatives la navigation et à l'utilisation collectées par le Windows Store afin de mieux comprendre le comportement des utilisateurs dans le Windows Store et d'améliorer les fonctionnalités et les services du Windows Store.

### **Choix et contrôle**

Si vous choisissez d'utiliser le Windows Store, les informations décrites dans cette section sont envoyées à Microsoft comme décrit ci-dessus.

Si vous souhaitez supprimer une évaluation que vous avez publiée pour une application, accédez à la description de l'application dans le Windows Store, modifiez l'évaluation et supprimez tout le texte.

## **Mises à jour automatiques des applications**

### **Quel est le rôle de cette fonctionnalité ?**

Cette fonctionnalité recherche, télécharge et installe des mises à jour pour les applications du Windows Store pour s'assurer que vous disposez des versions les plus récentes. Les mises à jour des applications peuvent inclure des mises à jour de sécurité, des mises à jour des performances, de nouvelles fonctionnalités ou du nouveau contenu. Il est possible que des applications mises à jour utilisent des fonctionnalités de Windows différentes de celles des versions précédentes, leur donnant ainsi accès à d'autres ressources sur votre PC. Vous pouvez obtenir des informations sur les modifications des fonctionnalités dans la page Description du produit de l'application dans le Windows Store.

### **Informations collectées, traitées ou transmises**

Pour permettre les mises à jour automatiques des applications, le Windows Store envoie les informations suivantes à Microsoft :

- liste des applications installées à partir du Windows Store par tous les utilisateurs sur votre ordinateur ;
- informations de licence pour chaque application ;
- réussites, échecs et erreurs que vous rencontrez lors de la mise à jour des applications à partir du Windows Store ;

- identificateur global unique (GUID) : nombre généré de façon aléatoire qui ne contient aucune information personnelle ;
- nom, numéro de révision et date de révision du BIOS ;
- informations de base relatives à votre ordinateur (fabricant, modèle et édition de Windows utilisée).

## Utilisation des informations

Ces informations sont utilisées pour dispenser le service de mise à niveau. Elles permettent également de générer des statistiques globales que nous utilisons pour analyser les tendances et améliorer nos produits et services. Elles ne sont pas utilisées pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

## Choix et contrôle

Si vous optez pour la configuration rapide de Windows au cours de son installation, le Windows Store recherche, télécharge et installe automatiquement les mises à jour des applications, même si vous êtes déconnecté du Windows Store. Si vous désactivez les mises à jour automatiques des applications, vous pouvez choisir, ou non, d'installer une mise à jour des applications au moment de vous connecter au Windows Store.

Pour désactiver les mises à jour automatiques des applications :

1. Ouvrez le Windows Store.
2. Effectuez un balayage à partir du bord droit de l'écran, puis appuyez sur **Paramètres**.  
  
Si vous utilisez une souris, pointez sur l'angle inférieur droit de l'écran, puis cliquez sur **Paramètres**.
3. Appuyez ou cliquez sur **Mises à jour des applications**.
4. Appuyez ou cliquez sur **Mettre à jour automatiquement mes applications** pour désactiver les mises à jour automatiques des applications.

Pour en savoir plus sur ce que la version la plus récente de l'application permet d'accomplir et savoir quand une application a été

mise à jour pour la dernière fois, vous pouvez consulter la page Description du produit de l'application dans le Windows Store.

## Autorisation pour les applications du Windows Store

### **Quel est le rôle de cette fonctionnalité ?**

De nombreuses applications que vous téléchargez du Windows Store sont conçues pour exploiter des fonctionnalités matérielles et logicielles propres à votre PC. Par exemple, une application photo peut nécessiter l'utilisation de votre webcam, tandis qu'un guide des restaurants peut avoir besoin de connaître votre emplacement pour vous recommander les bonnes tables à proximité.

### **Informations collectées, traitées ou transmises**

Les applications doivent vous informer de l'utilisation des fonctionnalités suivantes :

- Connexion Internet. Permet à l'application de se connecter à Internet.
- Connexions entrantes via un pare-feu. Permet à l'application d'envoyer des informations vers ou depuis votre PC via un pare-feu.
- Réseau domestique ou professionnel. Permet à l'application d'envoyer des informations entre votre PC et d'autres PC sur le même réseau.
- Vos bibliothèques d'images, de vidéos, de musiques ou de documents. Permet à l'application d'utiliser, de modifier ou de supprimer des fichiers stockés dans vos bibliothèques, y compris certaines données incorporées à ces fichiers, telles que les informations de localisation dans les photos.
- Stockage amovible. Permet à l'application d'accéder à des fichiers, d'en ajouter, de les modifier ou de les supprimer sur un disque dur externe, un disque mémoire flash USB ou un appareil mobile.
- Informations d'identification Windows. Permet à l'application d'utiliser vos informations d'identification pour s'authentifier et

accéder à un intranet d'entreprise.

- Certificats stockés sur votre PC ou une carte à puce. Permet à l'application d'utiliser des certificats pour se connecter de façon sécurisée à des organisations telles que des banques, des agences publiques ou bien votre employeur.
- Fonctionnalité de messagerie texte de votre PC. Permet à l'application d'envoyer et de recevoir des messages texte.
- Webcam et microphone. Permet à l'application de prendre des photos et d'enregistrer des fichiers audio et vidéo.
- Emplacement. Permet à l'application de déterminer votre emplacement approximatif d'après les informations d'un capteur GPS ou du réseau.
- Fonctionnalité de communication en champ proche de votre PC. Permet à l'application de se connecter à d'autres appareils situés à proximité qui exécutent la même application.
- Appareils mobiles. Permet à l'application de communiquer avec des appareils tels que votre téléphone mobile, votre appareil photo numérique ou un lecteur de musique mobile.
- Informations sur un appareil mobile. Permet à l'application d'effectuer des opérations d'accès, d'ajout, de modification ou de suppression sur les contacts, calendriers, tâches, notes, états ou sonneries de votre appareil mobile.
- Compte haut débit mobile. Permet à l'application de gérer votre compte haut débit mobile.

Les fonctionnalités utilisées par une application sont répertoriées sur la page Description de l'application correspondante. Si vous installez une application, Windows l'autorise à utiliser ces fonctionnalités, excepté l'emplacement, la messagerie texte, la webcam et le microphone, qui sont considérés comme des éléments particulièrement sensibles. La première fois qu'une application fait une demande d'accès à ces fonctionnalités sensibles, Windows vous demande votre autorisation. Vous pouvez à tout moment revenir sur votre décision.

Outre les autorisations mentionnées ci-dessus, si une application demande des informations provenant d'un périphérique qui stocke des informations vous concernant ou concernant votre comportement, Windows vous demande si vous voulez autoriser l'application à les utiliser. Par exemple, si vous connectez un appareil d'activité physique qui suit votre localisation, Windows demande si l'application est autorisée à utiliser les informations qu'il contient.

### **Utilisation des informations**

L'utilisation de ces fonctionnalités par chaque application est sujette aux pratiques de ses développeurs en matière de confidentialité. Si une application utilise l'une des fonctionnalités sensibles décrites ci-dessus, un lien pointant vers la déclaration de confidentialité du développeur de l'application figure sur la page Description de l'application dans le Windows Store.

### **Choix et contrôle**

Avant d'installer une application, vous pouvez examiner dans le Windows Store les fonctionnalités dont elle a besoin. Windows vous demande si vous voulez autoriser ou refuser l'accès aux fonctionnalités les plus sensibles (emplacement, messagerie texte, webcam et microphone) la première fois qu'une application souhaite les utiliser.

Lorsque vous affichez la page Description de l'application d'une application dans le Windows Store, vous pouvez constater la présence d'une liste abrégée des fonctionnalités utilisées par l'application en bas de la colonne de gauche. La liste complète est disponible sur la page Détails de la Description de l'application. Une fois que vous avez installé une application, vous pouvez examiner à tout la liste complète des fonctionnalités qu'elle l'utilise et contrôler l'accès aux plus sensibles d'entre elles. Pour ce faire, ouvrez l'application, ouvrez

**Paramètres**, puis sélectionnez **Autorisations**.

## **Recherche dans le Windows Store et recommandations concernant les applications personnalisées**

### **Quel est le rôle de cette fonctionnalité ?**

Lorsque vous accédez au Windows Store ou que vous y recherchez des applications, Microsoft fournit des recommandations et des résultats



de recherche pour vous aider à trouver des applications pertinentes.

### **Informations collectées, traitées ou transmises**

Pour affiner les résultats de la recherche, le Windows Store envoie à Microsoft des informations sur la façon dont vous interagissez avec lui, notamment ce que vous recherchez et les résultats de recherche que vous sélectionnez. Le Windows Store envoie également un identificateur associé à votre compte Microsoft pour fournir des résultats de recherche personnalisés basés sur vos interactions avec Bing et d'autres produits et services Microsoft. Vous pouvez choisir de ne pas obtenir de résultats personnalisés, auquel cas l'identificateur n'est pas transmis.

### **Utilisation des informations**

Le Windows Store utilise l'identificateur associé à votre compte Microsoft pour fournir des résultats de recherche et des recommandations personnalisés basés sur vos interactions avec le Windows Store et d'autres produits et services Microsoft, tels que Bing et le Windows Phone Store. Cela inclut des informations telles que les applications que vous avez achetées, les informations de profil que vous avez fournies dans votre compte Microsoft, ainsi que vos notations et évaluations des applications. Ces informations peuvent également servir à personnaliser d'autres produits et services proposés par Microsoft.

### **Choix et contrôle**

Lorsque vous êtes connecté à Windows par le biais d'un compte Microsoft, les résultats et recommandations personnalisés du Windows Store sont désactivés par défaut. Vous pouvez choisir de ne pas obtenir de résultats et recommandations personnalisés du Windows Store dans la section **Préférences** des paramètres du Windows Store.

**Vous pouvez contribuer à améliorer le Windows Store en envoyant les URL du contenu Web que les applications utilisent.**

### **Quel est le rôle de cette fonctionnalité ?**

Certaines applications que vous téléchargez à partir du Windows Store sont semblables à des sites Web et peuvent rendre votre ordinateur

vulnérable à des logiciels potentiellement dangereux, notamment des programmes malveillants. Si vous choisissez d'activer cette fonctionnalité, elle collecte des informations sur le contenu Web utilisé par ces applications pour aider Microsoft à diagnostiquer tout comportement potentiellement dangereux. Par exemple, Microsoft est susceptible d'utiliser ces informations pour supprimer une application du Windows Store.

### **Informations collectées, traitées ou transmises**

Si vous choisissez d'envoyer des informations sur le contenu Web utilisé par vos applications, Microsoft collecte alors des informations sur les URL et les types de contenu auxquels ces applications accèdent lorsqu'elles sont en cours d'exécution. Cela peut permettre d'identifier des applications qui reçoivent du contenu de sites Web dangereux ou nuisibles. Les rapports envoyés à Microsoft comprennent des informations telles que le nom ou l'identificateur de l'application, les URL complètes des adresses auxquelles l'application accède, ainsi que les URL complètes indiquant l'emplacement de tout code JavaScript auquel l'application accède. Windows génère un identificateur global unique (GUID) qui est envoyé à Microsoft avec chaque rapport. Le GUID permet de déterminer les données qui sont envoyées au fil du temps à partir d'un ordinateur particulier. Le GUID ne contient aucune information personnelle et n'est pas utilisé dans le but de vous identifier.

Pour préserver la confidentialité de vos informations personnelles, les informations transmises à Microsoft sont chiffrées. Il peut s'agir d'informations qui peuvent être associées à une page Web à laquelle ces applications accèdent, comme les termes de recherche ou les données que vous avez entrées dans les applications. Par exemple, si vous recherchez un mot dans une application de dictionnaire, le mot que vous recherchez peut être inclus dans les informations envoyées à Microsoft dans le cadre de l'adresse complète à laquelle accède l'application. Dans la mesure du possible, Microsoft filtre ces adresses pour tenter de supprimer toute information personnelle.

### **Utilisation des informations**

Microsoft examine périodiquement les informations envoyées pour détecter les applications susceptibles d'interagir avec du contenu non

sécurisé, comme des adresses Web ou des scripts dangereux. Ces informations peuvent être utilisées pour prendre des mesures contre des applications potentiellement dangereuses. Il peut arriver que des adresses de contenu Web contiennent des informations personnelles, et ce de manière involontaire. Dans ce cas, sachez que ces informations ne sont pas utilisées pour vous identifier, vous contacter ou cibler des publicités à votre égard. Nous utilisons le GUID pour déterminer l'étendue des commentaires que nous recevons et les classer par ordre de priorité. Par exemple, le GUID permet à Microsoft de faire la distinction entre un comportement potentiellement dangereux se produisant 100 fois sur un seul PC et le même comportement se produisant une fois sur 100 PC.

### **Choix et contrôle**

Si vous sélectionnez la configuration rapide lors de l'installation de Windows, Windows envoie des informations sur le contenu Web utilisé par les applications provenant du Windows Store et écrites en JavaScript. Si vous choisissez de personnaliser les paramètres, vous pouvez contrôler ce paramètre en sélectionnant **Utiliser les services en ligne SmartScreen pour protéger le PC contre les contenus malveillants des sites chargés par des applications du Windows Store et par Internet Explorer, ainsi que les téléchargements malveillants** sous **Participer à l'amélioration des produits et services Microsoft**. Une fois l'installation terminée, vous pouvez modifier ce paramètre dans la section **Confidentialité** disponible dans Paramètres du PC.

[Haut de la page](#)

Service de temps Windows

### **Quel est le rôle de cette fonctionnalité ?**

Le service de temps Windows synchronise automatiquement l'heure de votre PC avec un serveur de temps sur un réseau.

### **Informations collectées, traitées ou transmises**

Le service se connecte à un serveur de temps sur Internet ou à un réseau local à l'aide du protocole de temps du réseau (NTP) standard. Par défaut, ce service se synchronise avec time.windows.com une fois

par semaine. À l'exception d'informations standard relatives au PC, aucune donnée n'est envoyée au serveur de temps.

## **Utilisation des informations**

Les informations sont utilisées par le service de temps Windows pour synchroniser automatiquement l'heure de votre ordinateur.

## **Choix et contrôle**

Le service de temps Windows est activé par défaut. Vous pouvez désactiver cette fonctionnalité dans la section **Date et heure** de Paramètres du PC. Le fait de désactiver le service de temps Windows n'a aucun effet direct sur les applications ou d'autres services, mais l'horloge de votre ordinateur, dépourvue de source de temps fiable, peut se désynchroniser des autres ordinateurs sur le réseau ou Internet. En cas de différence de temps importante entre les ordinateurs du réseau, il se peut que les applications et les services qui sont liés au temps échouent ou cessent de fonctionner correctement.

[Haut de la page](#)

Résolution des problèmes Windows

## **Quel est le rôle de cette fonctionnalité ?**

La fonctionnalité Résolution des problèmes Windows vous aide à diagnostiquer et à résoudre les problèmes fréquemment rencontrés sur votre ordinateur.

## **Informations collectées, traitées ou transmises**

Une fois l'exécution d'un pack de résolution des problèmes terminée, les résultats sont enregistrés sur votre PC. Ces résultats peuvent contenir des informations personnelles, telles que votre nom d'utilisateur ou le nom d'un périphérique. La fonctionnalité Résolution des problèmes Windows peut vous aider à rechercher des solutions à votre problème dans l'Aide de Windows et les communautés en ligne de Windows. Les mots clés associés au problème sont envoyés à Microsoft pour tenter de trouver une solution. Par exemple, si votre imprimante ne fonctionne pas correctement et que vous recherchez de l'aide, les mots « imprimante », « imprimer » et « impression » sont envoyés à Microsoft.

## Utilisation des informations

Microsoft utilise les informations collectées lors de l'exécution de la fonctionnalité Résolution des problèmes Windows pour résoudre les problèmes que rencontrent les utilisateurs.

### Choix et contrôle

Pour supprimer les résultats de la résolution des problèmes, accédez à la section Dépannage dans le Panneau de configuration. Cliquez sur **Afficher l'historique**, sélectionnez un résultat, puis cliquez sur **Supprimer**.

[Haut de la page](#)

Dossiers de travail

### Quel est le rôle de cette fonctionnalité ?

Les dossiers de travail sont des dossiers sur votre ordinateur qui sont automatiquement synchronisés avec le serveur de fichiers de votre espace de travail.

### Informations collectées, traitées, stockées ou transmises

Quand vous enregistrez un fichier dans un dossier de travail, il est automatiquement synchronisé sur un serveur de fichiers géré par votre espace de travail. Les fichiers enregistrés dans votre dossier de travail à partir d'autres ordinateurs se synchronisent sur votre ordinateur.

## Utilisation des informations

Windows envoie et reçoit les fichiers inclus dans vos dossiers de travail pour que les dossiers restent synchronisés. L'utilisation des informations stockées sur les serveurs de votre espace de travail est soumise à la politique de confidentialité de votre espace de travail.

### Choix et contrôle

Vous pouvez gérer la connexion de votre ordinateur aux dossiers de travail dans la section **Espace de travail** disponible dans Paramètres du PC.

[Haut de la page](#)

## Espace de travail

L'Espace de travail vous permet de connecter votre appareil à Windows Intune (nécessite un abonnement distinct auprès de Microsoft) ou à un autre service de gestion des périphériques tiers. Si vous choisissez d'autoriser l'administrateur de votre entreprise à gérer votre ordinateur à l'aide de l'Espace de travail, cet administrateur pourra effectuer des tâches telles qu'appliquer des stratégies de sécurité sur votre ordinateur, installer des applications, afficher certaines configurations et d'autres informations sur votre ordinateur, ainsi que d'autres tâches de gestion. Consultez la politique de confidentialité ou l'administrateur système de votre entreprise pour obtenir plus d'informations sur l'utilisation de cette fonctionnalité par votre entreprise.

### **Informations collectées, traitées ou transmises**

Lorsque vous configurez et utilisez l'Espace de travail, votre ordinateur communique avec le service de gestion des périphériques utilisé par votre entreprise, lequel peut être hébergé par Microsoft. Les informations d'identification que vous entrez pour vous connecter à votre espace de travail sont envoyées au service.

### **Utilisation des informations**

Les informations envoyées au service de gestion des périphériques sont utilisées pour établir une connexion entre le service et votre ordinateur, et vous autoriser à installer une application en libre service à partir du Windows Store. Consultez la politique de confidentialité ou l'administrateur système de votre entreprise pour obtenir plus d'informations sur l'application en libre service.

### **Choix et contrôle**

Si votre entreprise utilise l'Espace de travail, vous pouvez vous y connecter ou vous en déconnecter via la section **Réseaux** Paramètres du PC. Une fois votre ordinateur connecté au service, vous pouvez afficher les informations relatives à la connexion ou vous déconnecter à tout moment.

[Haut de la page](#)

Pour obtenir des informations à jour sur les pratiques de traitement des données de Microsoft, passez en revue l'[Énoncé de confidentialité Microsoft](#). Vous pouvez également en savoir plus sur les derniers outils que nous proposons pour accéder à vos données et les contrôler, ainsi que sur la manière dont vous pouvez nous contacter si vous avez une demande en matière de confidentialité.

# Déclaration de confidentialité de Windows 8.1 et de Windows Server 2012 R2

[Point essentiel](#) [Déclaration](#) [Fonctionnalités](#) [Applications](#) [Serveur](#)

Notez que cette page constitue un avenant à la Déclaration de confidentialité de Windows 8.1 et Windows Server 2012 R2 de (« Déclaration de confidentialité de Windows ») qui comprend les sections suivantes :

- [Points clés](#)
- [Déclaration](#), qui constitue l'intégralité de la Déclaration de confidentialité de Windows 8.1, inclut des liens vers les déclarations de confidentialité relatives aux fonctionnalités de Windows qui possèdent leur propre déclaration
- [Avenant aux fonctionnalités](#), qui décrit les fonctionnalités qui ont un impact de confidentialité dans Windows 8.1 et Windows Server 2012 R2
- **Avenant aux applications** (la présente page), qui décrit les applications qui ont un impact sur les informations personnelles dans Windows 8.1, et qui inclut des liens vers les déclarations de

confidentialité applicables à chaque application

- [Avenant à la version serveur](#), qui décrit les fonctionnalités supplémentaires qui ont un impact sur les informations personnelles dans Windows Server 2012 R2

Pour comprendre les méthodes de collecte et d'utilisation des données ayant trait à une fonctionnalité ou un service particulier de Windows, nous vous conseillons de lire l'intégralité de la Déclaration de confidentialité et tout avenant applicable ou toute déclaration individuelle.

Si vous choisissez de participer au programme d'amélioration de l'expérience utilisateur au moment où vous configurez votre PC, alors ces applications collectent des informations sur la manière dont vous utilisez chaque application, leurs performances et leur fiabilité pour les consigner dans un rapport. Microsoft s'appuie sur les renseignements issus de ce programme pour améliorer ses produits et services. Ces informations ne sont pas utilisées pour vous identifier, vous contacter ou vous envoyer des publicités ciblées. Vous pouvez désactiver le programme d'amélioration de l'expérience utilisateur dans les paramètres du PC. Pour plus d'informations, voir la [Déclaration de confidentialité du programme d'amélioration de l'expérience utilisateur](#).

Les liens suivants permettent d'accéder aux déclarations de confidentialité applicables à chacune des applications répertoriées :

[Alarme](#)

[Calculatrice](#)

[Calendrier](#)

[Appareil photo](#)

[Finances](#)

[Cuisine](#)

[Jeux](#)

[Santé](#)

[Aide et conseils](#)

[Courrier](#)



[Cartes](#)

[Musique](#)

[Actualités](#)

[Contacts](#)

[Lecteur](#)

[Liste de lectures](#)

[Numérisation](#)

[Skype](#)

[Magnétophone](#)

[Sport](#)

[Voyage](#)

[Vidéo](#)

[Météo](#)

Pour obtenir des informations à jour sur les pratiques de traitement des données de Microsoft, passez en revue l'[Énoncé de confidentialité Microsoft](#). Vous pouvez également en savoir plus sur les derniers outils que nous proposons pour accéder à vos données et les contrôler, ainsi que sur la manière dont vous pouvez nous contacter si vous avez une demande en matière de confidentialité.

# Déclaration de confidentialité de Windows 8.1 et de Windows Server 2012 R2

[Point essentiel](#) [Déclaration](#) [Fonctionnalités](#) [Applications](#) [Serveur](#)

Dans cette page

[Journalisation des accès utilisateur](#)

[Gestionnaire de serveur](#)

[Services AD FS \(Active Directory Federation Services\)](#)

[Gestion des adresses IP](#)

[Accès à distance unifié](#)

[Services Bureau à distance](#)

[Programme](#)

Cette page constitue un avenant à la Déclaration de confidentialité Windows 8.1 et Windows Server 2012 R2 (« Déclaration de confidentialité Windows »). Celle-ci comprend les sections suivantes :

- [Points clés](#)
- [Déclaration](#), qui constitue l'intégralité de la Déclaration de confidentialité de Windows 8.1, et qui inclut des liens vers les déclarations de confidentialité relatives aux fonctionnalités de Windows qui possèdent leur propre déclaration
- [Avenant aux fonctionnalités](#), qui décrit les fonctionnalités qui ont un impact de confidentialité dans Windows 8.1 et Windows Server 2012 R2
- [Avenant aux applications](#), qui décrit les applications qui ont un impact de confidentialité dans Windows 8.1
- **Avenant à la version serveur** (cette page), qui décrit les

d'amélioration du produit Windows (CEIP) et rapport d'erreurs Windows (WER)

Journalisation de l'inventaire logiciel

fonctionnalités supplémentaires qui ont un impact de confidentialité dans Windows Server 2012 R2

Pour comprendre les méthodes de collecte et d'utilisation des données ayant trait à une fonctionnalité ou un service particulier de Windows, nous vous conseillons de lire l'intégralité de la Déclaration de confidentialité Windows et tout avenant applicable ou toute déclaration individuelle. Nous vous recommandons également de lire [ce livre blanc destiné aux administrateurs](#).

Pour plus d'informations sur l'impact de confidentialité des fonctionnalités incluses dans Windows Server 2012 R2 Essentials, consultez la [Déclaration de confidentialité Windows Server 2012 R2 Essentials et Windows Server Essentials Experience](#).

Journalisation des accès utilisateur

### **Quel est le rôle de cette fonctionnalité ?**

La journalisation des accès utilisateur collecte et regroupe les enregistrements des demandes de client de rôles de serveur (demandes utilisateur et de périphérique), ainsi que les produits installés (s'ils sont inscrits auprès de la journalisation des accès utilisateur) sur le serveur local. Ces données, sous la forme d'adresses IP, de noms d'utilisateur et dans certains cas, de noms d'hôte et/ou d'identités de machine virtuelle, sont stockées dans les bases de données locales du moteur ESE (Extensible Storage Engine) et sont accessibles uniquement par les administrateurs. UAL a un fournisseur WMIv2 et des applets de commande Windows PowerShell associées pour récupérer des données d'accès utilisateur destinées à la gestion des droits de licence d'accès client hors ligne, où les enregistrements réels de demandes de client uniques sont critiques.

### **Informations collectées, traitées ou transmises**

Les adresses IP, les noms d'utilisateur et, dans certains cas, les noms d'hôte (si le rôle de DNS est installé) et les identités de machine virtuelle (si le rôle Hyper-V est installé) sont collectés localement sur le serveur quand UAL est activé. Aucune donnée collectée n'est envoyée à Microsoft.

## Utilisation des informations

Les données UAL sont mises à la disposition des administrateurs via des bases de données ESE locales, le fournisseur WMI et les applets de commande Windows PowerShell. Windows n'utilise pas ces données en dehors de la fonctionnalité UAL.

## Choix et contrôle

La journalisation des accès utilisateur est activée par défaut. Le service de journalisation des accès utilisateur peut être arrêté et démarré lorsque le serveur est en cours d'exécution. Pour désactiver définitivement UAL, ouvrez Windows PowerShell, tapez Désactiver-UAL, puis redémarrez le serveur. Pour supprimer toutes les données historiques collectées, un administrateur doit d'abord arrêter le service, désactiver la journalisation des accès utilisateur, puis supprimer tous les fichiers contenus dans le dossier %SystemRoot%\System32\LogFiles\SUM.

[Haut de la page](#)

Gestionnaire de serveur

## Quel est le rôle de cette fonctionnalité ?

Le Gestionnaire de serveur est un outil de gestion qui permet à un administrateur d'analyser un ou plusieurs serveurs, ainsi que d'afficher l'état général ou spécifique à un rôle, afin d'effectuer des tâches de gestion et d'accéder à d'autres outils de gestion du serveur.

## Informations collectées, traitées ou transmises

Le Gestionnaire de serveur collecte les types d'informations suivants sur un serveur géré par l'administrateur :

- **Informations générales du serveur** : nom NetBios et nom de domaine complet (FQDN), informations d'identification entrées dans la fonctionnalité « Gérer en tant que », adresse IPv4, adresse IPv6, état de la facilité de gestion, description, version du système d'exploitation, type, dernière mise à jour, processeurs, mémoire, nom du cluster, type d'objet de cluster, état de l'activation, SKU, architecture du système d'exploitation, fabricant, configuration du programme d'amélioration du produit

et configuration du rapport d'erreur Windows.

- **Événements** : ID, gravité, source, journal, date et heure de chaque événement Windows et autres journaux choisis par l'administrateur.
- **Tous les services** : nom, état et type de démarrage.
- **Informations sur les rôles serveur** : résultats du BPA (Best Practice Analyzer) pour les rôles qui sont installés sur le serveur.
- **Informations sur les performances** : exemples des compteurs de performances et notifications concernant l'utilisation du processeur et la mémoire disponible.

### **Utilisation des informations**

Ces informations sont stockées dans le Gestionnaire de serveur et ne sont pas envoyées à Microsoft. Elles sont affichées dans le Gestionnaire de serveur pour aider les administrateurs à contrôler les systèmes.

### **Choix et contrôle**

Un administrateur peut activer ou désactiver la collecte des données pour n'importe quel serveur, à l'exception toutefois du serveur local, en ajoutant ou en supprimant le serveur dans le Gestionnaire de serveur. Un administrateur peut fournir de manière explicite des informations d'identification pour se connecter à un serveur distant. Le Gestionnaire de serveur demande à l'administrateur d'approuver explicitement le stockage local des informations d'identification dans le Gestionnaire de serveur, l'administrateur ayant à tout moment la possibilité de supprimer ces informations d'identification.

[Haut de la page](#)

Services AD FS (Active Directory Federation Services)

### **Quel est le rôle de cette fonctionnalité ?**

Les servicesAD FS sont une fédération d'entreprise et une solution d'authentification unique pour les applications locales ou basées sur d'autres réseaux. Grâce aux services AD FS, les administrateurs

peuvent donner aux utilisateurs la possibilité de collaborer entre organisations et d'accéder facilement à des applications sur des réseaux locaux ou autres, et ce tout en veillant à la sécurité des applications. Les services AD FS utilisent un service de jeton de sécurité basé sur les services de domaine Active Directory (AD DS) pour authentifier les utilisateurs et émettre des jetons de sécurité à l'aide de différents protocoles. Le jeton est signé numériquement et contient les réclamations relatives à l'utilisateur, qui proviennent de chaque élément ou d'une combinaison des services AD DS, du protocole LDAP, de SQL Server ou d'un magasin personnalisé.

### **Informations collectées, traitées ou transmises**

Les informations d'identification d'un utilisateur sont collectées lorsque l'utilisateur s'authentifie auprès des services AD FS. Les informations d'identification sont envoyées immédiatement aux services de domaine Active Directory pour l'authentification et AD FS ne les stocke pas localement. Les attributs de l'utilisateur dans les services de domaine Active Directory peuvent être utilisés pour générer des revendications sortantes, selon les règles de réclamation configurées par l'administrateur AD FS. Les revendications sortantes sont envoyées aux partenaires approuvés avec lesquels un administrateur AD FS a établi une relation d'approbation. Aucune information n'est envoyée à Microsoft.

### **Utilisation des informations**

Microsoft n'a pas accès à ces informations. Ces informations sont uniquement destinées au client.

### **Choix et contrôle**

Vous pouvez utiliser les services AD FS pour collecter ou envoyer des données à des partenaires approuvés.

[Haut de la page](#)

Gestion des adresses IP

### **Quel est le rôle de cette fonctionnalité ?**

La gestion des adresses IP (IPAM, IP Address Management) permet aux administrateurs de serveur d'effectuer le suivi de l'adresse IP, du

nom d'hôte et de l'identificateur du client (comme l'adresse MAC dans IPv4 et le DUID dans IPv6) des ordinateurs ou des périphériques d'un réseau à l'aide des informations d'ouverture de session utilisateur.

### **Informations collectées, traitées ou transmises**

Le serveur IPAM collecte les journaux et les événements d'audit des serveurs DHCP, des contrôleurs de domaine et des serveurs NPS (Network Policy Server), puis stocke localement l'adresse IP, le nom d'hôte, l'identificateur du client et le nom de l'utilisateur connecté. Un administrateur de serveur peut rechercher les journaux collectés selon l'adresse IP, l'identificateur du client, le nom d'hôte et le nom d'utilisateur à l'aide de la console IPAM. Aucune information n'est envoyée à Microsoft.

### **Utilisation des informations**

Microsoft n'a pas accès à ces informations. Ces informations sont uniquement destinées au client.

### **Choix et contrôle**

IPAM n'est pas installé par défaut et doit être installé par l'administrateur de serveur. Une fois IPAM installé, l'audit des adresses IP est automatiquement activé. Pour désactiver l'audit des adresses IP sur un serveur sur lequel IPAM est installé, démarrer le Planificateur de tâches sur le serveur IPAM, accédez à la tâche d'audit sous Microsoft\Windows\IPAM, puis désactivez la tâche.

[Haut de la page](#)

Accès à distance unifié

### **Quel est le rôle de cette fonctionnalité ?**

L'accès à distance unifié permet aux utilisateurs distants de se connecter à un réseau privé, tel qu'un réseau d'entreprise, sur Internet. L'accès à distance unifié utilise DirectAccess pour fournir aux réseaux d'entreprise des ordinateurs clients distants qui exécutent Windows 8 avec une connectivité sans interruption et transparente. Il fournit également la fonctionnalité de service d'accès à distance, qui est traditionnellement un service VPN, y compris la connectivité de site à site au niveau local ou sur d'autres réseaux.

## **Informations collectées, traitées ou transmises**

Dans le cadre de l'analyse des utilisateurs de l'accès à distance unifié, le serveur DirectAccess stocke les détails des utilisateurs distants se connectant au réseau privé. Cela inclut des informations telles que le nom d'hôte de l'utilisateur à distance, le nom d'utilisateur Active Directory et une adresse IP publique du client distant (si le client est derrière la traduction d'adresses réseau (NAT), il sera l'adresse IP publique). Ces données peuvent également être stockées sur les serveurs de base de données interne Windows (WID)/RADIUS, uniquement avec le consentement de l'administrateur. Seul un administrateur DirectAccess (utilisateur de domaine avec un compte d'administrateur local) accédant à un serveur peut voir ces informations et les consulter.

## **Utilisation des informations**

Ces informations sont utilisées par l'administrateur pour résoudre les problèmes liés à la connectivité des clients, ainsi qu'à des fins d'audit ou de mise en conformité. Aucune information n'est envoyée à Microsoft.

## **Choix et contrôle**

L'analyse des clients distants est activée par défaut et ne peut pas être désactivée. Les données d'analyse ne sont stockées dans les serveurs WID/RADIUS que si un administrateur a configuré l'utilisation d'une de ces options dans la gestion des comptes. Si aucun administrateur n'a configuré la gestion des comptes, aucune de ces informations n'est stockée. Un administrateur peut également configurer la gestion des comptes sur un serveur d'accès à distance de manière à ne pas stocker le nom d'utilisateur et les informations d'adresse IP.

[Haut de la page](#)

Services Bureau à distance

## **Quel est le rôle de cette fonctionnalité ?**

Les services Bureau à distance sont une plateforme visant à aider les entreprises à implémenter une stratégie de Bureau centralisée, à gérer les ordinateurs de bureau et les applications, et à améliorer la



flexibilité et la conformité tout en renforçant la protection des données.

### **Informations collectées, traitées ou transmises**

Dans le cadre de l'analyse des utilisateurs des services Bureau à distance, le serveur hôte de session Bureau à distance stocke des informations sur les utilisateurs distants se connectant à des ressources des services Bureau à distance. Cela inclut des informations telles que le nom d'hôte de l'utilisateur à distance, le nom d'utilisateur Active Directory et une adresse IP publique du client distant (si le client est derrière la traduction d'adresses réseau (NAT), il sera l'adresse IP publique). Ces données sont stockées automatiquement sur les serveurs de base de données interne Windows (WID)/SQL lorsque les utilisateurs se connectent. Aucune information n'est envoyée à Microsoft. Seul un utilisateur de domaine qui possède un compte d'administrateur local peut accéder à ces informations et les afficher.

### **Utilisation des informations**

Ces informations sont utilisées par l'administrateur pour résoudre les problèmes liés à la connectivité des clients, ainsi qu'à des fins d'audit interne ou de mise en conformité. Aucune information n'est envoyée à Microsoft.

### **Choix et contrôle**

L'analyse des clients est activée par défaut et ne peut pas être désactivée. Les informations d'analyse sont stockées dans le serveur WID/SQL.

[Haut de la page](#)

Programme d'amélioration du produit Windows (CEIP) et rapport d'erreurs Windows (WER)

### **Quel est le rôle de cette fonctionnalité ?**

Pour plus d'informations sur ces fonctionnalités, voir l'onglet [Avenant aux fonctionnalités](#) ou [ce livre blanc pour les administrateurs](#).

### **Informations collectées, traitées ou transmises**

Pour en savoir plus sur les informations spécifiques qui sont collectées, traitées et transmises par ces fonctionnalités, consultez les rubriques CEIP et WER de l'onglet [Avenant aux fonctionnalités](#) .

## Utilisation des informations

Pour en savoir plus sur la façon dont nous utilisons les informations collectées par ces fonctionnalités, consultez les rubriques CEIP et WER de l'onglet [Avenant aux fonctionnalités](#) .

## Choix et contrôle

Le programme CEIP est désactivé par défaut et la fonctionnalité WER est configurée par défaut de manière à générer une invite avant d'envoyer des rapports d'incident à Microsoft. Vous pouvez activer et désactiver la fonctionnalité Programme d'amélioration de l'expérience utilisateur à partir du Panneau de configuration du Gestionnaire de serveur et en utilisant des méthodes de contrôle en ligne de commande. La fonctionnalité Rapport d'erreurs Windows ne peut être contrôlée qu'à l'aide de méthodes en ligne de commande.

Pour activer ou désactiver la fonctionnalité Programme d'amélioration de l'expérience utilisateur à l'aide du Panneau de configuration, cliquez sur **Systeme et maintenance**, puis sur **Rapports et solutions aux problèmes**. Ensuite, sous **Voir aussi**, cliquez sur **Paramètres d'amélioration de l'expérience utilisateur** pour activer ou désactiver la fonctionnalité Programme d'amélioration de l'expérience utilisateur.

## Contrôles du Gestionnaire de serveur

Serveur local

- Activer la fonctionnalité Programme d'amélioration de l'expérience utilisateur  
Ouvrez le Gestionnaire de serveur et sélectionnez **Serveur local**. Cliquez sur le lien Programme d'amélioration de l'expérience utilisateur, sélectionnez **Oui, je souhaite participer au Programme d'amélioration de l'expérience utilisateur** dans la boîte de dialogue, puis cliquez sur **OK**.
- Désactiver la fonctionnalité Programme d'amélioration de l'expérience utilisateur  
Ouvrez le Gestionnaire de serveur et sélectionnez **Serveur**

**local.** Cliquez sur le lien Programme d'amélioration de l'expérience utilisateur, sélectionnez **Non, je ne souhaite pas participer** dans la boîte de dialogue, puis cliquez sur **OK**.

- Activer la fonctionnalité Rapport d'erreurs Windows  
Ouvrez le Gestionnaire de serveur et sélectionnez **Serveur local**. Cliquez sur le lien Rapport d'erreurs Windows, sélectionnez **Oui, envoyer automatiquement des rapports**, puis cliquez sur **OK**.
- Désactiver la fonctionnalité Rapport d'erreurs Windows  
Ouvrez le Gestionnaire de serveur et sélectionnez **Serveur local**. Cliquez sur le lien Rapport d'erreurs Windows, sélectionnez **Je ne veux pas participer, et Ne pas me demander à nouveau**, puis cliquez sur **OK**.

Plusieurs machines

- Activer la fonctionnalité Programme d'amélioration de l'expérience utilisateur  
Ouvrez le Gestionnaire de serveur et sélectionnez **Tous les serveurs**. Dans la vignette des serveurs, sélectionnez Tous les serveurs (Ctrl + A), cliquez avec le bouton droit, puis sélectionnez **Configurer le signalement de problèmes automatique Windows**. Sous l'onglet Programme d'amélioration de l'expérience utilisateur, sélectionnez **Oui, je souhaite y participer (recommandé)**. Appliquez ce paramètre à tous les serveurs en activant la case à cocher située en regard de Nom du serveur dans le contrôle Sélection des serveurs, puis cliquez sur **OK**.
- Désactiver la fonctionnalité Programme d'amélioration de l'expérience utilisateur  
Ouvrez le Gestionnaire de serveur et sélectionnez Tous les serveurs. Dans la vignette des serveurs, sélectionnez Tous les serveurs (Ctrl + A), cliquez avec le bouton droit, puis sélectionnez **Configurer le signalement de problèmes automatique Windows**. Sous l'onglet Programme d'amélioration de l'expérience utilisateur, sélectionnez **Non, je ne souhaite pas participer**. Appliquez ce paramètre à tous les

serveurs en activant la case à cocher située en regard de Nom du serveur dans le contrôle Sélection des serveurs, puis cliquez sur **OK**.

- Activer la fonctionnalité Rapport d'erreurs Windows  
Ouvrez le Gestionnaire de serveur et sélectionnez **Tous les serveurs**. Dans la vignette des serveurs, sélectionnez Tous les serveurs (Ctrl + A), cliquez avec le bouton droit, puis sélectionnez **Configurer le signalement de problèmes automatique Windows** . Sur l'onglet Rapport d'erreurs Windows, sélectionnez **Oui, envoyer automatiquement des rapports (recommandé)**. Appliquez ce paramètre à tous les serveurs en activant la case à cocher située en regard de Nom du serveur dans le contrôle Sélection des serveurs, puis cliquez sur **OK**.
- Désactiver la fonctionnalité Rapport d'erreurs Windows  
Ouvrez le Gestionnaire de serveur et sélectionnez **Tous les serveurs**. Dans la vignette des serveurs, sélectionnez Tous les serveurs (Ctrl + A), cliquez avec le bouton droit, puis sélectionnez **Configurer le signalement de problèmes automatique Windows** . Sur l'onglet Rapport d'erreurs Windows, sélectionnez **Non, je ne souhaite pas participer**. Appliquez ce paramètre à tous les serveurs en activant la case à cocher située en regard de Nom du serveur dans le contrôle Sélection des serveurs, puis cliquez sur **OK**.

[Haut de la page](#)

Journalisation de l'inventaire logiciel

### **Quel est le rôle de cette fonctionnalité ?**

La journalisation de l'inventaire logiciel fournit un nouvel ensemble de classes WMI et d'applets de commande Powershell pour simplifier l'inventaire de base de l'édition du système d'exploitation Windows Server, du logiciel installé sur Windows Server et des caractéristiques du serveur sur lequel le logiciel est en cours d'exécution. En outre, la journalisation de l'inventaire logiciel peut collecter toutes les heures des données en provenance de son

fournisseur WMI (si cette fonctionnalité est activée par un administrateur) et les transférer sur le réseau au serveur d'agrégation, si ce dernier a été spécifié à l'aide de l'applet de commande Set-SilLogging -TargetUri.

### **Informations collectées, traitées ou transmises**

Les données peuvent être transmises au serveur d'agrégation sur le réseau si cette option a été configurée par un administrateur. Par défaut, rien n'est collecté, traité ou transmis. Ces données incluent :

- Le nom Windows Server et l'édition du système d'exploitation installé.
- Une liste des noms, des versions et des éditeurs de tous les logiciels installés sur le serveur, ainsi que la date d'installation du logiciel.
- Le nom de domaine complet du système du serveur.
- Le nombre, le type et le fabricant des processeurs, processeurs logiques et cœurs installés ou affectés au système du serveur.

Les données collectées et traitées, mais pas transmises par défaut, même si la tâche horaire est activée et qu'un agrégateur cible est spécifié par l'administrateur :

- La classe MsftSil\_UalAccess et l'applet de commande Get-SilUalAccess traitent le nombre total d'utilisateurs uniques et de périphériques de chaque rôle ou produit enregistré avec la fonctionnalité de journalisation des accès utilisateur dans les deux jours précédant la requête. Il s'agit uniquement de chiffres, aucune information sur les utilisateurs ou les périphériques n'est imprimée ou transmise. SIL doit traiter les informations sur l'utilisateur et sur le périphérique à partir des classes UAL pour effectuer les calculs. Ces données sont accessibles uniquement par un administrateur de l'ordinateur local. SIL ne modifie pas l'accès nécessaire aux API UAL.

Aucune donnée collectée n'est envoyée à Microsoft.

### **Utilisation des informations**

Les fournisseurs WMI SIL regroupent les données fournies par d'autres

API qui existent déjà sur le système. Les données peuvent être transmises à un serveur pour une agrégation supplémentaire sur le réseau si cette option a été configurée par un administrateur. Par défaut, rien n'est collecté, traité ou transmis. Dans le cas de la classe MsftSil\_UalAccess et de l'applet de commande Get-SilUalAccess, les données traitées fournissent le nombre total d'utilisateurs uniques et de périphériques de chaque rôle ou produit enregistré avec la fonctionnalité de journalisation de l'accès utilisateur (UAL) dans les deux jours précédant la collecte, mais ne génèrent aucune donnée permettant d'identifier l'utilisateur ou le périphérique. Bien que cette classe WMI et que cette applet de commande existent sur le système, elles ne font pas partie de la charge utile de données SIL collectées et transmises à un agrégateur toutes les heures lorsque SIL a été configuré par un administrateur système pour le faire.

### **Choix et contrôle**

La tâche horaire SIL est désactivée par défaut. Toutes les API SIL sont disponibles par défaut pour toute requête effectuée par les administrateurs du système local. La tâche horaire SIL peut être démarrée et arrêtée pendant que le serveur est en cours d'exécution à l'aide des applets de commande Start-SilLogging et Stop-SilLogging. L'utilisation de l'applet de commande Set-SilLogging permet aux administrateurs du serveur de définir la date et l'heure auxquelles la tâche horaire commence (la valeur par défaut est de 3h à l'heure du système local), l'identificateur URI d'un serveur d'agrégation cible et l'empreinte de certificat nécessaire pour garantir une transmission des données en toute confiance.

Tous les paramètres de configuration SIL, y compris le démarrage et l'arrêt de la tâche horaire, peuvent être modifiés dans le Registre, mais uniquement lorsque le système est un ordinateur virtuel et avant qu'il ne soit démarré pour la première fois.

[Haut de la page](#)