

Pour plus d'informations sur les pratiques de traitement des données de Microsoft, veuillez consulter la [Déclaration de confidentialité Microsoft](#). Vous découvrirez également les derniers outils que nous proposons pour accéder à et contrôler vos données et comment nous contacter concernant toute demande de confidentialité.

Déclaration de confidentialité de Windows 8 et de Windows Server 2012

Points essentiels

[Déclaration](#) [Fonctionnalités supplémentaires](#) [Serveur supplémentaire](#)

Sur cette page

Dernière mise à jour : **Août 2012**

Vos informations

Ces points essentiels de la version complète [Déclaration de confidentialité de Windows 8 et de Windows Server 2012](#)

Vos choix.

(« Déclaration de confidentialité Windows ») présentent d'une manière générale la collecte de données et les bonnes pratiques de Windows 8 et Windows Server 2012 (« Windows »). Ils portent sur les fonctionnalités qui communiquent via Internet et n'ont pas pour objectif de constituer une description exhaustive. Ils ne s'appliquent pas aux autres sites en ligne/hors ligne, produits ou services de Microsoft.

Utilisations des informations

Comment nous contacter

Cette déclaration de confidentialité comprend quatre sections :

- Points essentiels (cette page)
- La déclaration, à savoir la déclaration de confidentialité Windows complète qui comprend des liens vers les fonctionnalités Windows disposant de leurs propres

déclarations autonomes

- La section Fonctionnalités supplémentaires, qui décrit les fonctionnalités ayant un impact sur la confidentialité dans Windows 8 et Windows Server 2012
- La section Serveur supplémentaire, qui décrit les fonctionnalités supplémentaires ayant un impact sur la confidentialité dans Windows Server 2012

Pour plus d'informations sur la manière de protéger votre ordinateur personnel, vos informations personnelles et votre famille en ligne, visitez notre centre de sécurité.

Vos informations

- Certaines fonctionnalités de Windows peuvent vous demander l'autorisation de collecter ou d'utiliser les informations de votre PC, notamment des informations personnelles. Windows utilise ces informations comme indiqué dans la version complète [Déclaration de confidentialité Windows](#), ainsi que dans le [Fonctionnalités supplémentaires](#) et le [Serveur supplémentaire](#).
- Certaines fonctionnalités Windows peuvent, avec votre autorisation, partager des informations personnelles sur Internet.
- Si vous choisissez d'enregistrer votre logiciel, vous devrez fournir des informations personnelles.
- Windows requiert l'activation afin de lutter contre le piratage de logiciels, et pour s'assurer que les clients obtiennent la qualité qu'ils sont en droit d'attendre. L'activation envoie des informations sur votre PC à Microsoft.
- Vous pouvez choisir de vous connecter à Windows avec un [Compte Microsoft](#), qui vous permet de synchroniser les paramètres de Windows et de vous connecter automatiquement aux applications et aux sites Web. Lorsque vous créez un compte Microsoft, vous êtes invité à fournir des informations personnelles.

- [Informations supplémentaires](#)

[Haut de la page](#)

Vos choix.

- Windows propose plusieurs façons de contrôler la façon dont les fonctionnalités de Windows transfèrent des informations sur Internet. Vous trouverez davantage d'informations sur le contrôle de ces fonctionnalités dans le document [Serveur supplémentaire](#).
- Afin d'améliorer votre expérience, certaines fonctionnalités utilisant Internet sont activées par défaut.
- [Informations supplémentaires](#)

[Haut de la page](#)

Utilisations des information

- Nous utilisons les informations collectées pour activer les fonctionnalités que vous utilisez ou fournir les services que vous demandez. Nous les utilisons également pour améliorer nos produits et services. Afin de nous aider à fournir nos services, nous communiquons périodiquement certaines informations à d'autres sociétés qui fonctionnent en notre nom. Seules les sociétés qui ont besoin d'utiliser ces informations dans le cadre de leurs activités sont autorisées à y accéder. Ces sociétés sont tenues de conserver ces informations confidentielles et ne doivent pas les utiliser à d'autres fins.
- [Informations supplémentaires](#)

[Haut de la page](#)

Comment nous contacter

Pour plus d'informations sur nos pratiques relatives à la confidentialité, accédez à la version complète [Déclaration de confidentialité Windows](#). Ou bien, vous pouvez nous écrire en

utilisant notre [formulaire Web](#).

[Haut de la page](#)

Pour plus d'informations sur les pratiques de traitement des données de Microsoft, veuillez consulter la [Déclaration de confidentialité Microsoft](#). Vous découvrirez également les derniers outils que nous proposons pour accéder à et contrôler vos données et comment nous contacter concernant toute demande de confidentialité.

Déclaration de confidentialité de Windows 8 et de Windows Server 2012

Points essentiels **Déclaration** Fonctionnalités supplémentaires Serveur supplémentaire

Sur cette page

Collecte et utilisation de vos informations

Collecte et utilisation des informations concernant votre ordinateur

Sécurité de vos informations

Modification de cette déclaration de confidentialité

Pour plus d'informations

Déclarations de

Cette déclaration aborde Windows 8 et Windows Server 2012 (« Windows »). Certains composants de Windows disposent de leurs propres déclarations de confidentialité, qui sont répertoriées sur le côté droit de cette page. Les déclarations de confidentialité pour les logiciels et les services liés à Windows et aux versions antérieures sont également répertoriées.

Pour plus d'informations sur les fonctionnalités spécifiques, reportez-vous à [Fonctionnalités supplémentaires](#) et [Serveur supplémentaire](#).

Cette déclaration se concentre sur les fonctionnalités qui communiquent avec Internet et n'est pas censée être une liste exhaustive.

Collecte et utilisation de vos informations

Les informations personnelles que nous collectons vous concernant sont utilisées par Microsoft ainsi que ses filiales et

confidentialité supplémentaires

Internet Explorer

Service de rapports
d'erreurs Microsoft

Microsoft Online

Outil de suppression
de logiciels
malveillants Microsoft
Windows

Services de mise à
jour

Windows Media Center

Windows Media Player

Windows 7

sociétés affiliées pour activer les fonctionnalités que vous utilisez, vous fournir les services requis et mener à bien les transactions que vous avez demandées ou autorisées. Elles peuvent également être utilisées pour analyser et améliorer les produits et services Microsoft.

À l'exception des cas cités dans cette déclaration, nous ne divulguons pas vos informations personnelles à des tiers sans votre consentement. Nous faisons parfois appel à d'autres sociétés pour fournir des services limités en notre nom, tels que l'analyse statistique de nos services. Nous fournissons uniquement à ces sociétés les informations personnelles nécessaires pour fournir le service, et il leur est interdit d'utiliser ces informations à d'autres fins.

Microsoft peut éventuellement accéder à des informations vous concernant ou les divulguer, y compris le contenu de vos communications, dans le but de : (a) nous conformer à la loi ou répondre à des demandes émanant des autorités judiciaires ; (b) protéger les droits ou la propriété de Microsoft ou de nos clients, notamment l'application des accords ou politiques qui encadrent votre utilisation du logiciel ; ou (c) si nous pensons, en toute bonne foi, que l'accès à vos informations ou la divulgation de vos informations est indispensable à la protection de la sécurité personnelle des employés et des clients de Microsoft ou du public de façon générale.

Les informations personnelles recueillies par Microsoft ou envoyées à Microsoft par Windows 8 peuvent être stockées et traitées aux États-Unis ou dans tout autre pays dans lequel Microsoft ou ses filiales, branches ou agents gèrent des infrastructures. Microsoft agit dans le cadre des règles libératoires définies par le Département américain du commerce, relatives à la collecte, l'utilisation et la conservation des données provenant de l'Union européenne, de l'Espace économique européen et de la Suisse.

[Haut de la page](#)

Collecte et utilisation des informations concernant votre ordinateur

Lorsque vous utilisez le logiciel avec les 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. Ces informations standard de l'ordinateur comprennent généralement votre adresse IP, les versions de votre système d'exploitation et de votre navigateur ainsi que les paramètres régionaux et de langue. Dans certains cas, elles peuvent également inclure l'ID du matériel (qui indique le fabricant, le nom et la version de l'appareil). Si une fonction ou un service donné envoie des informations à Microsoft, des informations standard relatives à l'ordinateur sont également envoyées.

Les détails de confidentialité pour chaque fonctionnalité Windows 8 de [Fonctionnalités supplémentaires](#) et [Serveur supplémentaire](#), ainsi que les fonctionnalités répertoriées sur le côté de cette page, décrivent les informations supplémentaires collectées et leur utilisation.

Les administrateurs peuvent utiliser la stratégie de groupe pour modifier la plupart des paramètres des fonctionnalités décrites ci-dessous. Pour plus d'informations, consultez la page [ce livre blanc pour les administrateurs](#).

[Haut de la page](#)

Sécurité de vos informations

Microsoft s'engage à protéger la sécurité de vos informations. Nous utilisons diverses technologies et procédures de sécurité pour assurer la protection de vos informations personnelles et éviter qu'elles ne soient consultées, utilisées ou divulguées sans autorisation. Par exemple, nous stockons les informations que vous nous confiez sur des systèmes informatiques à accès limité, situés sur des sites sécurisés. Lorsque nous transmettons des informations hautement confidentielles (par exemple, un numéro de carte de crédit ou un mot de passe) via Internet, nous utilisons une méthode de chiffrement, telle que le protocole Secure Sockets Layer (SSL).

[Haut de la page](#)

Modification de cette déclaration de confidentialité

Nous mettrons occasionnellement à jour cette déclaration de confidentialité en fonction des modifications apportées à nos produits et services et des commentaires de nos clients. Lorsque nous intégrons des modifications, nous changeons la date de dernière mise à jour affichée en haut de cette déclaration. En cas de changement notable apporté à cette déclaration ou à la façon dont Microsoft va utiliser vos données personnelles, nous vous en informons en publiant de façon visible un avis avant d'implémenter la modification, ou en vous envoyant directement une notification. Nous vous conseillons de consulter régulièrement cette déclaration afin d'être informé sur la façon dont Microsoft protège vos données.

[Haut de la page](#)

Pour plus d'informations

Vos commentaires concernant cette déclaration de confidentialité sont les bienvenus. Si vous avez des questions concernant cette déclaration ou que vous estimez que nous ne l'avons pas respectée, contactez-nous à l'aide de notre [formulaire Web](#).

Déclaration de confidentialité Microsoft

Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
États-Unis

[Haut de la page](#)

Pour plus d'informations sur les pratiques de traitement des données de Microsoft, veuillez consulter la [Déclaration de confidentialité Microsoft](#). Vous découvrirez également les derniers outils que nous proposons pour accéder à et contrôler vos données et comment nous contacter concernant toute demande de confidentialité.

Déclaration de confidentialité de Windows 8 et de Windows Server 2012

Points essentiels Déclaration **Fonctionnalités supplémentaires** Serveur supplémentaire

Dans cette page

Dernière mise à jour : octobre 2012

[Activation](#)

Notez que cette page constitue un supplément de la [Windows 8 et](#)

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

[Windows Server 2012](#) (« Déclaration de confidentialité de Windows »), qui comprend quatre sections :

[Management Services\)](#)

- [Points clés](#)

[Audit](#)

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

[Chiffrement de lecteur BitLocker](#)

[Détection et configuration des périphériques](#)

- Supplément relatif aux fonctionnalités (le présent document), décrivant les fonctionnalités qui ont un impact sur les informations personnelles dans Windows 8 et Windows Server 2012

[DirectAccess](#)

[Mise à jour dynamique](#)

- [Supplément sur le serveur](#), qui décrit les fonctionnalités supplémentaires qui ont un impact sur les informations

[Options d'ergonomie](#)

Observateur
d'événements

Contrôle parental

Télécopie

Personnalisation de
l'écriture manuscrite :
apprentissage
automatique

Groupe résidentiel

IME (éditeur de
méthode d'entrée)

Programme
d'amélioration de
l'installation

Impression Internet

Langues

Services de localisation

Nom et avatar du
compte

Reconnaissance du
réseau

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

Commander des
tirages

Assistant Compatibilité
des programmes

Propriétés

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 supplément applicable ou toute déclaration autonome.

Activation

Quel est le rôle de cette fonctionnalité ?

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 aux composants de votre ordinateur ou au logiciel peuvent vous obliger à réactiver le logiciel. Des modifications apportées au matériel ou aux logiciels de votre ordinateur peuvent vous obliger à réactiver Windows.

L'activation peut détecter et désactiver les attaques du mécanisme d'activation (logiciel qui contourne l'activation du logiciel). 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.

Informations collectées, traitées ou transmises

Lors de l'activation, les informations suivantes sont envoyées à Microsoft :

- Le code de produit Microsoft, (composé de cinq chiffres identifiant le produit Windows que vous activez).
- 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 code de site permet de déterminer si le produit a été acheté dans un magasin, reçu sous forme de copie d'évaluation,

Proximité	obtenu dans le cadre d'un programme de licences en volume ou préinstallé par un fabricant de PC.
Connexions d'accès à distance	<ul style="list-style-type: none"> • La date de l'installation et l'installation s'est effectuée correctement.
Connexions aux programmes RemoteApp et aux services Bureau à distance	<ul style="list-style-type: none"> • Des informations aidant à confirmer que la clé de votre produit Windows n'a pas été modifiée. • La marque et le modèle de l'ordinateur.
Connexion Bureau à distance	<ul style="list-style-type: none"> • Des renseignements qui indiquent la version du système d'exploitation et des logiciels.
Se connecter à un compte Microsoft	<ul style="list-style-type: none"> • Les paramètres régionaux et linguistiques.
Synchroniser vos paramètres	<ul style="list-style-type: none"> • Un numéro unique, appelé identificateur global unique (GUID, Globally Unique IDentifier) attribué à votre ordinateur.
Technologie Teredo	<ul style="list-style-type: none"> • La clé du produit (avec hachage) et l'ID du produit.
Services du module de plateforme sécurisée (TPM)	<ul style="list-style-type: none"> • Le nom, le numéro de révision et la date de révision du BIOS. • Le numéro de série du disque dur (avec hachage).
Certificats racine de mise à jour	<ul style="list-style-type: none"> • Le résultat de la vérification de l'activation. Cela inclut les codes d'erreur et les informations suivantes relatives aux attaques du mécanisme d'activation et aux logiciels assimilés à des programmes malveillants ou non autorisés détectés ou désactivés : <ul style="list-style-type: none"> • l'identifiant de l'attaque du mécanisme d'activation ; • l'état de l'attaque, par exemple si elle est nettoyée ou mise en quarantaine ; • l'identification du fabricant de l'ordinateur ; • 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.
Update Services	
Programme d'amélioration de l'expérience utilisateur Windows	
Windows Defender	
Service de rapport d'erreurs Windows	
Association de fichier Windows	
Aide de Windows	<ul style="list-style-type: none"> • Le nom et un hachage du contenu du fichier d'instructions pour

[Assistance à distance](#) 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. Des informations standard sur l'ordinateur sont également envoyées. Néanmoins, l'adresse IP de votre ordinateur n'est conservée que temporairement.

[Windows Search](#)
[Partage Windows](#)
[Windows SmartScreen](#)
[Reconnaissance vocale Windows](#)

Utilisation des informations

[Windows Store](#) 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.

[Service de temps Windows](#)

Choix et contrôle

[Résolution des problèmes Windows](#) 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.

[Haut de la page](#)

Client AD RMS (Active Directory Rights Management Services)

Quel est le rôle de cette fonctionnalité ?

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.

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](#)

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 peuvent ainsi désigner les informations recueillies, la durée de leur stockage et si elles peuvent être transmises à des tiers. 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](#)

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 OneDrive. Pour contribuer à protéger votre confidentialité, 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.

Si vous avez indiqué vouloir sauvegarder votre clé de récupération sur OneDrive, vous pouvez accéder ou supprimer la clé [ici](#).

[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 meilleure 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 commence par vérifier si aucun pilote approprié n'est déjà installé sur l'ordinateur. Dans la négative, Windows contacte le service en ligne Windows Update pour rechercher et télécharger les pilotes du périphérique. 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 des informations ou une application pour le périphérique sont disponibles, Windows les télécharge et les installe à partir du Windows Store. L'application est alors disponible dans votre compte Windows Store, dans la liste des applications que vous avez téléchargées.

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 ces informations pour vous identifier, vous contacter ou vous envoyer des publicités ciblées.

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 pour les nouveaux périphériques** sous Help protect and update your 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 identificateurs 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 identificateurs du matériel que l'opérateur mobile peut utiliser pour identifier votre compte.

Utilisation des informations

Microsoft utilise la partie de votre identificateur 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 identificateurs 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 repris 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.

Jumelage de périphérique 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 jumelage 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](#)

DirectAccess

Quel est le rôle de cette fonctionnalité ?

DirectAccess permet à votre ordinateur de se connecter à distance et de façon continue 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](#)

Mise à jour dynamique

Quel est le rôle de cette fonctionnalité ?

La fonction de mise à jour dynamique permet à Windows de réaliser une vérification unique à travers Windows Update pour obtenir les mises à jour les plus récentes pour votre ordinateur 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, l'on retrouve 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.

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. Pour plus en savoir plus sur les informations collectées par la mise à jour dynamique, consultez la [Déclaration de confidentialité de la fonctionnalité Update Services](#).

Choix et contrôle

Au moment où vous lancez l'installation de Windows, vous êtes invité à vous connecter à Internet pour installer les mises à jour.

[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 (même lorsque je porte des lunettes).
- 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 à 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 de 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 le compte d'un 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 le compte d'un 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 le compte d'un enfant lors de la création du compte, vous pouvez

choisir d'activer le Contrôle parental pour ce compte.

Si l'administrateur configurant le compte d'un 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'une tablette tactile ou d'un stylet. 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 détecter et à améliorer son interprétation de votre style d'écriture manuscrite et de votre vocabulaire, mais aussi d'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 visuel ;
- 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 visuels.

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

Choix et contrôle

La fonction d'apprentissage automatique est activée par défaut. Vous pouvez à tout moment activer ou désactiver l'apprentissage automatique en accédant aux paramètres avancés qui se trouvent dans le Panneau de configuration, sous la rubrique Langues. 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) de tous les comptes Microsoft sur votre ordinateur sont 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, dans Paramètres du PC, par le biais de l'option Groupe résidentiel.

[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.

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

Sauf dans le cas de l'éditeur IME pour le chinois simplifié (dans lequel la fonctionnalité de prédiction est désactivée par défaut), les fonctions 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 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](#)

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 8. 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. Ce GUID nous permet de déterminer quelles données sont envoyées par un même ordinateur au fil du temps. Le GUID ne contient pas d'informations confidentielles et ne sert pas à 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 8.

Choix et contrôle

Vous avez le choix de participer à ce programme au moment où vous installez Windows 8 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.

[Haut de la page](#)

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](#)

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. 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

Sur les ordinateurs fonctionnant avec Windows, les « services de localisation » font référence au logiciel Windows et au service en ligne Microsoft servant à déterminer le lieu approximatif où se trouve votre ordinateur, fournis aux applications ou aux sites Web auxquels vous autorisez l'usage de ces informations. La plateforme

Localisation Windows détermine l'emplacement physique grâce à des matériels spécialisés, par exemple un capteur GPS équipant votre ordinateur, ou par le biais de logiciels, tels que le service de localisation Windows.

Plateforme 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 peuvent demander l'autorisation d'accéder à la localisation de votre ordinateur. En fonction de la configuration de votre système, il se peut que la plateforme 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.

Cette plateforme n'empêche cependant les accès à la localisation de votre ordinateur par le biais d'autres méthodes. Par exemple, vous pouvez installer des périphériques (tel qu'un récepteur GPS) pouvant envoyer des informations de localisation directement à une application et contourner ainsi intégralement la plateforme. Indépendamment de vos paramètres de plateforme de localisation Windows, les services en ligne peuvent utiliser l'adresse IP de votre ordinateur afin de 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 depuis votre ordinateur, mais chaque fournisseur de localisation (par exemple le service de localisation Windows) est en mesure de transférer des informations si vous utilisez des applications de géopositionnement. Les applications autorisées à exploiter la plateforme de localisation pour déterminer votre emplacement peuvent en outre transmettre ou stocker ces informations.

Utilisation des informations

Si vous activez la plateforme de localisation Windows, les applications autorisées sont en mesure de connaître votre localisation 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 tiers, son utilisation de l'emplacement 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 **Activer la plateforme de localisation Windows pour permettre aux applications de demander leur emplacement aux utilisateurs** sous **Partager les informations avec des applications**. La première fois où une application du Windows Store demande la localisation de votre ordinateur, Windows vous demande alors si vous souhaitez l'y autoriser. Vous pouvez déterminer, dans la section Confidentialité des paramètres de l'ordinateur, si des applications peuvent demander votre emplacement, et vous pouvez déterminer, dans la section Autorisations de l'icône Paramètres de l'application, si une application individuelle du Windows Store peut utiliser votre emplacement.

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 toutes les applications dans la section Confidentialité des paramètres du PC. En outre, les administrateurs sont en mesure de désactiver la plateforme de localisation Windows pour tous les utilisateurs dans la section Emplacement du 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 ou celle des réseaux sans fil avoisinants.

Informations collectées, traitées ou transmises

Lorsqu'une application, que vous avez autorisé à accéder à votre localisation, demande votre point géographique, la plateforme de localisation Windows interroge tous les services de localisation installés (y compris le service de localisation Windows) afin de déterminer votre localisation actuelle. Le service de localisation Windows vérifie d'abord s'il dispose d'une liste des points d'accès Wi-Fi 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, que le service de localisation Windows 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 les SSID (nom des points d'accès Wi-Fi) ou réseaux Wi-Fi masqués. À des fins

de confidentialité et de sécurité, les informations relatives aux réseaux Wi-Fi transmises sont chiffrées via SSL.

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, consultez 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 aider à améliorer les services de localisation Microsoft en sélectionnant **Contribuer à l'amélioration des services Microsoft en envoyant des données d'emplacement lors de l'utilisation d'applications de géolocalisation** sous **Envoyer à Microsoft des informations pour contribuer à améliorer Windows et les applications**. 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 pouvez quand même utiliser 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](#)

Nom et avatar du compte

Quel est le rôle de cette fonctionnalité ?

Pour vous proposer du contenu personnalisé, les applications peuvent demander à Windows votre nom et l'image de votre compte. Votre nom et l'avatar de votre compte s'affichent dans les paramètres de l'ordinateur, dans la zone Votre compte de la section Utilisateurs. 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'image de votre compte en sélectionnant **Autoriser les applications à utiliser mon nom et l'image de mon compte** sous **Partager les informations avec des applications**. 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 **Personnaliser** 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 forfait bloqué, 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 fonction 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 elle 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** dans les paramètres de l'ordinateur. 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 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 en arrière-plan pendant que vous ne les utilisez pas, par exemple la synchronisation du courrier électronique.

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 Messagerie 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 via la section Personnaliser des paramètres de l'ordinateur. 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 des paramètres de l'ordinateur.

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 images 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 Windows. 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 renseignements que vous entrez sur le site Web du service d'impression de photographies en ligne sont transmis au service.

Utilisation des informations

Ceux que l'appareil photo stocke dans les fichiers d'images numériques peuvent être employés par le service d'impression de photographies en ligne lors du processus de développement, par exemple, pour adapter la couleur ou la netteté de l'image avant de l'imprimer. 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](#)

Assistant Compatibilité des programmes

Quel est le rôle de cette fonctionnalité ?

Si un problème d'incompatibilité est détecté sur une application 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'erreurs 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 Windows 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 PC 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 doté d'un matériel NFC pour partager liens, fichiers et autres informations. Il existe deux types de connexions de proximité : la Connexion sans fil et la Connexion de proximité. Avec la Connexion sans fil, vous pouvez créer une connexion temporaire ou durable entre des appareils par Wi-Fi, Wi-Fi Direct ou Bluetooth. Avec la Connexion de proximité, 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 adresses réseau Bluetooth et Wi-Fi, ainsi que le nom de votre PC.

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 la désactiver via les options proposées dans Périphériques et imprimantes, accessible à partir du Panneau de configuration.

Connexion de partage

Quel est le rôle de cette fonctionnalité ?

La fonctionnalité Connexion de partage 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 Connexion de partage 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 Connexion de partage 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 Connexion de partage. Aucune information n'est envoyée à Microsoft.

Choix et contrôle

Si le service Proximité en champ proche est activé, la fonctionnalité Connexion de partage l'est également. Pour plus d'informations, voir la section Service de proximité en champ proche.

[Haut de la page](#)

Connexions d'accès à distance

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.

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.

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 **Configurer une nouvelle connexion avec RemoteApp et les connexions du 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 aux services Bureau à distance vous permet d'établir une connexion distante avec un PC 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 PC. 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 l'image 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. Cette liste est stockée de façon permanente, sauf si l'administrateur décide de la supprimer. Aucune information n'est envoyée à Microsoft.

Utilisation des informations

Les informations collectées par la fonctionnalité Connexion Bureau à distance vous permettent de vous connecter à des PC 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 comme informations d'identification 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 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 accédez à la page de connexion de ces sites Web, vous êtes alors également connecté automatiquement aux sites Web qui utilisent des comptes Microsoft pour vos sessions.

Informations collectées, traitées ou transmises

Si vous entrez une adresse de messagerie comme compte Microsoft, lors de la configuration de votre ordinateur ou dans la section Utilisateurs des paramètres de l'ordinateur, 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 renseignements de sécurité peuvent vous être demandés, tels qu'un numéro de téléphone portable, pour vérifier que le compte est bien le vôtre si vous n'arrivez pas à vous y connecter. Si vous ne possédez pas de compte Microsoft, vous pouvez en créer un en utilisant l'adresse de messagerie de votre choix.

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 un compte Microsoft. Pour plus d'informations sur les paramètres qui se synchronisent et comment les contrôler, voir la section Synchroniser vos paramètres.
- Les applications Microsoft qui utilisent un compte Microsoft pour l'authentification (comme Courrier, Calendrier, Photos, Contacts, Messages, OneDrive, 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 OneDrive, vous pouvez vous y connecter automatiquement sans avoir à entrer de nouveau 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 tous les 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 vos paramètres](#).

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](#) qui s'affiche lorsque vous choisissez S'inscrire pour obtenir une nouvelle adresse de messagerie. 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 chacune des applications. La déclaration de confidentialité d'une application Microsoft se trouve dans l'icône Paramètres ou dans la boîte de dialogue À propos de de l'application.

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 vos paramètres. 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. Les déclarations de confidentialité des applications Windows Live (Courrier, Calendrier, Photos, Contacts, Messagerie, OneDrive) sont disponibles à l'adresse go.microsoft.com/fwlink/?LinkId=257483 ; celle de Microsoft Office est disponible à l'adresse go.microsoft.com/fwlink/?LinkId=257484. La déclaration de confidentialité d'une application est également disponible dans l'icône Paramètres ou dans la boîte de dialogue À propos de de l'application.

Vous n'avez pas à vous connecter à Windows à l'aide d'un compte Microsoft. Lorsque vous ajoutez un utilisateur à votre ordinateur, lors de la configuration de ce dernier ou depuis les options **Utilisateurs** des paramètres de l'ordinateur, vous pouvez utiliser un compte local ou un compte Microsoft. Vous pouvez passer d'un compte local à un compte Microsoft à tout moment dans la section **Utilisateurs** des paramètres de l'ordinateur. 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 **Utilisateurs** des paramètres de l'ordinateur.

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](#)

Synchroniser vos 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 ordinateur 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 :

- Langues
- Options d'ergonomie
- 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
- Paramètres pour les applications du Windows Store
- Vérificateur orthographique et dictionnaires IME
- Historique et favoris du navigateur Web
- Mots de passe réseau, d'applications et de sites Web enregistrés

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, y compris votre historique de

navigation, que vous avez choisi de synchroniser avec d'autres ordinateurs via votre compte Microsoft.

Utilisation des informations

Windows 8 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 avec un compte Microsoft, Synchroniser vos paramètres est activé. Vous pouvez choisir de synchroniser vos paramètres et de contrôler quels paramètres sont synchronisés dans la section **Synchroniser vos paramètres** 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 lecteur BitLocker, Carte à puce virtuelle, Démarrage sécurisé, Windows Defender et Stockage de certificats TPM.

Informations collectées, traitées ou transmises

Par défaut, Windows s'approprie 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 8. 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 lecteur BitLocker 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 et le certificat qui l'accompagne permettent 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 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.

Pour plus d'informations sur Windows Update et la protection de vos données personnelles, lisez la [Déclaration de confidentialité de la fonctionnalité Update Services](#).

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 PC.

[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

Si vous choisissez d'obtenir les mises à jour logicielles importantes pour votre PC, 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. Lors d'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 PC. Pour plus d'informations, lisez la [Déclaration de confidentialité de l'outil de suppression de logiciels malveillants Windows](#) .

Pour en savoir plus sur les autres informations collectées par Update Services, voir la [Déclaration de confidentialité de la fonctionnalité Update Services](#).

Utilisation des informations

Ces informations MSRT nous servent à améliorer nos produits et services destinés à lutter contre les programmes malveillants et d'autres problèmes de sécurité. Les informations contenues dans les rapports MSRT ne sont pas utilisées pour vous identifier ou vous contacter.

Pour savoir comment Update Services utilise les autres informations, voir la [Déclaration de confidentialité de la fonctionnalité Update Services](#).

Choix et contrôle

Si vous optez pour la configuration rapide pendant l'installation de Windows, vous activez de fait Update Services et configurez Windows Update pour installer les mises à jour automatiquement. Si vous choisissez de personnaliser les paramètres, vous pouvez contrôler l'activation de la fonctionnalité Update Services dans **Windows Update** sous **Protéger et mettre à jour votre PC**. Une fois Windows installé, vous pouvez modifier les paramètres de la fonctionnalité Update Services dans le Panneau de configuration. Pour plus d'informations, voir la déclaration de confidentialité des Services de mise à jour.

Si vous avez opté pour la recherche et l'installation des mises à jour importantes sur votre PC et que vous recevez l'outil MSRT en même temps que ces mises à jour, vous pouvez désactiver la fonctionnalité de création de rapports du logiciel en suivant [ces instructions](#) sur le site Web de Support Microsoft.

[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 :

- la configuration : notamment le nombre de processeurs dont

est équipé votre PC, le nombre de connexions réseau utilisées, les résolutions d'écran des périphériques d'affichage et la version de Windows en cours d'exécution ;

- 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 les fonctionnalités que vous utilisez le plus souvent, 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. Comme la plupart des utilisateurs décident de participer au CEIP dans les jours qui suivent l'installation de Windows, Microsoft utilise ces informations pour analyser et améliorer l'expérience d'installation de Windows.

Ces informations sont envoyées à Microsoft lorsque vous êtes connecté à Internet. Les rapports du CEIP ne collectent pas intentionnellement d'informations personnelles, telles que le nom, l'adresse et le numéro de téléphone. Toutefois, certains rapports peuvent recueillir involontairement certains éléments d'identification (le numéro de série d'un périphérique connecté à votre PC, par exemple). Microsoft filtre les informations contenues dans les rapports du CEIP pour essayer de supprimer toutes celles qui correspondent à des éléments d'identification personnels.

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. Ce GUID nous permet de déterminer quelles

données sont envoyées par un même ordinateur au fil du temps. Les applications Microsoft sous licence préinstallées avec Windows peuvent créer leurs propres identifiants uniques à utiliser avec le Programme d'amélioration de l'expérience utilisateur, qui peuvent être basés sur les informations de votre compte Microsoft.

En outre, le Programme d'amélioration de l'expérience utilisateur télécharge 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 comprenne 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 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 sont partagées de manière globale et 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, puis d'établir des priorités. Par exemple, le GUID permet à Microsoft de discerner un problème rencontré par un utilisateur une centaine de fois, d'une centaine d'utilisateurs rencontrant le même problème une fois. 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 sous licence avec Windows 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 activer le Programme d'amélioration de l'expérience utilisateur en sélectionnant **Participer au programme d'amélioration de l'expérience utilisateur pour contribuer à l'amélioration des logiciels et services Microsoft** sous **Envoyer à Microsoft des informations pour contribuer à améliorer Windows et les applications**. 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 document en ligne [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

Quel est le rôle de cette fonctionnalité ?

La communauté Microsoft Active Protection Service (MAPS) contre les programmes malveillants regroupe des personnes du monde entier, dont les utilisateurs de Windows Defender. Ce service permet aux utilisateurs de communiquer à Microsoft un rapport retraçant les programmes malveillants et autres formes de logiciels potentiellement indésirables. MAPS peut contribuer à la protection de votre ordinateur en téléchargeant automatiquement de nouvelles signatures pour les programmes malveillants récemment détectés.

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. Celles-ci 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.

Vous pouvez rejoindre MAPS en souscrivant un abonnement de base ou avancé. Si vous décidez d'activer 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 recueillies via des chemins d'accès de fichiers et des vidages de mémoire partiels, par exemple. 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 pour être mises à disposition de tous les utilisateurs à travers Windows Update.

Si vous rejoignez MAPS en souscrivant un abonnement de base ou

avancé :

- Microsoft peut demander un rapport Envoi d'exemples. Ce rapport contient certains fichiers de votre PC qui, selon Microsoft, pourraient être des logiciels potentiellement indésirables. Ce rapport d'exemples est ensuite utilisé pour une analyse détaillée. Vous êtes invité à donner confirmation avant chaque envoi du rapport Envoi d'exemples à Microsoft.
- 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.

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.

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 l'activation de MAPS en sélectionnant **Aider Microsoft à répondre aux applications et programmes malveillants en rejoignant Microsoft Active Protection Service (MAPS)** sous **Envoyer à Microsoft des informations pour contribuer à améliorer Windows et les applications**. Après avoir configuré Windows, vous pouvez modifier votre abonnement ou vos paramètres MAPS, y compris désactiver MAPS, à partir du menu Outils dans Windows Defender.

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 que 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.

[Haut de la page](#)

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 correspond 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 prévenir les problèmes et rendre les logiciels plus fiables, certaines solutions sont également incluses dans les Service Packs et les versions suivantes des logiciels.

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 génération de rapports envoie automatiquement des informations de base sur l'emplacement des problèmes. Certains rapports d'erreurs peuvent recueillir involontairement des informations personnelles. Par exemple, un rapport contenant un instantané de la mémoire de votre PC peut révéler votre nom, une partie du document sur lequel

vous travailliez ou encore des données que vous veniez d'envoyer à un site Web. Si un rapport est susceptible de contenir ce type d'informations, Windows vous demande confirmation avant l'envoi, même si vous avez activé la génération de rapports automatique. Les rapports comprenant des fichiers et des données, peuvent être stockés sur votre PC jusqu'à leur envoi ou leur suppression.

Suite à l'envoi d'un rapport, le service de génération de rapports peut éventuellement vous demander des informations supplémentaires 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 éventuellement vous contacter pour obtenir un complément d'informations et ainsi permettre la résolution du problème que vous avez 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. Ce GUID nous permet de déterminer quelles données sont envoyées par un même ordinateur au fil du temps. Il ne contient aucune information personnelle.

Pour contribuer à protéger votre confidentialité, 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. Le GUID permet de déterminer l'ampleur des problèmes, grâce aux commentaires reçus, puis d'établir des priorités. Par exemple, le GUID permet à Microsoft de discerner un problème rencontré par un utilisateur une centaine de fois, d'une centaine d'utilisateurs rencontrant le même problème une fois.

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 paramètre Rapport d'erreurs Windows en sélectionnant **Utiliser le rapport d'erreurs Windows pour rechercher des solutions** sous **Rechercher en ligne des solutions aux problèmes**. Après avoir configuré Windows, vous pouvez modifier ce paramètre dans la section Centre de maintenance du Panneau de configuration.

Pour plus d'informations, voir le document en ligne [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 Windows en ligne 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 par un même ordinateur 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 recueille pas de façon intentionnelle des informations pouvant servir à vous identifier. 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 du Programme d'amélioration de l'aide, vous pouvez les contrôler en sélectionnant **Contribuer à l'amélioration du contenu de l'aide de Windows en envoyant des informations au programme d'amélioration de l'aide** sous **Envoyer à Microsoft des informations pour contribuer à améliorer Windows et les applications**. 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 ?

La fonctionnalité Windows Search offre un point d'entrée rapide et cohérent pour effectuer une recherche dans des applications, des paramètres, des fichiers ou du contenu d'applications.

Informations collectées, traitées ou transmises

Lorsque vous utilisez la fonctionnalité Windows Search, les caractères que vous tapez dans le champ de recherche (à mesure que vous les tapez) et la requête de recherche finale que vous soumettez sont transmis uniquement à Windows et à toute application faisant l'objet de la recherche, de sorte que Windows ou cette application puisse faire des suggestions de recherche et présenter des résultats de recherche. Windows stocke les requêtes de recherche et des données indiquant votre fréquence de recherche dans les applications.

Utilisation des informations

Windows utilise les précédentes recherches stockées pour faire des suggestions de recherche dans le volet de recherche. Les informations stockées à propos de la fréquence de vos recherches dans les applications sont utilisées pour trier la liste des applications pouvant faire l'objet de recherches dans le volet de recherche par ordre de fréquence. Si vous effectuez une recherche dans une application tierce, l'utilisation des informations recueillies est soumise à la politique de confidentialité de l'éditeur tiers. 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

Windows stocke ces informations par défaut. Vous pouvez désactiver le stockage de ces informations ou supprimer toutes vos anciennes recherches stockées dans la section Recherche des paramètres de l'ordinateur.

[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 Recherche des paramètres de l'ordinateur.

[Haut de la page](#)

Windows SmartScreen

Quel est le rôle de cette fonctionnalité ?

Windows SmartScreen vérifie les fichiers et les applications auprès de Microsoft avant qu'ils soient ouverts ou exécutés pour vous prémunir contre les fichiers et les applications potentiellement dangereux et ainsi préserver l'intégrité de votre ordinateur. Si une application ou un fichier inconnu ou potentiellement dangereux est détecté, Windows vous demande ce que vous voulez faire avant de l'ouvrir.

Informations collectées, traitées ou transmises

Si vous décidez d'utiliser cette fonctionnalité, des informations sur certaines applications que vous utilisez et sur certains fichiers que vous téléchargez sur Internet sont transmises à Microsoft. Outre les informations standard sur le PC et le numéro de version du filtre Windows SmartScreen, ces informations peuvent inclure un nom de fichier, un identificateur de fichier (« hachage »), ainsi que des informations de certificat numérique. Pour préserver la confidentialité de vos informations, les informations transmises à Microsoft sont chiffrées via SSL.

Windows SmartScreen génère de façon aléatoire un numéro appelé GUID (Globally Unique IDentifier, identificateur global unique), qui est envoyé à Microsoft en même temps que les données concernant votre utilisation de SmartScreen. Ce GUID nous permet de déterminer quelles données sont envoyées par un même ordinateur au fil du temps. Il ne contient aucune information personnelle.

Utilisation des informations

Microsoft utilise les informations décrites ci-dessus pour vous avertir du caractère potentiellement dangereux de certains fichiers et applications. De même, nous utilisons ces informations pour analyser les performances de la fonctionnalité et pour améliorer la qualité de

nos produits et services. Le GUID permet de déterminer l'ampleur des problèmes, grâce aux commentaires reçus, puis d'établir des priorités. Par exemple, le GUID permet à Microsoft de discerner un problème rencontré par un utilisateur une centaine de fois, d'une centaine d'utilisateurs rencontrant le même problème une fois.

Microsoft n'utilise pas ces informations pour vous identifier, vous contacter ou 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 l'activation de Windows SmartScreen en sélectionnant **Utiliser le filtre Windows SmartScreen pour vérifier les fichiers et les applications auprès de Microsoft** sous **Protéger votre vie privée et votre PC**. Après avoir configuré Windows, vous pouvez modifier ce paramètre dans la section Centre de maintenance du Panneau de configuration.

[Haut de la page](#)

Reconnaissance vocale 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 (avec 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, 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 Windows Store, 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.

Le Windows Store recherche automatiquement des mises à jour pour vos applications et peut vous avertir lorsque de nouvelles mises à jour sont disponibles. Pour rechercher des mises à jour, le Windows Store envoie les informations suivantes à Microsoft :

- Liste des applications du Windows Store installées par tous les utilisateurs sur votre PC.
- Informations de licence pour chaque application, y compris le propriétaire de chaque licence.
- Paramètres de configuration de Windows Update et/ou

Microsoft Update, notamment si vous souhaitez ou non que les mises à jour soient automatiquement téléchargées ou installées.

- Réussites, échecs et erreurs que vous rencontrez lors de la mise à jour des applications du Windows Store.
- 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.
- Nom, numéro de révision et date de révision du BIOS : informations sur le jeu de 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.

Lorsque vous parcourez le Windows 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. Ces données d'activité ne sont en aucun cas utilisées dans le but de vous identifier ou de vous contacter.

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 d'application du Windows Store indique le nombre de mises à jour disponibles. Vous pouvez alors afficher la liste des mises à jour disponibles et sélectionner celle ou 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.

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.

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 cela, ouvrez l'application, appuyez ou cliquez sur l'icône Paramètres, puis sélectionnez **Autorisations**.

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, nous sommes susceptibles 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 quelles données sont envoyées au fil du temps à partir d'un ordinateur particulier. Le GUID ne contient pas d'informations personnelles et il n'est pas utilisé pour vous identifier.

Pour préserver la confidentialité de vos informations, 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 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 **Contribuer à l'amélioration du Windows Store en envoyant des URL relatives au contenu Web utilisé par les applications** sous **Envoyer à Microsoft des informations pour contribuer à améliorer Windows et les applications**. Une fois l'installation terminée, vous pouvez modifier ce paramètre dans la section Confidentialité des paramètres de l'ordinateur.

[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 du PC local.

Choix et contrôle

Le service de temps Windows est activé par défaut. Vous pouvez désactiver cette fonctionnalité ou choisir votre source de temps de prédilection en accédant à Date et heure dans le Panneau de configuration, en sélectionnant l'onglet Temps Internet, puis en cliquant sur **Modifier les paramètres**. Le fait de désactiver le service de temps Windows n'a aucun effet direct sur les applications ou d'autres services, mais l'horloge du PC local, dépourvue de source de temps fiable, peut se désynchroniser des autres PC sur le réseau ou Internet. En cas de différence de temps importante entre les PC 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 PC.

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

Si vous sélectionnez la configuration rapide lors de l'installation de Windows, la fonctionnalité Résolution des problèmes Windows recherche par défaut des packs de résolution des problèmes en ligne. Pour modifier ces paramètres, accédez à Dépannage dans le Panneau de configuration. Cliquez sur **Afficher l'historique**, sélectionnez un résultat, puis cliquez sur **Supprimer**.

[Haut de la page](#)

Pour plus d'informations sur les pratiques de traitement des données de Microsoft, veuillez consulter la [Déclaration de confidentialité Microsoft](#). Vous découvrirez également les derniers outils que nous proposons pour accéder à et contrôler vos données et comment nous contacter concernant toute demande de confidentialité.

Déclaration de confidentialité de Windows 8 et de Windows Server 2012

Points essentiels Déclaration Fonctionnalités supplémentaires **Serveur supplémentaire**

Sur cette page Dernière mise à jour : **Août 2012**

Journalisation des accès utilisateur (UAL) Cette page est un complément au [Déclaration de confidentialité de Windows 8 et de Windows Server 2012](#) (« Déclaration confidentialité de Windows ») La déclaration de confidentialité comprend quatre sections :

Gestionnaire de serveur

- [Points essentiels](#)

Services de fédération Active Directory (AD FS)

- Déclaration, le [Déclaration de confidentialité complète de Windows](#) qui comprend des liens vers les fonctionnalités Windows disposant de déclaration autonomes

Gestion des adresses IP

- [Fonctionnalités supplémentaires](#), qui décrit les fonctionnalités ayant un impact sur la confidentialité dans Windows 8 et Windows Server 2012

Accès à distance unifié

Services Bureau à distance

- Supplément du serveur (le présent document), qui décrit les fonctionnalités supplémentaires ayant un impact sur la confidentialité dans Windows Server 2012

Programme d'amélioration du produit Windows et Rapport d'erreurs Windows

Pour comprendre la collecte de données et les bonnes pratiques relevant d'une fonctionnalité ou d'un service particulier de Windows, vous devez lire la déclaration de confidentialité de Windows dans son intégralité ainsi que tout supplément applicable. En outre, vous devez lire [ce livre blanc pour les administrateurs](#).

Journalisation des accès utilisateur (UAL)

Rôle de la fonction

La Journalisation des accès utilisateur (UAL) collecte et rassemble les enregistrements de demandes client de rôles de serveur (demandes utilisateur et périphérique) et des produits installés (si ces derniers sont inscrits dans la journalisation des accès utilisateur) sur le serveur local. Ces données, qui se présentent 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 ESE (Extensible Storage Engine) et sont uniquement accessibles aux administrateurs. La journalisation des accès utilisateur est dotée d'un fournisseur WMIv2 et des applets de commande Windows PowerShell associées pour récupérer les données d'accès utilisateur prévues pour une gestion client hors ligne des droits de licence CAL, dans le cadre de laquelle il est essentiel de consigner les demandes client uniques.

Informations collectées, traitées ou transmises

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

Utilisation des informations

Les données de journalisation des accès utilisateur sont accessibles aux administrateurs par le biais de bases de données ESE locales, du fournisseur WMI et des applets de commande Windows PowerShell. Windows n'utilise pas ces données en dehors de la fonctionnalité de journalisation des accès utilisateur elle-même.

Choix et contrôle

La fonction UAL est activée par défaut. Elle peut être interrompue et redémarrée pendant que le serveur est en cours d'exécution. Pour désactiver la fonctionnalité UAL définitivement, ouvrez Windows PowerShell, tapez Disable-UAL et redémarrez le serveur. Un administrateur peut supprimer toutes les données historiques collectées, en commençant par interrompre le service, puis en désactivant UAL et en supprimant tous les fichiers du dossier %SystemRoot%\System32\LogFiles\SUM\.

[Haut de la page](#)

Gestionnaire de serveur

Rôle de la fonction

Le Gestionnaire de serveur est un outil de gestion qui permet à un administrateur de surveiller un ou plusieurs serveurs, et de consulter l'état général ou celui spécifique à un rôle, afin de réaliser 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 à partir d'un serveur géré par l'administrateur :

- **Informations générales du serveur** : Le nom NetBios et le nom de domaine complet (FQDN), les informations d'identification de compte saisies dans la fonctionnalité « Gérer en tant que », l'adresse IPv4, l'adresse IPv6, l'état de facilité de gestion, la description, la version du système d'exploitation, le type, la dernière mise à jour, les processeurs, la mémoire, le nom du cluster, le type d'objet cluster, l'état d'activation, la référence (SKU), l'architecture du système d'exploitation, le fabricant, la configuration du programme d'amélioration du produit et la configuration de la création de rapports d'erreurs Windows (WER).
- **Événements** : ID de gravité, source, journal, date et heure de chaque événement depuis Windows et d'autres journaux

choisis par l'administrateur.

- **Tous les services** : nom, état et type de démarrage.
- **Informations sur les rôles serveur** : Résultats de Best Practice Analyzer (BPA) pour les rôles installés sur le serveur.
- **Informations sur les performances** : exemples pour les compteurs de performance 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 analyser les systèmes.

Choix et contrôle

Un administrateur peut accepter ou refuser la collecte de données à partir de n'importe quel serveur, à l'exception du serveur local, en ajoutant ou en supprimant le serveur dans la section Gestionnaire de serveur. Un administrateur peut fournir explicitement des informations d'identification pour se connecter à un serveur distant. Le Gestionnaire de serveur demande à l'administrateur d'accepter explicitement l'enregistrement des informations d'identification localement dans le Gestionnaire de serveur. Ce dernier peut supprimer ces informations à tout moment.

[Haut de la page](#)

Services de fédération Active Directory (AD FS)

Rôle de la fonction

Active Directory Federation Services (ADFS) est une fédération de classe professionnelle et une solution d'authentification unique pour les applications locales ou connectées au réseau. AD FS permet aux administrateurs d'activer les utilisateurs pour collaborer entre les organisations, et d'accéder aisément aux applications connectées aux réseaux locaux ou autres, tout en assurant la sécurité des applications. AD FS utilise un service de jeton de sécurité qui s'appuie sur Active Directory Domain Services (AD DS) pour

authentifier les utilisateurs et leur émettre des jetons de sécurité à l'aide de différents protocoles. Le jeton est signé numériquement et contient les revendications relatives à l'utilisateur, qui proviennent de chacun des services AD DS ou d'une combinaison de plusieurs d'entre eux, du protocole LDAP, du serveur SQL ou d'un magasin personnalisé.

Informations collectées, traitées ou transmises

Les informations d'identification d'un utilisateur sont collectées lorsque ce dernier s'authentifie avec AD FS. Les informations d'identification sont immédiatement envoyées à Active Directory Domain Services en vue de l'authentification et AD FS ne les stocke pas localement. Les attributs de l'utilisateur dans Active Directory Domain Services peuvent servir à générer des revendications sortantes, selon les règles de revendication configurées par un administrateur AD FS. Les revendications sortantes seront envoyées aux partenaires approuvés, avec lesquels un administrateur AD FS aura 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 destinées à être utilisées par le client uniquement.

Choix et contrôle

Utilisez AD FS pour collecter ou envoyer des données à des partenaires approuvés.

[Haut de la page](#)

Gestion des adresses IP

Rôle de la fonction

La fonction Gestion des adresses IP (IPAM) permet aux administrateurs de serveur d'établir le suivi de l'adresse IP, du nom d'hôte et de l'identificateur de client (par exemple, l'adresse MAC dans IPv4 et DUID dans IPv6) des ordinateurs ou des périphériques connectés à un réseau avec les informations d'ouverture de session de l'utilisateur.

Informations collectées, traitées ou transmises

Le serveur IPAM collecte des journaux d'audit et des événements auprès des serveurs DHCP, des contrôleurs de domaine et des serveurs de stratégie réseau et stocke localement l'adresse IP, le nom d'hôte, l'identificateur de client et le nom d'utilisateur de l'utilisateur connecté. Un administrateur de serveur peut rechercher les fichiers journaux collectés en fonction de l'adresse IP, de l'identificateur de client, du nom d'hôte et du nom d'utilisateur, à l'aide de la console IPAM. Aucune de ces informations n'est envoyée à Microsoft.

Utilisation des informations

Microsoft n'a pas accès à ces informations. Ces informations sont destinées à être utilisées par le client uniquement.

Choix et contrôle

IPAM n'est pas installé par défaut et doit être installé par l'administrateur du serveur. Une fois la fonction IPAM installée, l'audit de l'adresse IP sera automatiquement activé. Pour désactiver l'audit de l'adresse IP sur un serveur où la fonction IPAM est installée, lancez le Planificateur de tâches sur le serveur IPAM, accédez à la tâche d'Audit sous Microsoft\Windows\IPAM, puis désactivez-la.

[Haut de la page](#)

Accès à distance unifié

Rôle de la fonction

L'accès distant unifié permet aux utilisateurs distants de se connecter à un réseau privé, tel qu'un réseau d'entreprise, via Internet. L'accès à distance unifié utilise DirectAccess pour assurer une connectivité continue et transparente entre des ordinateurs clients distants exécutant Windows 8 et les réseaux d'entreprise. Il fournit également une fonctionnalité de Service d'accès à distance (RAS), qui sont des services VPN classiques, comprenant notamment une connectivité locale de site à site ou à d'autres réseaux.

Informations collectées, traitées ou

transmises

Afin de garantir un suivi des utilisateurs distants unifié, le serveur DirectAccess stocke les détails sur les utilisateurs distants qui se connectent à un réseau privé. Cela inclut des informations telles que le nom d'hôte de l'utilisateur distant, le nom d'utilisateur Active Directory et une adresse IP publique du client distant (si le client utilise une traduction d'adresses réseau (NAT), il s'agira de l'adresse IP publique). Ces données peuvent également être stockées dans la base de données interne Windows (WID) ou dans des serveurs RADIUS, mais uniquement avec le consentement de l'administrateur. Seul un administrateur DirectAccess (un utilisateur de domaine doté d'un compte d'administrateur local) accédant à un serveur peut accéder et afficher ces informations.

Utilisation des informations

Ces informations seront utilisées par l'administrateur pour la résolution des problèmes de connectivité du client et également à des fins d'audit ou de conformité. Aucune information n'est envoyée à Microsoft.

Choix et contrôle

L'analyse du client à distance est activée par défaut et ne peut pas être désactivée. Les données d'analyse sont stockées dans les serveurs WID/RADIUS uniquement si un administrateur a configuré la gestion des comptes de sorte à ce que l'une de ces options soit utilisée. Si aucun administrateur n'a configuré cette gestion des comptes, aucune de ces informations ne sera stockée. Un administrateur peut également configurer la gestion des comptes sur un serveur d'accès à distance de sorte à ne pas stocker de noms d'utilisateur et d'adresses IP.

[Haut de la page](#)

Services Bureau à distance

Rôle de la fonction

Les Services Bureau à distance (RDS) fournissent une plateforme afin d'aider les entreprises à mettre en place une stratégie de bureau centralisée, à gérer les postes de travail et les applications et à améliorer la flexibilité et la conformité tout en renforçant la sécurité

des données.

Informations collectées, traitées ou transmises

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

Utilisation des informations

Ces informations seront utilisées par l'administrateur pour la résolution des problèmes de connectivité du client et également à des fins d'audit interne ou de conformité. Aucune information n'est envoyée à Microsoft.

Choix et contrôle

L'analyse du client est activée par défaut et ne peut pas être désactivée. Les informations d'analyses sont stockées dans le WID ou le serveur SQL.

[Haut de la page](#)

Programme d'amélioration du produit Windows et Rapport d'erreurs Windows

Rôle de la fonction

Pour plus d'informations sur ces composants, consultez l'onglet [Fonctionnalités supplémentaires](#) ou [ce livre blanc pour les administrateurs](#).

Informations collectées, traitées ou transmises

Pour en savoir plus sur les informations spécifiques collectées,

traitées et transmises via ces fonctionnalités, consultez les sections Programme d'amélioration du produit et Rapport d'erreurs Windows de l'onglet [Fonctionnalités supplémentaires](#) .

Utilisation des informations

Pour en savoir plus sur la manière dont nous utilisons les informations collectées par ces fonctionnalités, consultez les sections Programme d'amélioration du produit et Rapport d'erreurs Windows de l'onglet [Fonctionnalités supplémentaires](#) .

Choix et contrôle

Par défaut, le programme d'amélioration du produit et le rapport d'erreurs Windows vous demandent votre confirmation avant d'envoyer des rapports d'incident à Microsoft. Vous pouvez activer et désactiver le programme d'amélioration du produit depuis le Gestionnaire de serveur et le panneau de configuration, et à l'aide des méthodes de contrôle des lignes de commande. Le rapport d'erreurs Windows peut uniquement être contrôlé à l'aide des méthodes de ligne de commande.

Pour activer ou désactiver le programme d'amélioration du produit à l'aide du panneau de configuration, cliquez sur **Système et maintenance**, puis sur **Rapports et solutions aux problèmes**. Puis, dans le volet gauche, sous Voir aussi, cliquez sur **Paramètres d'amélioration de l'expérience utilisateur** pour activer ou désactiver le programme d'amélioration du produit.

Contrôles du Gestionnaire de serveur

Serveur local

- Activer le Programme d'amélioration du produit
Ouvrez le Gestionnaire de serveur et sélectionnez **Serveur local**. Cliquez sur le lien du 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 le rapport d'erreurs Windows
Ouvrez le Gestionnaire de serveur et sélectionnez **Serveur local**. Cliquez sur le lien du programme d'amélioration de l'expérience utilisateur et sélectionnez **Non, je ne souhaite**

pas y participer dans la boîte de dialogue, puis cliquez sur **OK**.

- Activer le rapport d'erreurs Windows
Ouvrez le Gestionnaire de serveur et sélectionnez **Serveur local**. Cliquez sur le lien de rapport d'erreurs Windows, sélectionnez **Oui, envoyer automatiquement des rapports de synthèse**, puis sur **OK**.
- Désactiver le rapport d'erreurs Windows
Ouvrez le Gestionnaire de serveur et sélectionnez **Serveur local**. Cliquez sur le lien de rapport d'erreurs Windows, sélectionnez **sélectionnez Je ne souhaite pas participer. Ne plus me demander**, puis sur **OK**.

Ordinateurs multiples

- Activer le Programme d'amélioration du produit
Ouvrez le Gestionnaire de serveur et sélectionnez **Tous les serveurs**. Dans la vignette Serveurs, sélectionnez tous les serveurs (Ctrl + A), faites un clic droit et sélectionnez **Configurer le signalement de problèmes automatique Windows**. Sur l'onglet du programme d'amélioration de l'expérience utilisateur, sélectionnez **Oui, je souhaite y participer (recommandé)**. Appliquez ce paramètre à tous les serveurs en cochant la case en regard de Nom du serveur dans la commande Sélectionner des serveurs, puis cliquez sur **OK**.
- Désactiver le rapport d'erreurs Windows
Ouvrez le Gestionnaire de serveur et sélectionnez Tous les serveurs. Dans la vignette Serveurs, sélectionnez tous les serveurs (Ctrl + A), faites un clic droit et sélectionnez **Configurer le signalement de problèmes automatique Windows**. Sur l'onglet du programme d'amélioration de l'expérience utilisateur, sélectionnez **Non, je ne souhaite pas y participer**. Appliquez ce paramètre à tous les serveurs en cochant la case en regard de Nom du serveur dans la commande Sélectionner des serveurs, puis cliquez sur **OK**.
- Activer le rapport d'erreurs Windows
Ouvrez le Gestionnaire de serveur et sélectionnez **Tous les**

serveurs. Dans la vignette Serveurs, sélectionnez tous les serveurs (Ctrl + A), faites un clic droit et sélectionnez **Configurer le signalement de problèmes automatique Windows** . Sous l'onglet Rapport d'erreurs Windows, sélectionnez **Oui, envoyer automatiquement des rapports de synthèse (recommandé)**. Appliquez ce paramètre à tous les serveurs en cochant la case en regard de Nom du serveur dans la commande Sélectionner des serveurs, puis cliquez sur **OK**.

- Désactiver le rapport d'erreurs Windows
Ouvrez le Gestionnaire de serveur et sélectionnez **Tous les serveurs**. Dans la vignette Serveurs, sélectionnez tous les serveurs (Ctrl + A), faites un clic droit et sélectionnez **Configurer le signalement de problèmes automatique Windows** . Sous l'onglet Rapport d'erreurs Windows, sélectionnez **Non, je ne souhaite pas y participer**. Appliquez ce paramètre à tous les serveurs en cochant la case en regard de Nom du serveur dans la commande Sélectionner des serveurs, puis cliquez sur **OK**.

[Haut de la page](#)