ivanti

# Cinq raisons pour lesquelles la gestion de l'espace de travail utilisateur est désormais indispensable sous Windows 10

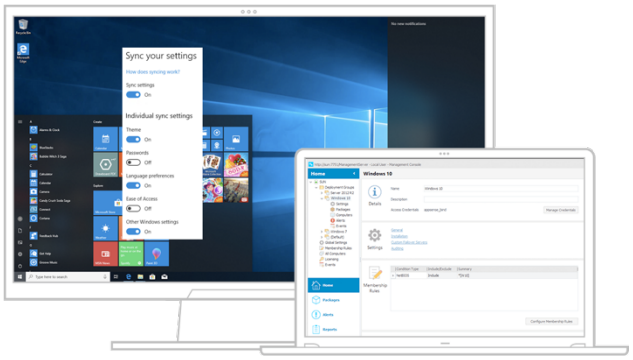
**Au fur et à mesure que de nouvelles fonctions sont ajoutées à Windows 10, il faut se poser la question : avez-vous toujours besoin de solutions tierces pour améliorer l'expérience utilisateur et protéger vos postes clients ? Vous devez considérer les 5 points suivants :**

## 1. La personnalisation est-elle gratuite ?

Windows 10 comporte la fonction intégrée « Synchroniser vos paramètres », qui semble à première vue inclure des options « intégrées » de personnalisation. Son objectif est que, lorsqu'un utilisateur passe d'un ordinateur à un autre, ses paramètres liés au poste de travail et aux applications le suivent. Cela permet un contrôle de base des paramètres qui suivent l'utilisateur.

C'est une excellente fonction pour le grand public, parce que ces paramètres sont synchronisés dans le Cloud Microsoft à l'aide de votre compte Microsoft. Chaque fois que vous vous connectez à Windows 10 sur un nouveau périphérique à l'aide de ce compte Microsoft, un grand nombre de vos paramètres sont automatiquement synchronisés. En entreprise, cependant, c'est un peu plus complexe. Si vous utilisez uniquement Active Directory sur site, vous pouvez fédérer et synchroniser un compte Microsoft via ADFS et utiliser « Synchroniser vos paramètres ». Cette option est désactivée si vous utilisez Azure AD, et vous devez utiliser la fonction Enterprise State Roaming, qui est très semblable mais stocke les paramètres avec votre compte d'entreprise dans Azure AD. Tout cela pose des problèmes au département IT.

D'abord, si vous utilisez AD sur site et synchronisez les données sur un compte Microsoft pour chaque utilisateur, des infos sensibles (comme les mots de passe) sont stockées hors de votre contrôle. Cela peut avoir des conséquences sur la sécurité, la confidentialité et le respect des réglementations, surtout avec la mise en place du RGPD. Si un utilisateur quitte l'entreprise, il conserve son compte Microsoft. Ce problème n'existe pas avec Enterprise State Roaming, mais vous devez pour cela posséder un abonnement Azure AD Premium, qui coûte plus cher.




Deuxièmement, la synchronisation sur un compte Microsoft et Enterprise State Roaming s'appliquent uniquement à un type rare d'applis UWP (Plateforme Windows universelle), également appelées applications modernes, aux applications Windows Store, Metro et même WinRT. Elles sont intégrées en nombre croissant dans Windows 10 (Edge, Calculatrice, Pense-bêtes et même le menu Démarrer) mais 99 % des applications utilisées dans l'entreprise reposent sur l'API Win32, et « Synchroniser vos paramètres » ne s'applique pas à ces applications.

Troisièmement, même pour les applications UWP, cette fonction exige que le développeur de l'application ait choisi de stocker les paramètres dans le Cloud Microsoft avec cette méthode. Et si le paramétrage voulu n'est pas inclus, il est impossible de l'ajouter sans solution tierce.

Office 365 comporte une fonction distincte d'itinérance des paramètres, qui capture certains paramètres Office dans le Cloud Microsoft. Cependant, la documentation est limitée et n'a pas été mise à jour pour Office 2016. De même que la fonction Windows 10 « Synchroniser vos paramètres », elle exige l'utilisation d'un compte Microsoft ou Azure AD, et vous n'avez aucun contrôle sur le choix des paramètres stockés. De plus, il n'y a aucune fonction d'annulation (rollback) ni d'archivage. Cela peut aussi s'appliquer à toutes les autres applications Win32.

C'est là qu'une solution tierce s'avère plus précieuse que jamais : elle permet une couverture totale et flexible de tous les paramètres de poste de travail et d'applications Windows, avec un contrôle total de l'IT tout en garantissant la confidentialité des données.

## 2. Sécurité sur le poste client

Windows 10 est la version de Windows la plus sécurisée jamais créée, et les technologies comme Device Guard (avec les fonctions, Windows Defender, Contrôle d'application, Configurable Code Integrity et Sécurité basée sur la virtualisation) et Credential Guard constituent de nouvelles barrières pour vous protéger des attaques traditionnelles. Ces deux technologies sont en fait des séries de technologies et vous pouvez, dans la situation la plus extrême, utiliser Device Guard pour convertir votre PC en un périphérique semblable à un téléphone ou une tablette de type Apple/Android, capable uniquement d'exécuter les applications provenant de Windows Store ou celles explicitement autorisées par le département IT. Ce dernier doit pour cela créer des signatures pour ces applications (et d'ailleurs, les recréer à chaque changement de l'application). Autrement dit, la version complète de Device Guard est une forme extrême de contrôle de l'exécution des applications, qui interdit l'exécution des exécutables indésirables. Mais elle rend aussi extrêmement difficile la gestion de votre parc existant d'applications métier et exige beaucoup de travail de la part du département IT chaque fois que l'une de ces applications change.

L'autre approche recommandée par Microsoft consiste à convertir les applications Win32 existantes en applications UWP (avec Pont du bureau), afin que les applications s'exécutent sans privilèges Administrateur, et puissent être encapsulées et protégées. Malheureusement, le processus de conversion n'est pas très simple et il nécessite presque toujours des changements de code dans l'application Win32, ce qui est impossible dans les applications les plus anciennes ou provenant de fournisseurs externes. Device Guard est depuis devenu plutôt une appellation marketing qui couvre différentes technologies, sous la marque Windows Defender.

Credential Guard sécurise le sous-système Windows LSA (Autorité de sécurité locale) pour en faire une machine virtuelle Hyper-V protégée par le matériel. Bien entendu, cela implique des besoins en matériel très exigeants, et peut empêcher les applications tierces qui interagissent avec LSA de fonctionner tant qu'elles n'ont pas été mises à jour pour Windows 10. Mais c'est une fonction de sécurité utile et elle bloque de nombreux vecteurs d'attaque.

Les fournisseurs tiers offrent toujours des fonctions beaucoup plus simples de gestion des problèmes comme l'élévation des privilèges utilisateur et le contrôle par l'administrateur local, l'accès réseau des navigateurs et des applications, ainsi qu'un contrôle plus flexible de l'exécution des applications à l'aide de métadonnées de fichier et autres fonctions de mise en correspondance de motifs. Ainsi, le département IT n'a pas de travail supplémentaire chaque fois qu'une application connaît une mise à jour mineure. Les fonctions Windows 10 citées plus haut ne rendent pas ces solutions moins précieuses.

## 3. Stockage des données

OneDrive est fantastique pour le grand public, et Windows 10 et Office 365 passent facilement à de nouveaux niveaux d'intégration avec OneDrive. OneDrive Entreprise donne au département IT davantage de contrôle sur les fichiers et dossiers utilisateur synchronisés dans le Cloud Microsoft, mais de nombreuses entreprises exigent que les données utilisateur soient conservées sur leurs propres périphériques et dans leur propre centre de données. Lorsque le stockage sur site est nécessaire et que la fonction Dossiers en mode hors connexion ne suffit pas, les solutions tierces permettent une synchronisation sélective, un contrôle détaillé des types de fichier et des transferts à l'arrière-plan, un audit complet de la distribution de fichiers et les mêmes avantages d'accès interplateforme que OneDrive.

Lorsque le stockage des fichiers utilisateur dans le Cloud est acceptable pour l'entreprise, Office 365 fournit 1 To de stockage pour chaque utilisateur, mais ce stockage est géré hors de la visibilité du département IT. Le département IT ne dispose d'aucune méthode facile pour l'audit de l'accès aux fichiers, pour la définition d'une stratégie concernant les types de fichier synchronisés et stockés, ou pour le contrôle des accès à un stockage mixte sur site et dans le Cloud. Là encore, c'est un domaine où un fournisseur tiers peut vous procurer une expérience utilisateur transparente, en exploitant le stockage Office 365 de 1 To par utilisateur tout en laissant le contrôle complet au département IT.

## 4. Migration et itinérance entre Windows 7 et 10, et entre Windows Server 2008 et 2016

La plupart des entreprises ont sauté Windows 8 et 8.1. Et, en raison de l'expérience de poste de travail de type Windows 8, un grand nombre ont aussi sauté 2012 et 2012 R2 pour les déploiements RDSH/XenApp/Terminal Server. Comme la prise en charge de Windows 7 prend fin en 2020, on constate enfin une accélération de l'adoption de Windows 10 dans l'entreprise. En outre, les utilisateurs recherchent l'expérience Windows 10 sur les postes de travail virtuels et sessions qu'ils partagent, si bien que vous devez passer à Windows Server 2016 (souvent en conjonction avec la mise à niveau vers Citrix XenApp).

Ceci étant dit, plus de 30 % des postes de travail d'entreprise fonctionnent toujours sous Windows 7, ce qui signifie que les utilisateurs vont faire des allers-retours entre la version 2 (Windows 7) et la version 5 (premières versions de Windows 10 et 2016), et la version 6 (versions plus récentes de Windows 10 et 2016) de leurs profils, sans parler des architectures d'UC x86 et x64. La fonction d'itinérance de profils prête à l'emploi de Windows n'en est tout simplement pas capable. Sans outil tiers capable de gérer l'itinérance entre les différentes versions des profils, l'expérience des utilisateurs n'est pas de bonne qualité.

## 5. Comment suivre l'adoption ?

Êtes-vous capable de citer les personnes de votre domaine qui utilisent Windows 10 ? Vous connaissez déjà les périphériques gérés où vous l'avez volontairement déployé, mais qu'en est-il des périphériques en BYOD et en COPE que les gens ont apportés sur le réseau ? Les outils Active Directory peuvent parfois vous aider, mais la découverte sans agent des éléments présents sur le réseau reste du domaine des fournisseurs tiers. Évidemment, Ivanti propose toute une gamme d'outils permettant non seulement le suivi des périphériques fonctionnant sous Windows 10, mais également de la version de la licence, du Build et du type de périphérique utilisés. Ces outils peuvent aussi générer des tableaux de bord interactifs, des alertes et des rapports au fur et à mesure de la progression de votre projet de migration. Consultez le site Web Ivanti pour en savoir plus sur les solutions de migration vers Windows 10.

## Récapitulatif

Windows 10 offre de nombreuses fonctions et améliorations très utiles. Cependant, dans une entreprise (quelle que soit sa taille) où le département IT veut contrôler et protéger la sécurité et l'expérience des utilisateurs, les solutions tierces sont indispensables pour :

1. L'itinérance et la récupération des paramètres liés au poste de travail et aux applications
2. Le contrôle des applications et une sécurité par moindres privilèges
3. La synchronisation et la découverte des données
4. L'itinérance entre Windows 10/2016 et les versions plus anciennes de Windows
5. Le suivi de l'adoption et de la propagation de Windows 10

**En savoir plus**

**ivanti.com/contact**