Manuel de l'administrateur

HP ThinPro 7,1

Première édition : avril 2019

Référence du document : L62791–051

Logiciels Open Source

Ce produit inclut des logiciels sous licence Open Source, notamment la Licence Publique Générale GNU et la Licence Publique Générale GNU Limitée ou d'autres licences Open Source. Si HP en a l'obligation ou, à sa seule discrétion, choisit de rendre le code source disponible dans le cadre de la licence logicielle Open Source applicable, le code source du logiciel peut être obtenu à partir de l'emplacement suivant : ftp://ftp.hp.com/pub/tcdebian/pool/thinpro710/.

Clé de syntaxe du langage d'entrée utilisateur

Le texte que vous devez entrer dans une interface utilisateur est indiqué par `Police à espacement fixe`.

Élément	Description
`Texte sans crochets ni accolades`	Éléments que vous devez saisir exactement comme illustré
`<Texte entre chevrons>`	Un espace réservé pour une valeur que vous devez fournir ; Omettre les crochets
`[Texte entre crochets]`	Éléments en option ; Omettre les crochets
`{Texte entre accolades}`	Un ensemble d'éléments parmi lesquels vous devez en choisir un seul ; Omettre les accolades
`|`	Un séparateur d'éléments parmi lesquels vous devez en choisir un seul ; Omettre la barre verticale
`...`	Éléments qui peuvent ou doivent être répétés ; Omettre les points de suspension

Sommaire

1 Mise en route

Le présent guide est destiné aux administrateurs de clients légers HP basés sur le système d'exploitation HP ThinPro et considère que vous serez connecté au système en tant qu'administrateur lors de la modification des configurations système ou de l'utilisation des outils d'administration, tel que décrit dans ce guide.

REMARQUE : HP ThinPro peut utiliser deux configurations OS : ThinPro et Smart Zero. Les clients légers basés sur HP ThinPro peuvent être achetés avec l'une ou l'autre configuration OS définie comme configuration par défaut et vous pouvez basculer entre les configurations OS via le Panneau de configuration.

Pour en savoir plus sur chaque configuration OS, consultez la section Choix d'une configuration OS à la page 1. Pour plus d'informations sur le basculement entre les configurations OS, reportez-vous à la section Centre de personnalisation à la page 66.

Informations complémentaires

REMARQUE : Il est possible que le contenu des sites web indiqués dans ce tableau soit disponible uniquement en anglais.

Ressource	Table des matières
Site web d'assistance HP http://www.hp.com/support	Guides de l'administrateur, guides de référence matériel, livres blancs et autres documents ▲ Recherchez le modèle de client léger, puis reportez-vous à la section **Guides d'utilisation** de la page d'assistance correspondant à ce modèle. **REMARQUE :** Les logiciels HP Device Manager et HP Remote Graphics possèdent chacun une page d'assistance ; par conséquent recherchez plutôt le nom de l'application, puis reportez-vous à la section **Guides d'utilisation**.
Site web d'assistance de Microsoft http://support.microsoft.com	Documentation pour les produits logiciels de Microsoft
Site web d'assistance de Citrix http://www.citrix.com/support	Documentation pour les produits logiciels de Citrix
Site web d'assistance de VMware http://www.vmware.com/support	Documentation pour les produits logiciels de VMware

Choix d'une configuration OS

HP ThinPro comprend deux configurations OS, chacune étant adaptée à un scénario de déploiement de client léger distinct :

- La configuration OS **ThinPro** correspond à la version complète du système d'exploitation et convient mieux aux environnements polyvalents qui nécessitent une administration avancée ou une personnalisation par l'utilisateur final. Les caractéristiques de cette configuration OS sont les suivantes :

- Démarre dans l'écran de connexion du bureau ThinPro ou d'Active Directory
- fournit plus de types de connexion que la configuration Smart Zero ;
- autorise plusieurs connexions (de tous les types pris en charge) à configurer et exécuter simultanément.

- La configuration OS **ThinPro** est la version la plus simple et la plus sécurisée du système d'exploitation et convient mieux aux environnements à usage unique, tels que les environnements de type kiosque, qui nécessitent une administration minimale et une personnalisation réduite, voire inexistante, par l'utilisateur final. Les caractéristiques de cette configuration OS sont les suivantes :
  - démarre directement une session virtuelle et masque le bureau, caractéristique également appelée « mode kiosque » ;
  - fournit moins de types de connexion que la configuration ThinPro ;
  - Compatible avec une seule connexion à configurer et à exécuter à la fois.
  - Incompatible avec l'authentification d'Active Directory ou l'authentification unique

REMARQUE : Vous pouvez basculer entre les configurations OS via le Panneau de configuration (voir la section Centre de personnalisation à la page 66).

Vous pouvez également personnaliser certains des paramètres par défaut de chaque configuration OS. Par exemple, pour changer les types de connexion disponibles, activez le mode kiosque pour ThinPro ou démarrez sur le bureau pour Smart Zero.

Pour en savoir plus sur le mode kiosque, consultez la section Mode kiosque à la page 12.

Le tableau suivant fournit la liste des types de connexion disponibles par défaut pour chaque configuration OS.

Configuration OS	Types de connexion disponibles par défaut
ThinPro	• Citrix® • RDP • VMware® Horizon® View™ • Navigateur Web (Firefox) • XDMCP • Secure Shell • Telnet • Custom
Smart Zero	• Citrix • RDP • VMware Horizon View • Navigateur Web (Firefox)

Choix d'un service de gestion à distance

Quelle que soit la configuration OS utilisée, vous pouvez utiliser deux services de gestion à distance différents pour gérer les clients légers basés sur ThinPro :

- **HP Device Manager (HPDM)** est la solution idéale pour les environnements de grande taille comprenant plusieurs systèmes d'exploitation, y compris un mélange de clients légers basés sur HP ThinPro et Windows®. HPDM fournit une plus grande variété d'options de gestion que HP Smart Client Services. Pour plus d'informations sur HPDM ou pour le télécharger, rendez-vous sur http://www.hp.com/go/hpdm.
- **HP Smart Client Services** permet de gérer uniquement les clients légers basés sur HP ThinPro et est optimisé pour être utilisé avec Smart Zero et dans un scénario « zéro gestion ». Pour plus d'informations, voir HP Smart Client Services à la page 69. Pour plus d'informations sur la façon de télécharger HP Smart Services Client, reportez-vous à la section Obtention de HP Smart Client Services à la page 70.

HP recommande d'évaluer les deux services et de choisir celui qui est le mieux adapté à votre déploiement.

Démarrage du client léger pour la première fois

Lorsque vous démarrez pour la première fois un nouveau client léger basé sur HP ThinPro, un programme de configuration s'exécute automatiquement. L'Assistant de configuration initiale vous permet de sélectionner une langue, de sélectionner la configuration du clavier, de sélectionner une connexion réseau et de configurer les paramètres de date et d'heure.

CONSEIL : Si vous souhaitez modifier la configuration d'un seul client léger, puis copier et déployer la configuration sur d'autres clients légers, commencez par utiliser l'Assistant de configuration initiale et le Panneau de configuration pour modifier la configuration, puis déployez la configuration à l'aide de HPDM ou de HP ThinState. Pour plus d'informations, reportez-vous à la section Présentation de l'interface utilisateur graphique (IUG) à la page 7 ou Panneau de configuration à la page 48 Pour plus d'informations sur HP ThinState, reportez-vous à la section HP ThinState à la page 59.

Basculement entre le mode Administrateur et le mode Utilisateur

▲ Cliquez avec le bouton droit sur le bureau ou cliquez sur **Démarrer**, puis sélectionnez **Basculer en administrateur** dans le menu.

Pour plus d'informations sur le bureau, consultez la section Bureau à la page 7.

Pour plus d'informations sur le Panneau de configuration, reportez-vous aux sections Barre des tâches à la page 7 et Panneau de configuration à la page 48.

REMARQUE : Lorsque vous passez en mode Administrateur pour la première fois, vous êtes invité à définir un mot de passe administrateur. Par la suite, le mot de passe Administrateur doit être saisi à chaque que vous basculez vers le mode Administrateur. Lorsque l'authentification Active Directory est activée, vous pouvez également passer en mode Administrateur en saisissant les informations d'authentification du domaine d'une personne dans le groupe d'administration de domaine.

En mode Administrateur, l'écran est encadré d'une bordure rouge.

2 HP ThinPro PC Converter (Convertisseur PC ThinPro)

À partir de ThinPro 7.1, ThinPro peut être utilisé sur du matériel autre que des clients légers HP à l'aide de l'outil de déploiement HP ThinPro PC Converter. Le système doit répondre à ces exigences minimales :

- Processeur : Tout processeur x86 64 bits.
- Mémoire : 2 Go de mémoire, avec au moins 1 Go de mémoire libre pour l'utilisation du système d'exploitation.
- Stockage : 2 Go ou plus de stockage interne pour l'installation.
- Carte graphique : Intel ATI/AMD ou Nvidia. Si la carte graphique n'est pas reconnue, le mode VESA à rendement limité peut être utilisé.
- Audio : L'assistance audio est facultative.
- Mise en réseau : Adaptateur réseau sans fil ou filaire reconnu.
- USB : HP recommande des unités flash USB-C haute performance 2.0 ou 3.0.
- Licence : Le logiciel ThinPro doit être correctement sous licence.

La première fois qu'un système démarre avec ThinPro, une fenêtre de contrôle de compatibilité apparaît indiquant l'état de compatibilité du système avec chacune de ces exigences.

Outil de déploiement

L'outil de déploiement HP ThinPro PC Converter vous permet d'exécuter ThinPro sur un PC qui exécute Microsoft Windows et qui répond aux exigences minimales. Cet outil permet la création d'une unité flash USB contenant l'image ThinPro. Vous pouvez démarrer et exécuter l'image ThinPro à partir de l'unité flash USB créée ou vous pouvez installer l'image ThinPro directement sur le PC. Vous avez également la possibilité de créer une image de déploiement de masse déployable par des outils de gestion à distance.

Pour plus d'informations, reportez-vous au *Manuel de l'administrateur de l'outil de déploiement HP THINPRO PC Converter*.

Vérification de la compatibilité et installation

La première fois que ThinPro est démarré à partir d'une unité flash USB, la fenêtre de vérification de la compatibilité s'affiche. L'outil de vérification de la compatibilité évalue le matériel sur le système pour voir s'il est conforme aux exigences minimales et si le logiciel ThinPro a reconnu le périphérique et a attribué un pilote de périphérique. Si le système ne répond pas aux exigences minimales, ou si le matériel requis est introuvable, l'outil de vérification de la compatibilité affichera un avertissement et des informations supplémentaires.

REMARQUE : L'outil de vérification de la compatibilité ne fait qu'un examen superficiel de l'état du matériel et du pilote. Il n'effectue pas de vérification des fonctionnalités détaillées comme l'envoi de paquets réseau, la lecture de fichiers audio, le test de blocs de mémoire incorrects ou l'évaluation des performances. HP n'est pas en mesure de garantir que tous les composants matériels du PC fonctionnent bien avec ThinPro, même si l'outil de vérification de la compatibilité détermine que le PC est compatible.

Si ThinPro est en cours d'exécution à partir d'une unité flash USB, et si le contrôle de compatibilité passe toutes les vérifications requises, deux boutons apparaissent en bas de la fenêtre. Le premier bouton permet d'installer le logiciel ThinPro directement sur le stockage interne. Le deuxième bouton vous permet d'exécuter ThinPro à partir de l'unité flash USB sans installation directe sur le PC.

REMARQUE : Le bouton d'installation apparaît uniquement avec une unité flash USB créée avec l'option de l'unité Flash d'installation de l'outil de déploiement. L'option de l'unité flash amorçable n'autorise pas l'installation.

Lors de l'installation de ThinPro sur le PC, vous avez la possibilité d'enregistrer les paramètres qui ont été configurés lors de l'exécution de ThinPro à partir de l'unité flash USB. Si les paramètres ne sont pas enregistrés, l'image d'usine par défaut de ThinPro sera installée.

L'outil de vérification de la compatibilité peut également être démarré manuellement à partir de la liste des outils administrateur sous le bouton Démarrer.

Licence

Les clients légers HP pris en charge sont titulaires d'une licence automatique et n'ont pas besoin de fichiers de licence. Si un système est sous licence automatique, la plupart des sources d'informations de licence répertoriées ci-dessous ne seront pas visibles.

Tous les autres systèmes nécessitent des fichiers de licence valides pour exécuter ThinPro. Les fichiers de licence proviennent de HP Inc. Software Depot.

L'outil de déploiement vous invite à accéder aux fichiers de licence valides. Les fichiers que vous sélectionnez seront automatiquement copiés lorsque vous créez une unité flash USB de démarrage et d'installation ThinPro, et également lorsque vous créez une image de déploiement de masse.

Si l'outil de déploiement et les licences valides sont utilisés pour installer ThinPro sur un périphérique, il n'est pas nécessaire d'installer manuellement les fichiers de licence. Cependant, si vous installez ThinPro via d'autres moyens, vous devrez peut-être copier les fichiers de licence dans le répertoire `/persistent/licenses` sur le périphérique. Vous pouvez utiliser HP Device Manager (ou d'autres mécanismes) pour effectuer ce déploiement.

Types de licence

Il existe trois types de fichiers de licence :

- Une licence d'essai vous permet d'exécuter ThinPro pendant une courte période sans payer les frais de licence.
- Une licence unitaire vous permet d'exécuter une version particulière de ThinPro indéfiniment. Cela indique également que les droits de redevance ont été payés et que cela déverrouille tout logiciel soumis à une redevance.
- Une licence d'assistance permet d'accéder aux correctifs système et aux améliorations, et permet de mettre à niveau le système vers les versions plus récentes de ThinPro.

En fonction de la combinaison de licences présente sur le système, diverses fonctions seront rendues visibles, cachées ou désactivées.

Icône de la barre d'état système

Une icône de la barre d'état système indique l'état de licence du système.

Icône	Description
	Licence valide.
	Expiration prochaine de la licence.
	Licence non valide (telle qu'une licence d'essai expirée).

Le survol de l'icône de la barre des tâches fournit des informations sur les licences actives trouvées sur le système. Un clic droit va lancer l'application Info Système avec l'onglet **Licence** sélectionné.

notifications

Les notifications peuvent apparaître à intervalles réguliers au-dessus de l'icône de la barre d'état système.

Les notifications de courtoisie mettent en garde lorsqu'une licence d'assistance ou une licence d'essai se rapproche de la date d'expiration. Vous pouvez désactiver les notifications de courtoisie via certains paramètres de registre. Consultez la section Clés de registre à la page 85 pour en savoir plus.

D'autres notifications mettent en garde contre les erreurs de licence telles que les fichiers de licence expirés, manquants ou non valides. Vous ne pouvez pas désactiver ces types de notifications.

Informations système

L'onglet Licence logicielle de l'application Informations système indique à la fois l'état global de licence du système et les détails de chaque fichier de licence qui se trouve sur le système, y compris les dates de début et de fin, le nombre de licences, le numéro de série de licence, ainsi que d'autres informations.

Filigrane d’arrière-plan du bureau

Le texte en filigrane est affiché sur l'arrière-plan du bureau avec une licence d'essai ou avec une combinaison de licences expirées ou non valides. Vous ne pouvez pas désactiver ce texte en filigrane.

Outils de mise à jour système

Si un système n'est pas sous licence automatique et qu'il n'est pas titulaire d'une licence de support actif, les correctifs et mises à niveau affichés par Easy Update et d'autres outils de mise à jour système seront limités.

Logiciels sous redevance

Certains logiciels utilisés par ThinPro comportent des redevances rattachées. Par exemple, n'importe quelle fonctionnalité utilisant le décodage vidéo H. 264. Si le système n'est pas sous licence automatique et qu'aucune licence d'unité valide n'est disponible sur le système, les logiciels sous redevance seront désactivés. Les licences d'essai n'autorisent pas les logiciels sous redevance.

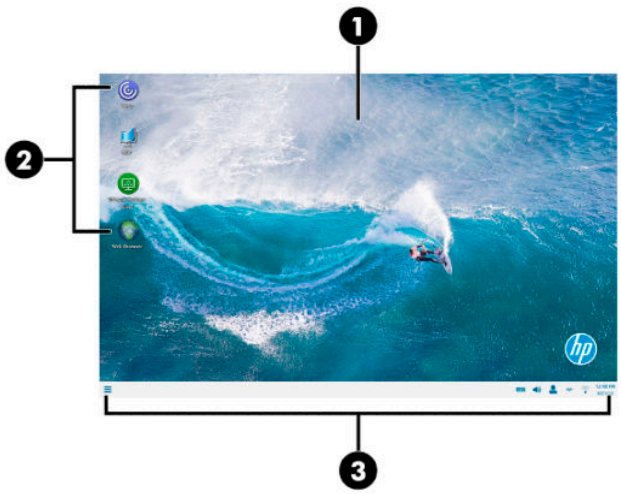
Connexions

Si aucune combinaison de licence valide n'est disponible sur le système, la possibilité de créer des connexions à distance vers d'autres systèmes peut être limitée ou désactivée.

3 Présentation de l'interface utilisateur graphique (IUG)

Bureau

REMARQUE : L'illustration suivante présente le bureau pour ThinPro avec des paramètres régionaux américains. Pour Smart Zero, la barre des tâches est verticale et alignée à droite par défaut et le thème du bureau varie selon le type de connexion. Le format d'affichage de certaines informations de la barre des tâches varie en fonction des paramètres régionaux.



Élément		Description
(1)	Bureau	Dans ThinPro, vous pouvez organiser les raccourcis de connexion dans la zone du bureau et personnaliser le thème d'arrière-plan. Dans Smart Zero, le bureau est remplacé par un écran de connexion personnalisable avec un thème spécifique au type de connexion choisi.
(2)	Raccourcis de connexion	Double-cliquez sur un raccourci de connexion pour démarrer une connexion. Cliquez avec le bouton droit sur l'icône pour afficher un menu d'actions liées à la connexion actuelle et sélectionnez pour faire glisser l'icône vers un nouvel emplacement.
(3)	Barre des tâches	Fournit un accès rapide aux programmes et fonctions système (consultez la section Barre des tâches à la page 7 pour plus d'informations).

Barre des tâches

REMARQUE : L'illustration suivante présente la barre des tâches pour ThinPro avec des paramètres régionaux américains. Pour Smart Zero, la barre des tâches est verticale et alignée à droite par défaut. Le format d'affichage de certaines informations de la barre des tâches varie en fonction des paramètres régionaux.

Élément		Description
(1)	Démarrer	Affiche un menu principal Pour plus d'informations, voir menu Démarrer à la page 46.
(2)	Zone des applications	Affiche les icônes des applications actuellement ouvertes. **CONSEIL :** Vous pouvez appuyez sur Ctrl+Alt, puis appuyer à plusieurs reprises sur la touche Tabulation pour sélectionner une application à afficher au premier-plan.
(3)	Barre d'état système	Fournit un accès rapide à ou fournit des informations sur certaines fonctions et services. Placez le curseur sur un élément de la barre d'état système pour afficher une infobulle (certains éléments uniquement). Sélectionnez pour lancer une action de configuration, et cliquez avec le bouton droit de la souris pour afficher un menu. Les éléments dans la barre d'état système peuvent inclure les éléments suivants, mais certains peuvent ne pas apparaître selon la configuration du système : • Mélangeur audio • Keyboard (Clavier) : Sélectionnez cette icône pour modifier la disposition du clavier, ouvrir le clavier virtuel ou modifier l'architecture du système. Cliquez avec le bouton droit de la souris pour ouvrir le clavier virtuel. Pour afficher le nom de la disposition du clavier actuelle, pointez le curseur de la souris sur l'icône. • Statut du réseau câblé : Cliquez avec le bouton droit sur cette icône pour afficher plus d'informations sur un réseau connecté. • État du réseau sans fil : Sélectionnez cette icône pour afficher la liste des réseaux sans fil disponibles et vous connecter à l'un d'eux, en créant un profil de réseau sans fil qui lui correspond. • État d'Automatic Update : L'icône d'Automatic Update (mise à jour automatique) s'affiche lorsque la mise à jour automatique est à la recherche de mises à jour ou met à jour l'ordinateur. Pour afficher plus d'informations, cliquez sur l'icône. Si ThinPro ne parvient pas à trouver un serveur de mise à jour automatique valide ou si la clé de registre pour afficher l'icône est désactivée, l'icône ne s'affiche pas. • Intelligent Input Bus (Ibus) : Ibus est un cadre de méthode d'entrée (IM) pour les entrées multilingues dans les systèmes d'exploitation de type UNIX. • Icône Batterie : Pour ouvrir le gestionnaire d'alimentation, cliquez avec le bouton droit sur cette icône et sélectionnez **Adjust Power Settings** (Réglage des paramètres d'alimentation). • Icône Utilisateur : Indique que l'authentification Active Directory est activée. Sélectionnez pour verrouiller l'écran ou mettre à jour le mot de passe du domaine. Pour afficher l'utilisateur actuel, pointez le curseur de la souris sur l'icône. • Icône de licence : Indique l'état de licence ThinPro. Survolez l'icône pour afficher les détails des licences actuellement actives et cliquez avec le bouton droit de la souris pour accéder à la page Informations système pour afficher plus de détails sur les licences. Cela n'est pas visible sur les clients légers HP actuels, car ils sont sous licence automatique.
(4)	Date et heure	Affiche la date et l'heure du jour et ouvre les paramètres de date et d'heure.

4 Configuration des connexions

Gestion des connexions de bureau

La gestion des connexions peut s'effectuer directement à partir du bureau, ainsi que par l'intermédiaire de l'ancien Connection Manager (se reporter à Gestionnaire de connexion (ThinPro uniquement) à la page 10) ou le menu Démarrer. Par défaut, le bureau affiche une icône en tant que raccourci pour chaque connexion configurée.

Lorsque vous démarrez l'ordinateur, plusieurs exemples d'icônes de connexion sont affichées sur le bureau. Vous pouvez créer un nouveau raccourci de connexion générique pour tous les types de connexion prises en charge par ThinPro.

▲ Pour créer un nouveau raccourci de connexion, cliquez avec le bouton droit sur le bureau, puis sélectionnez **Créer**.

Toutes les icônes sont automatiquement placées dans une grille. Vous pouvez cliquer et faire glisser une icône vers toute autre position de la grille sur le bureau. Une fois qu'une icône a été déplacée vers une position de la grille, elle est immobilisée dans cette position. Elle reste dans cette position même si d'autres raccourcis de connexion sont ajoutés, supprimés ou réarrangés.

Toutes icônes non fixées dans une position de la grille restent flottantes. Elles peuvent être déplacées automatiquement lorsque les raccourcis de connexion sont ajoutés, supprimés ou réarrangés. Pour modifier une icône fixée en une icône flottante, cliquez avec le bouton droit sur l'icône et supprimez **Fixer la position**.

Vous pouvez démarrer, arrêter, modifier, copier, renommer ou supprimer chaque connexion. Si la modification d'utilisateur n'est pas activée, les utilisateurs non-administrateurs peuvent uniquement démarrer ou arrêter une connexion.

▲ Pour gérer une connexion sur le bureau, cliquez avec le bouton droit sur l'icône de connexion, puis sélectionnez une action.

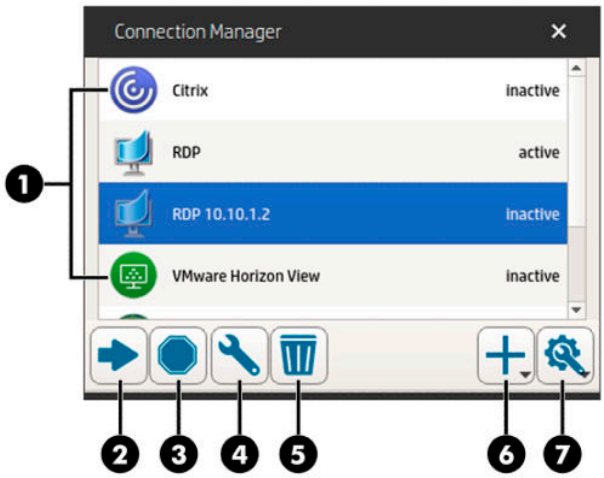
REMARQUE : Si la modification d'utilisateur n'est pas activée, vous devez passer en mode administrateur pour gérer une connexion.

- **Start/Stop** (Arrêt/départ) : Démarre une connexion ou interrompt une connexion active. Vous pouvez également double-cliquer sur l'icône de connexion. Lorsque la connexion est active, un cercle vert s'affiche sur l'icône de connexion, et l'icône de connexion est affichée dans la barre des tâches. Lorsqu'une connexion démarre, si les paramètres de connexion sont manquants, une boîte de dialogue vous demande les paramètres manquants. Par exemple, lorsqu'aucune des icônes de démarrage n'a de serveur distant de défini, une boîte de dialogue vous demande d'indiquer l'adresse ou le nom du serveur distant lorsque la connexion est démarrée.
- **Edit** (Modifier) : Ouvre l'éditeur de connexion complet.
- **Copy** (Copier) : Crée une copie de la connexion avec tous les paramètres de la connexion d'origine et un nom unique.
- **Rename** (Renommer) : Vous permet de renommer la connexion. Vous pouvez également double-cliquer sur le texte sous l'icône de connexion ou utiliser l'éditeur de connexion.
- **Delete** (Supprimer) : Supprime la connexion.

Gestionnaire de connexion (ThinPro uniquement)

REMARQUE : HP recommande d'utiliser les raccourcis de connexion. Toutefois, vous pouvez utiliser l'ancienne interface de Connection Manager.

L'illustration suivante présente le Gestionnaire de connexion avec des paramètres régionaux américains.



Élément		Description
(1)	Liste des connexions	Affiche la liste des connexions configurées en indiquant si chaque connexion est active ou inactive.
(2)	Démarrer	Démarre la connexion sélectionnée.
(3)	Arrêter	Arrête la connexion sélectionnée.
(4)	Modifier	Permet de modifier la connexion sélectionnée.
(5)	Supprimer	Supprime la connexion sélectionnée.
(6)	Ajouter	Permet d'ajouter une nouvelle connexion. **REMARQUE :** Reportez-vous à la section Choix d'une configuration OS à la page 1 pour obtenir la liste des types de connexions disponibles.
(7)	Paramètres	Vous permet de modifier les paramètres généraux pour les connexions Citrix. Ces paramètres s'appliquent à toutes les connexions de ce type.

Pour ouvrir Connection Manager :

1. En mode Administrateur, cliquez sur **Démarrer**, puis tapez `Connection Manager (Gestionnaire de connexion)` dans la boîte de recherche.
2. Sélectionnez **Connection Manager**.

Pour plus d'informations sur la configuration des connexions, reportez-vous aux sections suivantes :

- Configuration des connexions à la page 9
- Types de connexion à la page 13

Paramètres de connexion avancés

Le tableau suivant décrit les paramètres disponibles sous la catégorie Avancé lors de la modification d'une connexion, quel qu'en soit le type.

REMARQUE : Ces paramètres affectent uniquement la connexion que vous configurez.

Option	Description
Connexion de repli	Spécifie la connexion de secours. Si la connexion ne parvient pas à démarrer, la connexion de secours prend le relais. **REMARQUE :** Cette option n'est pas disponible pour les connexions de type VMware Horizon View.
Priorité du démarrage automatique	Détermine l'ordre du démarrage automatique des connexions. **0** signifie que le démarrage automatique est désactivé. Les autres valeurs déterminent l'ordre de démarrage, **1** étant la priorité la plus élevée.
Partager les informations d'authentification avec l'écran de veille	Permet aux utilisateurs de déverrouiller l'économiseur d'écran local à l'aide de leurs informations d'authentification pour cette connexion. **REMARQUE :** Cette option est uniquement disponible pour les connexions de type Citrix, RDP et VMware Horizon View.
Reconnexion automatique	Si l'option est activée, cette connexion essaie de se reconnecter automatiquement en cas de perte de la connexion. **REMARQUE :** L'arrêt d'une connexion dans le Gestionnaire de connexion empêche la reconnexion automatique.
Attente du réseau avant connexion	Désactivez cette option si votre connexion n'a pas besoin du réseau pour démarrer ou si vous ne souhaitez pas attendre le réseau pour démarrer la connexion.
Afficher l'icône sur le Bureau	Si cette option est activée, une icône de bureau est créée pour cette connexion. Cette option est activée par défaut. Si cette option est désactivée, la connexion n'est pas visible sur le bureau, mais est visible dans le menu Démarrer et dans Connection Manager.
Autoriser l'utilisateur à lancer cette connexion	Si cette option est activée, cette connexion peut être lancée par un utilisateur final.
Autoriser l'utilisateur à modifier cette connexion	Si cette option est activée, cette connexion peut être modifiée par un utilisateur final.
Options de boîte de dialogue de connexion	Activez ou désactivez ces options pour configurer la boîte de dialogue de connexion. **REMARQUE :** Cette option est uniquement disponible pour les connexions de type Citrix, RDP et VMware Horizon View. Les options suivantes sont disponibles : • **Afficher le champ de nom d'utilisateur** • **Afficher le champ de nom d'utilisateur** • **Afficher le champ de mot de passe** • **Afficher le champ de domaine** • **Afficher la case à cocher « Se souvenir de moi »** **REMARQUE :** Cette option permet d'enregistrer le nom d'utilisateur et le domaine, mais le mot de passe doit toujours être entré à chaque fois.

Mode kiosque

Lorsque le mode kiosque est configuré pour un client léger, il effectue une ouverture de session automatique sur la connexion par défaut au démarrage, à l'aide des informations d'authentification prédéfinies de l'utilisateur. Si la connexion est perdue suite à une fermeture de session, une déconnexion ou une défaillance du réseau, elle se reconnecte automatiquement dès que possible.

CONSEIL : L'hôte distant peut être configuré pour démarrer automatiquement les ressources lors de l'ouverture de session, pour que le mode kiosque soit plus simple d'utilisation.

La façon la plus simple de configurer le mode kiosque pour un client léger est de passer à Smart Zero (reportez-vous à la section Centre de personnalisation à la page 66) et de configurer une connexion. Lorsque vous avez terminé, les paramètres suivants sont configurés automatiquement :

- La barre des tâches est masquée automatiquement.
- La connexion démarre automatiquement.
- La connexion se reconnecte automatiquement.
- La connexion partage les informations d'authentification de l'utilisateur avec l'économiseur d'écran local.
- Le thème du bureau est configuré en fonction du thème par défaut de ce type de connexion.
- Le protocole de redirection USB du gestionnaire USB est configuré en fonction du protocole de ce type de connexion.

Si vous souhaitez configurer le mode kiosque pour un client léger dans ThinPro (par exemple, si vous souhaitez utiliser un type de connexion disponible uniquement avec ThinPro), vous devez configurer manuellement les paramètres suivants pour la connexion souhaitée :

- Dans le Customization Center (Centre de personnalisation), définissez le paramètre de barre des tâches sur **Masquer automatiquement**.
- Dans les paramètres de connexion, effectuez les opérations suivantes :
  - Définissez **Priorité du démarrage automatique** sur **1**.
  - Activez le paramètre **Reconnexion automatique**.
  - S'il est disponible, activez le paramètre **Partager les informations d'authentification avec l'écran de veille**.
  - Pour la connexion Navigateur Web uniquement, sélectionnez l'option **Activer le mode kiosque**.
- Dans le gestionnaire USB, définissez le protocole de la redirection USB approprié, si nécessaire.

CONSEIL : En mode kiosque, pour minimiser la connexion et revenir au bureau local, appuyez sur Ctrl+alt +fin.

5 Types de connexion

Citrix

Le tableau ci-dessous décrit les backends Citrix XenApp.

Type d'accès	Version de XenApp
PNAgent (hérité)	7.6 LTSR ou 7.15 LTSR et 7.16 ou supérieur
Navigateur Internet	7.6 LTSR ou 7.15 LTSR et 7.16 ou supérieur
StoreFront	7.6 LTSR ou 7.15 LTSR et 7.16 ou supérieur
Espace de travail	7.6 LTSR ou 7.15 LTSR et 7.16 ou supérieur

Le tableau ci-dessous décrit les backends Citrix XenApp®.

Type d'accès	Version de XenApp
PNAgent (hérité)	7.6 LTSR ou 7.15 LTSR et 7.16 ou supérieur
Navigateur Internet	7.6 LTSR ou 7.15 LTSR et 7.16 ou supérieur
StoreFront	7.6 LTSR ou 7.15 LTSR et 7.16 ou supérieur
Espace de travail	7.6 LTSR ou 7.15 LTSR et 7.16 ou supérieur

Gestionnaire de connexion Citrix

REMARQUE : Les paramètres de connexion, de configuration et avancés affectent uniquement la connexion que vous êtes en train de configurer. Les paramètres généraux affectent toutes les connexions Citrix.

Connection (Connexion)

Le tableau suivant décrit les paramètres disponibles sous la catégorie Connection (Connexion) lors de la modification d'une connexion Citrix.

Option	Description
Nom	Le nom de la connexion.
Mode de connexion	Définit l'un des modes de connexion suivants : • **PNAgent** • **StoreFront** • **Espace de travail** **REMARQUE :** Les options d'authentification sont affichées après cette option et varient en fonction du mode de connexion sélectionné. Pour plus d'informations, reportez-vous à la documentation Citrix.

Option	Description
	REMARQUE : Vous pouvez tester les paramètres de connexion en sélectionnant le bouton **Test connection** (Tester la connexion).
URL	Le nom d'hôte ou l'adresse IP du serveur Citrix. Si vous configurez une connexion à un serveur sur un site HTTPS, entrez le FQDN du site et le certificat de racine local dans la liste de certificats Citrix. La case à cocher en regard de cette option force une connexion HTTPS, si elle est cochée.
Ignore Certificate Check (Ignorer la vérification des certificats)	Ignore la vérification du certificat du serveur Citrix. **REMARQUE :** Le mode espace de travail ne peut ignorer la vérification des certificats.
Informations d'authentification	Définit l'un des modes de connexion suivants : • **Connexion anonyme** : Pour les serveurs StoreFront qui autorisent les utilisateurs non authentifiés (anonymes). • **Utiliser les informations d'authentification unique** : Les informations d'authentification utilisées le sont également pour démarrer la connexion. • **Demander les informations d'identification au démarrage de la connexion** : Aucun composant d'information d'authentification n'est fourni au préalable. • **Utiliser un utilisateur, un mot de passe et/ou un domaine prédéfinis** : Tout ou partie des informations d'authentification est stockée et fournie pour la connexion. • **Utiliser une carte à puce prédéfinie** : La connexion est prévue pour être utilisée avec une carte à puce pour l'authentification.
Utilisateur	Nom d'utilisateur pour cette connexion.
Mot de passe	Mot de passe pour cette connexion.
Domaine	Nom de domaine pour cette connexion (facultatif).
Tester la connexion	Vérifie l'URL et les informations d'authentification.

Configuration

Le tableau suivant décrit les paramètres disponibles sous la catégorie Configuration lors de la modification d'une connexion Citrix.

Option	Description
Reconnecter automatiquement les applications à l'ouverture de session	Lorsque cette option est sélectionnée, les ressources qui ont été ouvertes lors de la dernière fermeture de session de l'utilisateur seront réouvertes lorsqu'ils se reconnectent. **CONSEIL :** Si vous n'utilisez pas la fonction SmoothRoaming Citrix, désactivez cette option pour augmenter votre vitesse de connexion.
Mode Démarrage auto	Permet de configurer le démarrage automatique d'une application ou d'un bureau spécifique lorsque la connexion Citrix est établie. Si cette option est définie sur **Démarrer automatiquement une ressource unique**, et si une seule ressource est publiée, cette ressource démarre automatiquement. **REMARQUE :** L'option reste sans effet si **Reconnexion auto des applications à l'ouverture de session** est sélectionnée et s'il existe des applications auxquelles se reconnecter. Si vous avez sélectionné Démarrage auto de l'application ou Démarrage auto du bureau, sélectionnez le bouton **Énumération** pour récupérer la liste des ressources (applications

Option	Description
	ou bureaux) et les afficher dans le Gestionnaire de connexions Citrix, ce qui vous permet de sélectionner les ressources à démarrer automatiquement lors de la connexion. Si vous avez sélectionné Démarrer automatiquement une ressource unique, cliquez sur le bouton **Énumération** pour récupérer le nombre de ressources. S'il n'y a qu'une seule ressource, elle démarre automatiquement lors de la connexion.
Show resources (Afficher les ressources)	Lorsque cette option est sélectionnée, vous devez alors sélectionner l'emplacement d'affichage des ressources : ● **Dans une fenêtre** : Affiche les ressources dans une fenêtre. ● **Directement sur le bureau** : Affiche les ressources sur le bureau.
Afficher les ressources dans le menu Démarrer	Lorsque cette option est sélectionnée, les ressources à distance de la connexion sont affichées dans le menu Démarrer.
Afficher uniquement les ressources auxquelles des utilisateurs se sont abonnés	Si cette option est sélectionnée, seules les ressources auxquelles les utilisateurs se sont abonnés sont affichées lors d'une connexion Citrix. **REMARQUE :** Cette option n'est pas prise en charge lorsque vous utilisez Citrix self-service UI.

Paramètres généraux

REMARQUE : Ces paramètres affectent toutes les connexions Citrix.

Pour modifier les paramètres généraux :

▲ Dans Citrix Connection Manager, cliquez sur l'onglet **Paramètres généraux**, puis sélectionnez **Xen Connection General Settings Manager (Gestionnaire de paramètres généraux de connexion Xen)**.

Options

Le tableau suivant décrit les paramètres disponibles sous la catégorie Options lors de la modification des paramètres généraux Citrix.

Option	Description
Activer HDX MediaStream	Active HDX MediaStream.
Activer MultiMedia	Activer Multimédia
Activer la barre de connexion	Active la barre de connexion.
Activer Auto Reconnect	Active une reconnexion automatique des connexions abandonnées.
Activer la fiabilité de la Session	Active la fonction de Fiabilité de Session Citrix. Pour plus d'informations, reportez-vous à la documentation Citrix.
Activer le canal de la carte à puce	Active la fonction de canal de la carte à puce. **REMARQUE :** Si vous voulez utiliser une carte à puce dans la session Citrix mais n'utilisez pas une connexion par carte à puce, activez cette option.
Durée de la fiabilité de session (secondes)	Spécifie le délai d'expiration de la fiabilité de session en secondes. La valeur par défaut est de 180 secondes.
Activer la Redirection dans le presse-papiers	Active la redirection dans le presse-papiers.
Utiliser la compression des données	Utilise la compression des données pour cette connexion.

Option	Description
Activer Compression H264	Active la compression H264. Reportez-vous à la documentation Citrix pour déterminer si cette méthode de compression de données convient mieux à vos cas d'usage.
Activer l'action Coller du bouton central	Active la fonction Coller du bouton central de la souris.
Chaîne de l'agent utilisateur	Spécifier une chaîne d'agent utilisateur à utiliser pour les requêtes envoyées au serveur Citrix. Cette option est utile pour la configuration Netscaler.
Son	Permet de régler la qualité sonore ou désactive le son entièrement.
Protocole transport	Indique le protocole de transport pour la connexion et l'utilisation ou non d'un protocole de transport de remplacement. • **Désactivé** (par défaut) : Utilisez TCP. • **Allumé** : Utiliser UDP et ne pas retomber en TCP en cas d'échec. • **Favori** : Essayer UDP d'abord et retomber en TCP en cas d'échec.
Utiliser les suites chiffrées obsolètes	Spécifie si les suites de chiffrement obsolètes : TLS_RSA, RD4-MD5, RC4_128_SHA sont autorisées ou non.

Local Resources (Ressources locales)

Le tableau suivant décrit les paramètres disponibles sous la catégorie Local Resources (Ressources locales) lors de la modification des paramètres généraux Citrix.

Option	Description
État de la redirection USB Citrix	Pour configurer, sélectionnez **USB Manager (Gestionnaire USB)**. Reportez-vous à la section Redirection des périphériques USB à la page 65. • **Activé** : La redirection USB est prise en charge pour la connexion Citrix. • **Désactivé** : La redirection USB est désactivée pour la connexion Citrix.
imprimantes	Contrôle comment la redirection d'imprimante locale est traitée.
Entrée webcam/audio	Contrôle comment la redirection de la webcam locale et d'une entrée audio est traitée.
Mappage du lecteur/Redirection	Spécifie la méthode utilisée pour accéder au lecteur local. **REMARQUE :** Sélectionner une seule méthode de redirection de lecteur. • **Redirection USB** : Active la redirection USB. Pour plus d'options, ouvrez **USB Manager**. • **Dynamic Drive Mapping (Mappage d'unité dynamique)** : Active le mappage d'unité dynamique. • **Static Drive Mapping (Hérité) (Mappage d'unité statique (Hérité))** : Active le mappage d'unité statique, qui vous permet de spécifier les mappages d'unités vers des chemins locaux. Pour spécifier ces chemins d'accès, sélectionnez **Configurer les dossiers de mappage**.

Window (Fenêtre)

Le tableau suivant décrit les paramètres disponibles sous la catégorie Window (Fenêtre) lors de la modification des paramètres généraux Citrix.

Option	Description
Mode TWI	Vous permet d'afficher une fenêtre sans discontinuité unique sur le bureau ThinPro local comme s'il s'agissait d'une application native.
Taille de la fenêtre par défaut	Lorsque **le Mode TWI** est défini sur **Force seamless Off** (FORCER l'arrêt sans discontinuité), cela contrôle la taille de la fenêtre par défaut.
Couleurs de fenêtres par défaut	Permet de régler la profondeur de couleur par défaut.
Écran gauche Écran droit Écran supérieur Écran inférieur	Lorsque l'option **Show the Virtual Desktop on all monitors** (Afficher le bureau virtuel sur tous les écrans) est désactivée, ces champs vous permettent de spécifier comment le bureau virtuel est affiché par les écrans spécifiques.

Libre service

Le tableau suivant décrit les paramètres disponibles sous la catégorie Libre service lors de la modification des paramètres généraux Citrix (pour le mode espace de travail uniquement).

Option	Description
Option 1 Activer le mode kiosque	Configurez un périphérique utilisateur pour démarrer en mode kiosque, dans lequel le libre-service démarre en mode plein écran.
Option 1.1 Afficher la barre des tâches	Spécifie si la barre des tâches est affichée ou non. Le Centre de personnalisation dispose d'options supplémentaires pour personnaliser la barre de tâches.
Option 1.2 Activer le mode utilisateur partagé	Plusieurs utilisateurs peuvent partager l'appareil.
Option 2 Préférences - Désactiver l'espace de travail Citrix	Désactiver l'élément de menu Citrix – Préférences dans l'interface utilisateur Libre-service.
Option 3 Désactiver le centre de connexion	Désactiver l'élément de menu Citrix – Centre de connexion dans l'interface utilisateur Libre-service.

Firewall (Pare-feu)

Le tableau suivant décrit les paramètres disponibles sous la catégorie Firewall (Pare-feu) lors de la modification des paramètres généraux Citrix.

Option	Description
Type de proxy	Spécifie le type de proxy.
Adresse du proxy	L'adresse IP du serveur proxy.
Port du proxy	Le port pour la connexion au serveur proxy.
Nom d'utilisateur	Le nom d'utilisateur à utiliser pour la connexion au serveur proxy.
Mot de passe	Le mot de passe à utiliser pour la connexion au serveur proxy.
Utiliser une adresse alternative pour la connexion du pare-feu	Le client Citrix ICA demande l'adresse secondaire définie pour le serveur lors de la connexion de serveurs à l'intérieur du pare-feu. L'adresse secondaire doit être spécifiée pour chaque serveur dans une batterie de serveurs.

Keyboard Shortcuts (Raccourcis clavier)

Le tableau suivant décrit les paramètres disponibles sous la catégorie Keyboard Shortcuts (Raccourcis clavier) lors de la modification des paramètres généraux Citrix.

Option	Description
Activer UseLocalIM	Utilise la méthode de saisie locale pour interpréter les données saisies au clavier. Prise en charge uniquement pour les langues européennes.
Utiliser le numéro EUKS	Contrôle l'utilisation d'EUKS (Extended Unicode Keyboard Support) sur les serveurs Windows. Les options valides sont décrites ci-dessous : • 0 : EUKS n'est pas utilisé. • 1 : EUKS est utilisé comme remplacement. • 2 : EUKS sert à chaque fois que possible.
Dossier configuration clavier	Spécifie le fichier de mappage du clavier. Sélectionnez **Auto** pour permettre au fichier d'être sélectionné automatiquement. Sinon, sélectionnez un fichier de mappage spécifique. **REMARQUE :** Pour utiliser votre propre fichier de mappage du clavier, l'enregistrer dans le dossier : `/usr/lib/ICAClient/keyboard/`.
Transmission des raccourcis clavier	Spécifie la manière dont les touches de raccourci doivent être gérées. Les paramètres suivants sont disponibles : • **Traduit** : Les raccourcis clavier s'appliquent au bureau local (côté client). • **Directement sur les bureaux plein écran uniquement** : Les raccourcis clavier s'appliquent au bureau à distance (côté serveur), mais uniquement pour une session de ICA non sans discontinuité en mode plein écran. • **Direct** : Les raccourcis clavier s'appliquent au bureau à distance (côté serveur) pour les sessions de ICA sans discontinuité et avec discontinuité lorsque leurs fenêtres disposent de la mise au point du clavier.
Arrêt de la gestion directe des touches	Spécifie la combinaison de touches qui désactive le traitement direct des raccourcis clavier.
Alt+F1 ... Alt+F12	Vous permet d'ajouter des raccourcis de clavier à gérer.

Session

Le tableau suivant décrit les paramètres disponibles sous la catégorie Session lors de la modification des paramètres généraux Citrix.

Option	Description
Délai de fermeture de session automatique avant le lancement de l'application	Lorsque vous utilisez un serveur Citrix avec plusieurs ressources publiées, cette option indique le nombre de secondes disponibles pour que l'utilisateur lance une application après l'ouverture de session avant que le système ne se déconnecte automatiquement et revienne à l'écran d'ouverture de session initial.
Délai de fermeture de session automatique après la fermeture de l'application	Lorsque vous utilisez un serveur Citrix avec plusieurs ressources publiées, cette option indique le nombre de secondes disponibles entre la fermeture de la dernière ressource publiée Xen et la fermeture de session automatique de l'utilisateur et l'affichage de l'écran d'ouverture de session initial.

Option	Description
Délai du contrôle du serveur	Pour effectuer une vérification basique de la connectivité au serveur et au port sélectionnés, définissez cette option sur une valeur autre que la valeur par défaut **–1**.

CONSEIL : Si l'une de ces valeurs est inférieure à 0, la fermeture de session automatique est désactivée.

REMARQUE : Les délais de traitement de Citrix sont susceptibles d'augmenter le temps de fermeture de session automatique.

Avancé

REMARQUE : Reportez-vous à la section Paramètres de connexion avancés à la page 11 pour plus d'informations sur les paramètres disponibles dans la catégorie Avancé lors de la modification d'une connexion.

RDP

Le client RDP est basé sur FreeRDP 1.1 et répond aux exigences suivantes concernant le RDP :

- RemoteFX à accélération matérielle
- Prise en charge de MMR lors de la connexion à des hôtes si la fonction Desktop Experience (Expérience Bureau) est activée
- Prise en charge de USBR lors de la connexion à des serveurs RDP pour l'activer

Paramètres RDP par connexion

REMARQUE : Ces paramètres affectent uniquement la connexion que vous configurez.

réseau

Le tableau suivant décrit les paramètres disponibles sous la catégorie Réseau lors de la modification d'une connexion RDP.

Option	Description
Nom de la connexion	Un nom personnalisé pour cette connexion
Nom/adresse du serveur	Le nom du serveur ou l'adresse IP pour cette connexion, ou l'URL d'alimentation de l'accès par internet aux services de bureau à distance (RD). Si nécessaire, le port peut être ajouté au serveur après deux points (par défaut, le port est le 3389 pour une connexion RDP directe). **REMARQUE :** L'URL d'alimentation de l'accès par Internet aux services de bureau à distance doit commencer par `https://`. Par défaut, il est ajouté automatiquement comme spécifié par la clé de Registre `rdWebFeedUrlPattern`, qui définit le modèle de l'URL.
Informations d'authentification	• **Utiliser les informations d'authentification unique** : Les informations d'authentification utilisées le sont également pour démarrer la connexion. • **Demander les informations d'identification au démarrage de la connexion** : Aucun composant d'information d'authentification n'est fourni au préalable. • **Utiliser un utilisateur, un mot de passe et/ou un domaine prédéfinis** : Tout ou partie des informations d'authentification est stockée et fournie pour la connexion.

Option	Description
	• **Utiliser une carte à puce prédéfinie** : La connexion est prévue pour être utilisée avec une carte à puce pour l'authentification.
Utilisateur	Le nom d'utilisateur de cette connexion
Mot de passe	Le mot de passe de cette connexion
Domaine	Le nom de domaine de cette connexion (facultatif)
Utiliser la passerelle RD	Active d'autres options de la passerelle RD, comme l'adresse de la passerelle, le port et les informations d'authentification
Server Probe	Lance Server Probe, qui peut être utilisé afin de déterminer quelles fonctions de RDP sont prises en charge par votre serveur RDP.

Service

Le tableau suivant décrit les paramètres disponibles sous la catégorie Service lors de la modification d'une connexion RDP.

Option	Description
Service	Permet de régler le service RDP à l'une des opérations suivantes : • **Ordinateur distant** : Lorsque vous utilisez ce service, une connexion RDP directe est créée à un ordinateur distant. Une application à distance ou un Shell alterné peut éventuellement être lancé lors de la connexion. Les options supplémentaires suivantes sont disponibles pour un service de l'ordinateur distant : – Si le **Mode** est réglé sur **Remote Application** (Application à distance), le champ **Application** spécifie le chemin d'accès de l'application à exécuter. – Si le **Mode** est réglé sur **Alternate Shell** (Shell alterné), le champ **Commande** spécifie la commande qui exécute l'application à exécuter dans le shell alterné. Par exemple, pour exécuter Microsoft® Word, entrez `Word.exe`. En cas de **Mode** défini sur **Alternate Shell** (Shell alterné), le champ **Directory** (Répertoire) spécifie le chemin du répertoire de travail du serveur pour les fichiers programme de l'application. Par exemple, le répertoire de travail de Microsoft Word est `C:\Program Files\Microsoft`. • **RD Web Access** : Lorsque vous utilisez ce service, une liste de ressources d'applications distantes est récupérée sur le serveur et présentée à l'utilisateur, et la connexion RDP réelle est lancée lorsqu'une ressource est sélectionnée. Les options supplémentaires suivantes sont disponibles pour l'accès Web aux RD (services bureau à distance) : – **Conserver la fenêtre de sélection de ressources ouverte** : Lorsque cette option est sélectionnée, les utilisateurs peuvent ouvrir plusieurs ressources simultanément dans la fenêtre de sélection de ressource. – **Démarrer automatiquement une ressource unique** : Lorsque cette option est sélectionnée, et s'il y a une seule ressource publiée, cette ressource se lance automatiquement lors de la connexion. – **Filtre de ressources** et **Navigateur d'alimentation Web** : Ces options peuvent être utilisées pour limiter les ressources à distance qui seront mises à la disposition de l'utilisateur dans la fenêtre de sélection de ressource. – **Délai d'attente de déconnexion automatique** : Avec cette option sélectionnée, vous pouvez définir la durée qu'une connexion d'accès Web peut être maintenue avant qu'elle soit automatiquement fermée comme mesure de sécurité.

Option	Description
	REMARQUE : Un avantage de l'utilisation de l'accès par internet aux RD est qu'il gère les détails des connexions acquises et l'URL d'équilibre de charge automatiquement. Pour plus d'informations à ce sujet, consultez le livre blanc HP ThinPro *RD Web Access Deployment Example* (disponible en anglais uniquement).

Window (Fenêtre)

Le tableau suivant décrit les paramètres disponibles sous la catégorie Window (Fenêtre) lors de la modification d'une connexion RDP.

Option	Description
Masquer la décoration de fenêtre	Ce paramètre permet de s'assurer que des éléments à l'écran, tels que la barre de menus, les options de réduction et de fermeture, et les bordures du volet de fenêtre, ne sont pas affichés.
Dimension de la fenêtre	Définit la taille de la fenêtre sur **plein écran**, **taille fixe** ou **pourcentage**.
Taille en pourcentage	Si **Dimension de la fenêtre** est défini sur **pourcentage**, cette option définit le pourcentage de l'écran occupé par une fenêtre du bureau. **REMARQUE :** La taille qui en résulte peut être arrondie. **REMARQUE :** RemoteFX ne prend en charge qu'un nombre de résolutions bien défini.
Taille fixe	Si **Dimension de la fenêtre** est défini sur **taille fixe**, cette option définit la largeur et la hauteur en pixels qu'occupe la fenêtre du bureau.

Options

Le tableau suivant décrit les paramètres disponibles sous la catégorie Options lors de la modification d'une connexion RDP.

Option	Description
Activer les évènements de mouvement	Si cette option est activée, les déplacement de la souris sont transmis en permanence au serveur RDP.
Activer la compression des données	Active la compression de masse des données entre le serveur RDP et le client.
Activer le cryptage RDP obsolète	Active le cryptage RDP de dernière génération lorsque NLA n'est pas disponible.
Activer le cache hors écran	Si cette option est activée, la mémoire en dehors de l'écran est utilisée pour mettre en cache les bitmaps.
Joindre à la console d'administration	Associe la connexion au port de la console administrateur.
Copier/coller l'intersession	Si cette option est activée, le copier-coller est activé entre les différentes sessions RDP.
Activer la mise en mémoire tampon des primitives RDP6	Si cette fonction est activée, les performances graphiques non RemoteFX sont augmentées au coût des mises à jour d'écran les moins fréquentes.
Activer le codec Progressive RemoteFX	Active le codec Progressive RemoteFX, qui transmet le bureau sous forme d'une série d'images de plus en plus nettes. **REMARQUE :** Ce codec peut provoquer des artefacts visuels sur les bureaux présentant du contenu hautement dynamique, c'est pourquoi il peut être désactivé, si nécessaire.

Option	Description
Enable Multimedia Redirection (Activer la redirection multimédia)	Permet aux fichiers multimédia d'être envoyés directement vers le client pour une lecture locale.
Politique de vérification de certificat	Sélectionnez l'une des opérations suivantes : • **Accepter tous les certificats de serveur RDP** • **Utiliser les hôtes en mémoire ; avertir en cas de certificat invalide ou inconnu** • **Passer les hôtes en mémoire ; avertir en cas de certificat invalide ou inconnu** • **Se connecter uniquement à des serveurs RDP pré-approuvés**
Version du TLS	Définit la version TLS (Transport Layer Security) à utiliser au cours des étapes initiales de négociation avec le serveur RDP. Définissez cette option sur la version TLS utilisée par votre serveur RDP ou essayez de la régler sur **auto**. **REMARQUE :** Il existe certains défauts côté serveur sur des serveurs RDP auxquels les correctifs n'ont pas été appliqués, susceptibles de provoquer l'échec de la valeur auto, c'est pourquoi il ne s'agit pas de la valeur par défaut.
Envoyer le nom d'hôte en tant que	Pour l'attribution de licence par périphérique, ceci détermine comment le nom d'hôte du client est envoyé au serveur RDP. Sélectionnez **nom d'hôte** ou **mac**.
Nom d'hôte à envoyer	Généralement, le nom d'hôte du client léger est utilisé pour les licences d'accès Client. Ce champ permet d'envoyer une autre valeur. **CONSEIL :** Sélectionnez l'icône **(i)** en regard de cette option pour plus d'informations.
Information sur la répartition des charges	Utilisez cette option avec une connexion RDP via Broker. **CONSEIL :** Sélectionnez l'icône **(i)** en regard de cette option pour plus d'informations.

REMARQUE : Pour plus d'informations sur les options **Enable deprecated RDP encryption** (Activer le chiffrement RDP obsolète) et **TLS Version** (Version TLS), consultez le livre blanc HP ThinPro *Security Layers for RDP Connections* (disponible en anglais uniquement).

Ressources locales

Le tableau suivant décrit les paramètres disponibles sous la catégorie Ressources locales lors de la modification d'une connexion RDP.

REMARQUE : HP recommande une redirection des périphériques de haut niveau pour tous les périphériques locaux, sauf si une raison spécifique justifie plutôt l'utilisation de la redirection USB (USBR). Pour plus d'informations à ce sujet, consultez le livre blanc HP ThinPro *USB Manager* (disponible en anglais uniquement).

Option	Description
Périphériques audio	Détermine si les périphériques audio sont redirigés par la redirection audio RDP de haut niveau, la redirection USB de bas niveau, ou s'ils sont désactivés pour cette connexion.
Imprimantes	Détermine si les imprimantes sont redirigées par la redirection d'imprimante de haut niveau (qui exige qu'elles soient configurées dans l'outil Imprimantes du Panneau de configuration), la redirection USB de bas niveau, si elles sont désactivées pour cette connexion.
Ports série/parallèle	Détermine si les ports série et parallèle sont redirigés ou désactivés pour cette connexion.

Option	Description
Stockage USB	Détermine si les périphériques de stockage USB, tels que les unités flash USB et optiques, sont redirigés par la redirection de stockage de haut niveau, la redirection USB de bas niveau, ou s'ils sont désactivés pour cette connexion.
Partitions locales	Détermine si les partitions locales de l'unité flash USB du client léger sont redirigées ou désactivées pour cette connexion.
Cartes Smart Card	Détermine si les cartes à puce sont redirigées par la redirection de carte à puce de haut niveau ou désactivées pour cette connexion. **REMARQUE :** Lorsque le paramètre **Utiliser la carte à puce prédéfinie** est activé, ce paramètre est désactivé.
Other USB Devices (Autres périphériques USB)	Détermine si d'autres classes de périphériques USB (tels que les webcams et tablettes) sont redirigées par la redirection USB de bas niveau ou désactivées pour cette connexion.

Expérience

Le tableau suivant décrit les paramètres disponibles sous la catégorie Expérience lors de la modification d'une connexion RDP.

Option	Description
Choisir votre vitesse de connexion pour optimiser les performances	Le choix d'une vitesse de connexion entre **LAN**, **Large bande** et **Modem** active ou désactive les options suivantes pour optimiser les performances : • **Arrière-plan de l'ordinateur** • **Lissage des polices** • **Composition du Bureau** • **Afficher le contenu de la fenêtre pendant le déplacement** • **Animation du menu et de la fenêtre** • **Thèmes** Le choix de l'option **Paramètres préférés du client** permet au client RDP de choisir les options qui offriront la meilleure expérience RDP. Vous pouvez également sélectionner votre propre combinaison personnalisée d'options.
Surveillance de l'état de la connexion de bout en bout	Sélectionnez cette option pour activer les options de délai. **REMARQUE :** Pour plus d'informations à ce sujet, consultez le livre blanc HP ThinPro *RDP Connection Drop Detection* (disponible en anglais uniquement).
Délai d'avertissement	Spécifie la durée en secondes au terme de laquelle l'utilisateur est averti d'une perte de connexion après avoir reçu le dernier trafic réseau en provenance du serveur. Cette fonction peut être désactivée en effaçant l'option ou en définissant la durée sur zéro. Lorsque l'option **Afficher la boîte de dialogue d'avertissement** est sélectionnée, une boîte de dialogue d'avertissement s'affiche lorsque ce délai est atteint. Dans le cas contraire, l'avertissement est inscrit dans le journal de connexion uniquement. **CONSEIL :** HP vous recommande d'augmenter le délai pour les réseaux qui rencontrent fréquemment des périodes chargées ou des pannes momentanées.

Option	Description
Délai de reprise	Spécifie la durée en secondes pendant laquelle le client RDP attend que la connexion se rétablisse sans action particulière après avoir reçu le dernier trafic réseau en provenance du serveur. À la fin de cette période, le client RDP tente une rapide reconnexion avec la session.
Délai d'erreur	Spécifie la durée en secondes pendant laquelle le client RDP attend avant d'arrêter les tentatives de reconnexion au serveur après avoir reçu le dernier trafic réseau en provenance du serveur.

Diagnostics

Le tableau suivant décrit les paramètres disponibles sous la catégorie Diagnostics lors de la modification d'une connexion RDP.

Ces fonctionnalités diagnostiquent des problèmes spécifiques et sont désactivées par défaut.

Option	Description
Afficher le tableau de bord RDP	Si cette option est activée, le tableau de bord RDP est affiché pendant la connexion. **CONSEIL :** Sélectionnez l'icône **(i)** en regard de cette option pour plus d'informations.
Visualiser le graphique affichant l'état de santé de la connexion	Lorsque cette option est activée, un graphique en deux dimensions du temps de réponse du serveur RDP s'affiche lorsque la connexion est lancée. **CONSEIL :** Sélectionnez l'icône **(i)** en regard de cette option pour plus d'informations.
Analyse de la redirection USB	Cette fonction détermine et affiche la méthode actuelle de la redirection de chaque périphérique USB redirigé. **CONSEIL :** Sélectionnez l'icône **(i)** en regard de cette option pour plus d'informations.
X11 synchrone	Force le nettoyage fréquent des tampons X11 au détriment des performances.
Consignation	Active le fichier journal X11. Sélectionnez l'option **Autoflush** (Nettoyage automatique) pour augmenter la fréquence de la sortie de consignation au détriment des performances.
Capture	Autorise la capture et la lecture d'une sortie X11 à partir d'une session.

Avancé

REMARQUE : Reportez-vous à la section Paramètres de connexion avancés à la page 11 pour plus d'informations sur les paramètres disponibles dans la catégorie Avancé lors de la modification d'une connexion.

RemoteFX

RemoteFX est un protocole d'affichage graphique avancé conçu pour remplacer les composants graphiques du protocole RDP traditionnel. Il utilise les capacités d'accélération matérielle du processeur graphique du serveur pour coder les contenus d'écran via le codec RemoteFX et envoyer des mises à jour de l'écran au client RDP. RemoteFX utilise des technologies de recouvrement avancées et des graphismes adaptatifs, afin de s'assurer qu'il offre la meilleure expérience possible en fonction de type de contenu, de la CPU et de la disponibilité de bande passante de réseau et vitesse de rendu.

RemoteFX est activé par défaut. L'administrateur ou utilisateur n'a pas besoin de modifier les paramètres pour l'activer. Le client RDP négocie avec chaque serveur RDP qu'il contacte et RemoteFX est utilisé en cas de disponibilité.

REMARQUE : Pour plus d'informations à ce sujet, consultez le livre blanc HP ThinPro *Enabling RemoteFX for RDP* (disponible en anglais uniquement).

Sessions RDP multi-écrans

La prise en charge de plusieurs moniteurs ne nécessite pas de configuration spéciale. Le client RDP identifie automatiquement le moniteur spécifié comme moniteur principal dans les paramètres locaux et place les icônes de la barre des tâches et du bureau sur ce moniteur. Lorsqu'une fenêtre est agrandie dans la session à distance, la fenêtre couvre uniquement le moniteur sur lequel elle a été agrandie.

Les préférences d'affichage et les résolutions des moniteurs peuvent être affichées mais elles ne peuvent pas être modifiées dans la session à distance. Pour modifier la résolution de la session, fermez la session et modifiez la résolution sur le client léger local.

Par défaut, toutes les sessions RDP sont affichées en plein écran et couvrent tous les moniteurs pour une meilleure expérience de virtualisation. D'autres options de fenêtre sont disponibles dans le gestionnaire de connexion RDP.

REMARQUE : Les sessions de l'hôte de virtualisation des services Bureau à distance (RDVH) avec prise en charge des cartes graphiques sont susceptibles de prendre en charge un nombre limité de résolutions et d'écrans. Les limites sont spécifiées lorsque le périphérique graphique virtuel RemoteFX est configuré pour la machine virtuelle RDVH.

REMARQUE : Pour plus d'informations sur les sessions RDP multi-écrans, consultez le livre blanc *True Multi-Monitor Mode for RDP* (disponible en anglais uniquement).

Redirection multimédia RDP

La redirection multimédia (MMR) est une technologie intégrée à Windows Media Player sur l'hôte distant qui diffuse les contenus multimédias codés vers le client RDP au lieu de les lire sur l'hôte distant et de les recoder via RDP. Cette technologie réduit la charge du serveur et le trafic réseau, et améliore nettement l'expérience multimédia, en prenant en charge la lecture 24 ips des vidéos 1080p avec synchronisation automatique du son. MMR est activée par défaut. Un client RDP négocie avec chaque serveur RDP qu'il contacte et MMR est utilisée en cas de disponibilité.

MMR utilise également un schéma avancé de détection des codecs qui identifie si le client léger prend en charge le codec demandé par l'hôte distant avant de tenter de le rediriger. Le résultat est que seuls les codecs pris en charge sont redirigés alors que tous les codecs non pris en charge retombent sur les rendus côté serveur.

CONSEIL : Par souci de simplification de gestion, HP recommande que MMR soit activée ou désactivée sur l'hôte distant.

Redirection des périphériques RDP

La redirection du périphérique permet de s'assurer que lorsqu'un utilisateur branche un périphérique sur le client léger, ledit périphérique est automatiquement détecté et accessible dans la session à distance. RDP prend en charge la redirection de nombreux types différents de périphériques.

Redirection USB RDP

La redirection USB fonctionne par transmission d'appels de protocole USB de bas niveau sur le réseau à l'hôte distant. N'importe quel périphérique USB branché sur l'hôte local apparaît dans l'hôte distant comme un périphérique USB natif, comme s'il était branché au niveau local. Les pilotes Windows standards prennent en charge le périphérique dans la session à distance, et tous les types de périphériques sont pris en charge sans nécessiter de pilote supplémentaire sur le client léger.

Certains périphériques n'effectuent pas la redirection USB par défaut. Par exemple, les claviers, souris et autres périphériques d'entrée USB ne sont généralement pas configurés pour la redirection, car la session à distance s'attend à ce que l'entrée provienne du client léger. Certains périphériques tels que les périphériques de stockage de masse, les imprimantes et les périphériques audio peuvent utiliser des options supplémentaires pour la redirection.

Tenez compte de ces informations supplémentaires sur la redirection USB avec RDP :

- Le serveur doit être compatible avec la redirection USB pour qu'elle soit disponible pour le client léger. La redirection USB à usage général est compatible avec les serveurs RDVH équipés de RemoteFX, Windows 8, Windows 10, Windows Server 2012 et Windows Server 2016.
- Le protocole dans le gestionnaire USB du Panneau de configuration doit être configuré sur RDP.
- Pour les connexions RDP, les commandes du gestionnaire USB déterminent si un périphérique USB est redirigé. Les paramètres de la connexion déterminent comment un périphérique USB est redirigé.

Redirection de stockage de masse RDP

Par défaut, la session RDP redirige tous les périphériques de mémoire de grande capacité vers l'hôte distant à l'aide de la redirection de lecteur de haut niveau. Lorsqu'un appareil tel qu'un lecteur flash USB, un lecteur DVD-ROM USB ou un disque dur externe USB est branché sur le client léger, le client léger détecte et monte l'unité sur le système de fichiers local. Ensuite, RDP détecte un lecteur monté et le redirige vers l'hôte distant. Dans l'hôte distant, il apparaîtra comme une nouvelle unité de disque dans l'Explorateur Windows, avec le nom `< étiquette périphérique > sur < nom d'hôte du client >`; par exemple, `paul_usb sur HP04ab598100ff`.

Il existe trois restrictions à ce type de redirection.

- Le périphérique ne s'affiche pas dans la barre des tâches de l'hôte distant avec une icône permettant son éjection. De ce fait, assurez-vous de laisser au périphérique suffisamment de temps pour synchroniser les données après une copie avant de le retirer. Cette procédure évite la corruption du périphérique. En général, il faut moins d'une seconde après la fermeture de la boite de dialogue de copie de fichier. Toutefois, jusqu'à 10 secondes peuvent s'avérer nécessaires en fonction de la vitesse d'écriture du périphérique et de la latence du réseau.
- Seuls les systèmes de fichiers pris en charge par le client léger peuvent être montés. Les systèmes de fichiers pris en charge sont FAT32, NTFS ISO9660 (CD-ROM), UDF (DVD-ROM) et ext3.
- Le périphérique est traité comme un répertoire ; les tâches courantes relatives au lecteur comme le formatage et la modification de l'étiquette du disque ne sont pas disponibles.

La redirection USB des périphériques de stockage peut être désactivée dans les paramètres d'une connexion. Si vous le souhaitez, vous pouvez désactiver entièrement la redirection du stockage de masse. Pour cela, désactivez la redirection USB, puis modifiez les clés de registre comme décrit dans le tableau suivant.

Entrée de registre	Valeur à établir	Description
root/USB/root/holdProtocolStatic	1	Garantit que le type d'USBR n'est pas modifié automatiquement lorsqu'une connexion est établie ou arrêtée
root/USB/root/protocol	local	Garantit que la connexion RDP ne tente pas de rediriger un quelconque périphérique vers la session à distance

Pour désactiver complètement le montage local de périphériques de stockage de masse USB ou pour désactiver la redirection des périphériques de stockage de masse USB mais toujours autoriser les autres périphériques à rediriger, dans le système de fichiers de client léger, supprimer la règle udev `/etc/udev/rules.d/010_usbdrive.rules`.

Redirection d'imprimante USB

Par défaut, RDP dispose de deux méthodes de redirection d'imprimante :

- **Redirection USB** : Toute imprimante USB branchée sur l'appareil apparait en tant qu'imprimante locale au sein de la session à distance. Le processus d'installation de l'imprimante standard doit se produire dans la session à distance si l'imprimante n'est pas déjà installée sur l'hôte distant. Il n'y a aucun paramètre à gérer localement.
- **Redirection de haut niveau** : Si la redirection USB n'est pas disponible sur l'hôte distant ou si l'imprimante est une imprimante série ou parallèle, utilisez une redirection de haut niveau. Configurez l'imprimante pour utiliser un spooler d'impression local, et le client RDP configurera automatiquement une imprimante distante qui enverra des commandes d'impression par le biais d'un canal virtuel, depuis l'hôte distant vers le client léger.

  Un pilote postscript générique est utilisé si aucun pilote n'est spécifié, mais d'autres fonctionnalités supplémentaires de l'imprimante peuvent être disponibles si l'imprimante est configurée localement avec un pilote Windows spécifique. Ce pilote Windows doit correspondre au pilote que l'imprimante utiliserait si elle était localement raccordée à un système d'exploitation Windows. Ces informations peuvent habituellement être trouvées dans l'onglet **Modèle** dans les propriétés de l'imprimante.

REMARQUE : Consultez la section Configuration d'une imprimante série ou parallèle à la page 77 pour en savoir plus.

Redirection audio RDP

Par défaut, la redirection audio de haut niveau redirige les flux audio de l'hôte distant vers le client léger. Il est possible que vous deviez configurer un contrôle vocal de base et RDP 7.1 contient un certain nombre de fonctions avancées de redirection audio qui peuvent nécessiter une configuration supplémentaire.

Reportez-vous aux notes suivantes sur l'utilisation de la redirection audio avec RDP :

- RDP offre la meilleure qualité audio que la bande passante du réseau permet. RDP réduit la qualité audio dans le cas d'une lecture avec une connexion à faible bande passante.
- Aucun mécanisme natif de synchronisation audio ou vidéo standard n'est disponible avec le RDP standard. Les vidéos longues sont susceptibles de ne pas se synchroniser avec l'audio. MMR ou RemoteFX peuvent résoudre ce problème.
- HP recommande la redirection audio de haut niveau, mais la redirection USB des périphériques audio est possible si des fonctions supplémentaires sont présentes, telles que le contrôle du volume numérique. Seule la redirection de haut niveau est disponible pour les périphériques analogiques.

- La redirection du microphone est activée par défaut. Il peut être nécessaire de régler le volume du microphone par défaut sur le client léger. Les paramètres des serveurs Windows RDP plus anciens doivent être modifiés pour permettre une entrée audio.
- Les paramètres de volume locaux et distants affectent tous deux le volume final. HP recommande de paramétrer le volume local au niveau maximum et de régler le volume sur l'hôte distant.

Redirection de carte Smart Card RDP

Par défaut, les cartes Smart Card sont redirigées à l'aide de la redirection de haut niveau, ce qui leur permet d'être utilisées pour l'ouverture de session et d'autres applications distantes.

Pour activer l'ouverture de session par carte Smart Card pour une connexion RDP :

▲ Sélectionnez **Utiliser la carte à puce prédéfinie** dans le RDP Connection Manager (Gestionnaire de connexions RDP).

Cette opération permet à l'utilisateur de se connecter sans entrer au préalable ses informations d'authentification. Le client RDP démarre la session RDP et l'utilisateur est invité à s'authentifier par carte Smart Card.

Cette technologie nécessite que les pilotes pour le pilote de lecteur de carte Smart Card soient installés sur le client léger. Par défaut, les pilotes CCID et Gemalto sont installés, ce qui ajoute un support pour la majorité des lecteurs de carte Smart Card disponibles. Des pilotes supplémentaires peuvent être installés en les ajoutant à `/usr/lib/pkcs11 /`.

REMARQUE : Lorsque l'identification par carte Smart Card est activée, l'authentification au niveau du réseau n'est pas prise en charge et est automatiquement désactivée.

VMware Horizon View

Paramètres VMware Horizon View par connexion

REMARQUE : Ces paramètres affectent uniquement la connexion que vous configurez.

Réseau

Le tableau suivant décrit les paramètres disponibles sous la catégorie Réseau lors de la modification d'une connexion VMware Horizon View.

Option	Description
Nom	Entrez le nom de cette connexion.
Adresse	Entrez le nom d'hôte ou l'adresse IP d'un serveur VMware Horizon View.
Informations d'authentification	• **Connectez-vous anonymement en utilisant un accès non authentifié** • **Utiliser les informations d'authentification unique** : Les informations d'authentification utilisées le sont également pour démarrer la connexion. • **Demander les informations d'identification au démarrage de la connexion** : Aucun composant d'information d'authentification n'est fourni au préalable. • **Utiliser un utilisateur, un mot de passe et/ou un domaine prédéfinis** : Tout ou partie des informations d'authentification est stocké et fourni pour la connexion. • **Utiliser une carte à puce prédéfinie** : La connexion est prévue pour être utilisée avec une carte à puce pour l'authentification.

Option	Description
Utilisateur	Entrez le nom d'utilisateur à utiliser pour la connexion.
Mot de passe	Entrez le mot de passe à utiliser pour la connexion.
Domaine	Entrez le domaine à utiliser pour la connexion.

Général

Le tableau suivant décrit les paramètres disponibles sous la catégorie Général lors de la modification d'une connexion VMware Horizon View.

Option	Description
Activer MMR	Permet la redirection multimédia pour BLAST et les connexions PCoIP. **REMARQUE :** HP vous recommande de désactiver cette option. Pour les connexions effectuées avec le protocole RDP, utilisez l'option Enable Multimedia Redirection. Reportez-vous à la section Options RDP à la page 30.
Activer la connexion automatique USB à l'insertion	Activer la redirection de périphérique USB lorsqu'un périphérique USB est inséré.
Activer la connexion automatique USB au démarrage	Activer la redirection de périphérique USB lorsqu'une connexion VMware View démarre.
Envoyer Ctrl + Alt + Suppr au bureau virtuel	Activer envoyer directement Ctrl + Alt + Suppr vers le bureau virtuel.
Permettre le partage de données Horizon Client	Si votre administrateur Horizon a choisi de participer au programme d'amélioration de l'expérience client, VMware collecte et reçoit des données anonymes sur les systèmes clients afin de hiérarchiser la compatibilité matérielle et logicielle.
Activer la redirection du lecteur client	Permet la fonctionnalité de dossier partagé pour BLAST et les connexions PCoIP. Cette option est activée par défaut.
Ne pas démarrer l'application en grand	Si activée, les applications ne démarrent pas dans des fenêtres agrandies.
Connexion automatique	Lorsque cette option est activée, la session de l'utilisateur est automatiquement ouverte lorsque la connexion est établie. **REMARQUE :** HP vous recommande d'activer cette option.
Pack de virtualisation pour Skype for Business	Permet la virtualisation de Skype pour les professionnels. **REMARQUE :** Les appels vidéo peuvent utiliser la plupart de la capacité de traitement d'un client léger. HP vous recommande de désactiver cette option.
Bureau par défaut	Spécifie un bureau pour démarrer automatiquement lorsqu'une connexion VMware Horizon View est lancée.
Preferred Protocol (Protocole favori)	Permet de sélectionner PCoIP, RDP ou BLAST comme protocole favori ou de choisir une sélection ultérieure du protocole.
Application Size (Taille de l'application)	Permet de régler la taille de la fenêtre d'application. Vous pouvez sélectionner **All Monitors** (Tous les écrans), **Full Screen** (Plein écran), **Large Window** (Grande fenêtre) ou **Small Window** (Petite fenêtre).
Taille du bureau	Permet de régler la taille de la fenêtre du bureau. Vous pouvez sélectionner **All Monitors** (Tous les écrans), **Full Screen** (Plein écran), **Large Window** (Grande fenêtre) ou **Small Window** (Petite fenêtre).
imprimantes	Contrôle comment la redirection d'imprimante locale est traitée : • **ThinPrint** : Partage les imprimantes à l'aide de la redirection de haut niveau.

Option	Description
	• **USB Redirection (Redirection USB)** • **Désactiver** **REMARQUE :** Pour les connexions effectuées avec le protocole RDP, reportez-vous à la section Redirection d'imprimante USB à la page 27.

Sécurité

Le tableau suivant décrit les paramètres disponibles sous la catégorie Sécurité lors de la modification d'une connexion VMware Horizon View.

Option	Description
Fermer après déconnexion	Entraîne la fermeture automatique du client VMware Horizon View lorsque les utilisateurs se déconnectent de leurs bureaux ou lorsque la session prend fin en raison d'une erreur. Cette option est une fonction de sécurité conçue afin qu'un utilisateur n'ait pas besoin d'effectuer d'action supplémentaire pour se déconnecter entièrement une fois sa session de bureau terminée. Cette option est activée par défaut pour des raisons de sécurité, mais elle peut être désactivée si les utilisateurs constatent qu'ils basculent souvent vers un nouveau pool de bureaux après une fermeture de session et ne souhaitent pas se reconnecter entièrement.
Masquer la barre de menus supérieure	Permet de masquer la barre de menus supérieure aux utilisateurs. Cette option est activée par défaut. Désactivez-la si les utilisateurs préfèrent accéder aux options de la taille de fenêtre ou de sélection du pool de bureaux dans une session VMware Horizon View.
Empêcher les utilisateurs de changer l'adresse du serveur	Si cette option est activée, les utilisateurs finaux ne peuvent pas modifier l'adresse du serveur.
Activer le moniteur d'itinérance de session	Ferme la connexion si la session est en itinérance depuis un autre client. Cette option est supportée uniquement sur les connexions PCoIP.
Politique de vérification de certificat	Sélectionnez l'une des opérations suivantes : • **Autoriser toutes les connexions** • **Avertir** • **Refuser les connexions non sécurisées**

Options RDP

Le tableau suivant décrit les paramètres disponibles sous la catégorie Options RDP lors de la modification d'une connexion VMware Horizon View.

Option	Description
Envoyer les événements de mouvement de la souris	Autorise les événements de déplacement pour cette connexion.
Activer la compression de données	Utilise la compression des données pour cette connexion.
Activer le cryptage RDP obsolète	Active le cryptage pour cette connexion.

Option	Description
Autoriser le cache hors champ	Si cette option est activée, la mémoire en dehors de l'écran est utilisée pour mettre en cache les bitmaps.
Ajouter à la console d'administration	Associe la connexion au port de la console administrateur.
Copier/coller sur plusieurs sessions	Si cette option est activée, le copier-coller est activé entre les différentes sessions RDP.
Activer la mise en tampon de primitives RDP6	Si cette fonction est activée, les performances graphiques non RemoteFX sont augmentées au coût des mises à jour d'écran les moins fréquentes.
Activer le codec Progressive RemoteFX	Active le codec Progressive RemoteFX, qui transmet le bureau sous forme d'une série d'images de plus en plus nettes.
Enable Multimedia Redirection (Activer la redirection multimédia)	Permet aux fichiers multimédia d'être envoyés directement vers le client pour une lecture locale. Pour plus d'informations, voir Redirection multimédia RDP à la page 25.
Version du TLS	Définit la version TLS (Transport Layer Security) à utiliser au cours des étapes initiales de négociation avec le serveur RDP. Définissez cette option sur la version TLS utilisée par votre serveur RDP ou essayez de la régler sur **auto**. **REMARQUE :** Il existe certains défauts côté serveur sur des serveurs RDP auxquels les correctifs n'ont pas été appliqués, susceptibles de provoquer l'échec de la valeur auto, c'est pourquoi il ne s'agit pas de la valeur par défaut.
Envoyer le nom d'hôte en tant que	Pour l'attribution de licence par périphérique, ceci détermine comment le nom d'hôte du client est envoyé au serveur RDP. Sélectionnez **nom d'hôte** ou **mac**.
Nom d'hôte à envoyer	Généralement, le nom d'hôte du client léger est utilisé pour les licences d'accès Client. Ce champ permet d'envoyer une autre valeur. **CONSEIL :** Sélectionnez l'icône **(i)** en regard de cette option pour plus d'informations.
Information sur la répartition des charges	Utilisez cette option avec une connexion RDP via Broker. **CONSEIL :** Sélectionnez l'icône **(i)** en regard de cette option pour plus d'informations.
Son de l'ordinateur distant	Spécifie l'emplacement où doit être lu le son de l'ordinateur distant (à distance ou localement) ou s'il ne doit pas être lu du tout.
Activer le mappage de port	Permet de mapper les ports série et parallèles du client léger à la session à distance.
Activer le mappage des imprimantes	Permet de mapper la file d'impression locale à la session distante. Utilisez cette option si la redirection USB n'est pas disponible sur l'hôte distant ou si l'imprimante est une imprimante série ou parallèle. Configurez l'imprimante pour utiliser un spooler local, et le client VMware Horizon View configurera automatiquement une imprimante distante qui enverra des commandes d'impression par le biais d'un canal virtuel, depuis l'hôte distant vers le client léger. Cette méthode nécessite à la fois que l'imprimante soit configurée sur le client léger, et qu'un pilote Windows soit spécifié sur le client léger car le client VMware Horizon View doit indiquer à l'hôte distant quel pilote il convient d'utiliser pour l'imprimante distante. Ce pilote Windows doit correspondre au pilote que l'imprimante utiliserait si elle était localement raccordée à un système d'exploitation Windows. Ces informations peuvent habituellement être trouvées dans l'onglet **Modèle** dans les propriétés de l'imprimante.
Dossiers partagés	Pour **Ajouter**, **Supprimer** ou **Modifier** des dossiers partagés.

RDP Experience (Expérience RDP)

Le tableau suivant décrit les paramètres disponibles sous la catégorie RDP Experience (Expérience RDP) lors de la modification d'une connexion VMware Horizon View.

Option	Description
Choisissez votre vitesse de connexion afin d'optimiser les performances	Le choix d'une vitesse de connexion entre **LAN**, **Large bande** et **Modem** active ou désactive les options suivantes pour optimiser les performances : • **Arrière-plan du bureau** • **Lissage des polices** • **Composition du Bureau** • **Afficher le contenu de la fenêtre pendant le déplacement** • **Animation du menu et de la fenêtre** • **Thèmes** Le choix de l'option **Paramètres préférés du client** permet au client VMware Horizon View de choisir les options à utiliser. Vous pouvez également sélectionner votre propre combinaison personnalisée d'options.
Surveillance de l'état de la connexion de bout en bout	Sélectionnez cette option pour activer les options de délai.
Délai d'avertissement	Spécifie la durée en secondes au terme de laquelle l'utilisateur est averti d'une perte de connexion après avoir reçu le dernier trafic réseau en provenance du serveur. Cette fonction peut être désactivée en effaçant l'option ou en définissant la durée sur zéro. Lorsque l'option **Afficher la boîte de dialogue d'avertissement** est sélectionnée, une boîte de dialogue d'avertissement s'affiche lorsque ce délai est atteint. Dans le cas contraire, l'avertissement est inscrit dans le journal de connexion uniquement. **CONSEIL :** HP vous recommande d'augmenter le délai pour les réseaux qui rencontrent fréquemment des périodes chargées ou des pannes momentanées.
Délai de reprise	Spécifie la durée en secondes pendant laquelle le client RDP attend que la connexion se rétablisse sans action particulière après avoir reçu le dernier trafic réseau en provenance du serveur. À la fin de cette période, le client RDP tente une rapide reconnexion avec la session.
Délai d'erreur	Spécifie la durée en secondes pendant laquelle le client RDP attend avant d'arrêter les tentatives de reconnexion au serveur après avoir reçu le dernier trafic réseau en provenance du serveur. **CONSEIL :** Sélectionnez l'icône **?** en regard de ce champ pour plus d'informations.

Avancé

REMARQUE : Reportez-vous à la section Paramètres de connexion avancés à la page 11 pour plus d'informations sur les paramètres disponibles dans la catégorie Avancé lors de la modification d'une connexion.

Sessions multi-écrans VMware Horizon View

VMware Horizon View prend en charge les sessions multi-moniteurs. Afin d'améliorer l'expérience de virtualisation, les sessions de VMware Horizon View utilisent par défaut le plein écran et s'étendent sur tous les moniteurs. Pour choisir une taille de fenêtre différente, sélectionnez **Full Screen – All Monitors** (Plein écran – Tous les écrans) sous le type de protocole du pool de bureaux de la connexion, puis sélectionnez une autre option dans la liste de dimensions de fenêtre. La prochaine fois que vous vous connecterez à une session, la fenêtre s'ouvrira dans la taille sélectionnée.

Raccourcis clavier VMware Horizon View

Raccourcis clavier Windows

Pour aider à administrer les systèmes Windows, VMware Horizon View prend en charge les raccourcis clavier Windows. Par exemple, lorsque Ctrl+Alt+Suppr est utilisé, VMware Horizon View affiche un message présentant les options suivantes :

- Envoyer une commande **Ctrl**+**Alt**+**Suppr**.
- Déconnecter la session : Utilisez cette option lorsque vous n'avez aucun autre moyen de mettre fin à la session.

Les raccourcis clavier Windows sont transmis à la session de bureau à distance. Par conséquent, les raccourcis clavier locaux, comme les touches Ctrl+Alt+Tabulation et Ctrl+Alt+F4, ne fonctionnent pas dans la session à distance.

CONSEIL : Pour pouvoir basculer entre les sessions, désactivez l'option **Masquer la barre de menus supérieure** dans le gestionnaire de connexion VMware Horizon View ou dans la clé de registre `root/ConnectionType/view/connections/<UUID>/hideMenuBar`.

Touches multimédias

VMware Horizon View utilise les touches multimédias pour contrôler des fonctions telles que le volume, la lecture, la mise en pause et le mode muet lors d'une session de bureau à distance. Cela permet de prendre en charge les programmes multimédias comme Windows Media Player.

Redirection des périphériques VMware Horizon View

Redirection USB VMware Horizon View

Pour activer USBR pour les connexions VMware Horizon View, sélectionnez **VMware Horizon View** comme protocole distant dans le gestionnaire USB.

Pour en savoir plus sur l'USBR, notamment la redirection spécifique à une classe ou à un périphérique, reportez-vous à Redirection USB RDP à la page 26.

Redirection audio VMware Horizon View

Si vous n'avez pas besoin de fonctions d'enregistrement audio, utilisez une redirection audio de qualité élevée. Les flux audio seront lus au moyen de la prise 3,5 mm ou, par défaut, des écouteurs USB branchés. Utilisez le gestionnaire audio local pour régler le niveau d'entrée/sortie et sélectionner la lecture et les périphériques de capture.

Le client VMware Horizon prend en charge une redirection d'enregistrement audio de haut niveau uniquement via le type de connexion PCoIP sur unités x86 lors de la connexion à un serveur exécutant VMware Horizon View 5.2 Feature Pack 2 ou version supérieure ou le type de connexion BLAST sur unités x86 lors de la connexion à un serveur exécutant VMware Horizon View 7.x ou version supérieure. Si vous avez besoin de la prise en charge des fonctions d'enregistrement audio et que vous utilisez une autre configuration, utilisez l'une des méthodes suivantes :

- Si votre système utilise le client VMware Horizon View Client 1.7 ou une version ultérieure, utilisez le protocole RDP pour permettre la redirection audio de qualité élevée au moyen de la prise audio 3,5 mm ou d'écouteurs USB.

REMARQUE : Pour utiliser la redirection d'enregistrement audio de qualité élevée via le protocole RDP, le serveur doit le prendre en charge et être configuré pour permettre l'enregistrement audio via une session distante. Le serveur doit fonctionner sous Windows 7 ou une version ultérieure. Vous devez également vous assurer que la clé de registre `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\fDisableAudioCapture` est définie sur `0`.

- Si vous disposez d'un casque USB avec microphone, vous pouvez utiliser USBR. Configurez la redirection du casque USB vers la session. Le casque s'affiche comme un périphérique audio. Par défaut, les périphériques audio USB ne sont pas redirigés et le client VMware Horizon View utilise la redirection audio de haut niveau. Pour rediriger le casque USB, utilisez le gestionnaire USB du client léger et sélectionnez le casque USB à rediriger. Vérifiez que **VMware Horizon View** est sélectionné comme protocole USBR et que le casque est sélectionné sous la rubrique des périphériques à rediriger.

REMARQUE : VMware et HP ne recommandent pas l'utilisation d'USBR pour les écouteurs. Une grande partie de la bande passante du réseau est nécessaire pour diffuser des données audio via le protocole USBR. Par ailleurs, une qualité sonore médiocre est possible avec cette méthode.

Redirection de carte Smart Card VMware Horizon View

Pour utiliser une carte Smart Card pour se connecter au serveur VMware Horizon View :

1. Assurez-vous que l'ouverture de session par carte Smart Card est activée dans le gestionnaire de connexion VMware Horizon View.

   Après le lancement de la connexion, le client VMware Horizon View affiche une liste d'informations d'authentification pour le serveur.

2. Pour déverrouiller les informations d'authentification et accéder au serveur VMware Horizon View, entrez le code PIN adéquat pour ce serveur.

REMARQUE : Une fois le code PIN correct fourni, les informations d'identification de l'utilisateur serviront à vous connecter au serveur de VMware Horizon View Manager. Reportez-vous à la documentation de VMware Horizon View pour en savoir plus sur comment configurer le serveur pour prendre en charge l'identification par carte Smart Card. Tant que le serveur est configuré pour autoriser l'identification par carte Smart Card, les informations d'authentification de l'utilisateur seront directement transmises et serviront à se connecter au bureau sans avoir de nouveau à saisir le code PIN.

REMARQUE : Pour vous connecter au serveur de l'administrateur de VMware Horizon View Manager avec une carte Smart Card, le pilote de carte Smart Card local doit être installé sur le client léger. Reportez-vous à la section Redirection de carte Smart Card RDP à la page 28 pour plus d'informations sur l'installation du pilote de carte Smart Card. Une fois connectée à l'hôte distant, la carte Smart Card sera transmise à l'hôte distant à l'aide d'un canal virtuel, pas l'USBR. Cette redirection par canal virtuel permet de s'assurer que la carte Smart Card peut être utilisée pour des tâches telles que la signature de courrier électronique, le verrouillage de l'écran, etc., mais il peut s'avérer, en conséquence, que la carte Smart Card ne s'affiche pas en tant que périphérique de carte Smart Card dans le gestionnaire de périphériques Windows.

REMARQUE : Les pilotes de carte Smart Card adéquats doivent être installés sur l'hôte distant.

Redirection de webcam VMware Horizon View

Le client VMware Horizon View prend en charge la redirection de webcam de haut niveau uniquement via RTAV sur les unités x86 connectés à un serveur principal sous VMware Horizon View 5.2 Feature Pack 2 ou une version ultérieure. D'autres méthodes de connexion ne prennent pas en charge la redirection de webcam de haut niveau et peuvent rediriger les webcams uniquement avec USBR. Des tests et validations effectués en interne ont permis à HP de déterminer que la connexion d'une webcam via le protocole USBR de base entraîne des problèmes de performance. HP ne recommande pas l'utilisation de cette configuration et conseille aux clients qui doivent utiliser cette fonction de tester les unités x86 avec la technologie RTAV pour bénéficier de

niveaux de performances satisfaisants. Avec USBR, la webcam peut mal fonctionner ou ne pas fonctionner du tout. Pour plus d'informations, reportez-vous à la section Redirection USB RDP à la page 26.

Redirection de port COM VMware Horizon View

Pour activer la redirection de port COM pour la connexion VMware horizon View :

▲ Définir `root/ConnectionType/view/general/enableComPortRedirection` à 1 dans regeditor.

REMARQUE : Par défaut, ce paramètre est activé.

Changement de protocole VMware Horizon View

Le client VMware Horizon View peut utiliser le protocole PCoIP, RDP, ou BLAST.

Pour changer de protocole :

1. Dans le client VMware Horizon View, sélectionnez un pool qui prend en charge un des protocoles pris en charge :
2. Dans le menu **Connection** (Connexion), sélectionnez **Settings** (Paramètres).
3. Modifiez le protocole à l'aide de la zone déroulante située en regard de **Connect Via** (Se connecter via).

REMARQUE : Utilisez VMware Horizon View Manager pour définir le protocole à utiliser pour chaque pool de bureaux.

CONSEIL : HP recommande d'utiliser le protocole PCoIP pour améliorer l'expérience de bureau. Cependant, le protocole RDP offre plus d'options de personnalisation et est susceptible de mieux fonctionner sur des connexions plus lentes.

Exigences de VMware Horizon View portant sur le HTTPS et la gestion des certificats

Les versions VMware Horizon View Client 1.5 et VMware Horizon View Server 5.0 et ultérieures nécessitent HTTPS. Par défaut, le client VMware Horizon View lance un avertissement en cas de certificat de serveur non reconnu, tel qu'un certificat autosigné (comme le certificat par défaut de VMware Horizon View Manager) ou un certificat périmé. Si un certificat est signé par une Autorité de certification (CA) et que la CA n'est pas reconnue, la connexion renvoie une erreur et l'utilisateur n'est pas autorisé à se connecter.

HP recommande d'utiliser un certificat signé vérifié par une CA racine standard reconnue avec le serveur de VMware Horizon View Manager. Cela permet de s'assurer que les utilisateurs pourront se connecter au serveur sans recevoir d'avertissement ou avoir à configurer quoi que ce soit. Si vous utilisez une CA interne, la connexion du client VMware Horizon View renvoie une erreur jusqu'à ce que vous réalisiez l'une des tâches suivantes :

- Utilisez Certificate Manager (Gestionnaire de certificats) pour importer le certificat en provenance d'un fichier ou d'une URL.
- Utilisez une mise à jour de profil à distance pour importer un certificat.
- Dans le gestionnaire de connexion VMware Horizon View, définissez **Niveau de sécurité de la connexion** sur **Autoriser toutes les connexions**.

Le tableau suivant décrit le degré confiance du certificat lorsque le niveau de sécurité est défini sur **Refuse insecure connections** (Refuser les connexions non sécurisées).

Confiance du certificat	Résultat
Certifié	Reconnu
Auto-signé	Erreur
Expiré	Erreur
Non certifié	Erreur

Le tableau suivant décrit le degré confiance du certificat lorsque le niveau de sécurité est défini sur **Warn** (Avertir).

Confiance du certificat	Résultat
Certifié	Reconnu
Auto-signé	Avertissement
Expiré	Avertissement
Non certifié	Erreur

Le tableau suivant décrit le degré confiance du certificat lorsque le niveau de sécurité est défini sur **Allow all connections** (Autoriser toutes les connexions).

Confiance du certificat	Résultat
Certifié	Reconnu
Auto-signé	Non reconnu
Expiré	Non reconnu
Non certifié	Non reconnu

Le tableau suivant décrit le comportement à la connexion associé à chaque résultat.

Résultat	Description
Reconnu	Connexion sans boite de dialogue d'avertissement et affichage d'une icône de verrouillage verte
Non reconnu	Connexion sans boite de dialogue d'avertissement et affichage d'une icône de déverrouillage rouge
Avertissement	Connexion avec une boite de dialogue d'avertissement et affichage d'une icône de déverrouillage rouge
Erreur	Ne permet pas la connexion

Navigateur Web

Paramètres de navigateur Web par connexion

REMARQUE : Ces paramètres affectent uniquement la connexion que vous configurez.

Configuration

Le tableau suivant décrit les paramètres disponibles sous la catégorie Configuration lors de la modification d'une connexion de navigateur Web.

Option	Description
Nom	Le nom de la connexion.
URL	L'URL de la connexion.
Utilisation prévue	Vous permet de spécifier comment la redirection USB est effectuée lorsque la connexion Web Browser démarre. Sélectionnez **Citrix**, **RDP** ou **Internet**.
Autoriser la connexion par carte à puce	Vous permet d'utiliser l'authentification par carte à puce pour une connexion si vous sélectionnez une URL ou une icône qui démarre une connexion distante.
Activer le mode kiosque	Active le mode kiosque.
Activer le plein écran	Utilise le mode plein écran pour la connexion.
Activer la boîte de dialogue d'impression	Active la boîte de dialogue d'impression.

Préférences

Utilisez ces options pour configurer la connexion Web Browser. Ces options peuvent être partagées par plusieurs connexions Web Browser ou être spécifiques à une seule connexion.

Avancé

REMARQUE : Reportez-vous à la section Paramètres de connexion avancés à la page 11 pour plus d'informations sur les paramètres disponibles dans la catégorie Avancé lors de la modification d'une connexion.

Types de connexions supplémentaires (ThinPro uniquement)

REMARQUE : Par défaut, ces types de connexion ne sont pas disponibles dans Smart Zero. Pour plus d'informations, reportez-vous à la section Choix d'une configuration OS à la page 1.

XDMCP

REMARQUE : Ces paramètres affectent uniquement la connexion que vous configurez.

Configuration

Le tableau suivant décrit les paramètres disponibles sous la catégorie Configuration lors de la modification d'une connexion XDMCP.

Option	Description
Nom	Le nom de la connexion.
Type	Le type de connexion XDMCP. Les options valides sont les suivantes : **sélecteur requête** et **diffusion**.
Adresse	Cette valeur est requise si la valeur **Type** est définie sur **requête**.
Utiliser un serveur de polices	Utilise un serveur de polices X distant au lieu de polices installées localement.
Serveur de polices	Le serveur de polices n'est pas activé sauf si l'option **Utiliser le serveur de polices** est sélectionnée.
Configurer l'affichage	Sélectionnez cette option pour paramétrer la configuration de l'affichage pour la connexion. Si vous ne paramétrez pas cette configuration, la configuration par défaut sera utilisée.

Avancé

REMARQUE : Reportez-vous à la section Paramètres de connexion avancés à la page 11 pour plus d'informations sur les paramètres disponibles dans la catégorie Avancé lors de la modification d'une connexion.

Secure Shell

REMARQUE : Ces paramètres affectent uniquement la connexion que vous configurez.

Configuration

Le tableau suivant décrit les paramètres disponibles sous la catégorie Configuration lors de la modification d'une connexion SSH.

Option	Description
Nom	Le nom de la connexion.
Adresse	L'adresse IP du système distant.
Port	Le port distant à utiliser pour la connexion.
Nom d'utilisateur	Le nom d'utilisateur à utiliser pour la connexion.
Exécuter l'application	L'application à exécuter pour établir la connexion.
Compression	Sélectionnez cette option si vous souhaitez compresser les données échangées entre le serveur et le client léger.
Transfert de la connexion X11	Si le serveur a un serveur X sous-jacent, sélectionnez cette option pour permettre à l'utilisateur d'ouvrir des interfaces utilisateur à partir de la session SSH et de les afficher localement sur le client léger.
Forcer l'allocation TTY	Sélectionnez cette option et indiquez une commande pour débuter une session temporaire en vue d'exécuter la commande. Une fois la commande prise en compte, la session prend fin. Si aucune commande n'est indiquée, alors la session est exécutée normalement, comme si l'option n'avait pas été sélectionnée.
Couleur du premier plan	La couleur par défaut du texte dans la session SSH.

Option	Description
Couleur de l'arrière-plan	La couleur par défaut de l'arrière-plan dans la session SSH.
Police	Les options valides sont les suivantes : **7X14**, **5X7**, **5X8**, **6X9**, **6X12**, **7X13**, **8X13**, **8X16**, **9X15**, **10X20** et **12X24**.

Avancé

REMARQUE : Reportez-vous à la section Paramètres de connexion avancés à la page 11 pour plus d'informations sur les paramètres disponibles dans la catégorie Avancé lors de la modification d'une connexion.

Telnet

REMARQUE : Ces paramètres affectent uniquement la connexion que vous configurez.

Configuration

Le tableau suivant décrit les paramètres disponibles sous la catégorie Configuration lors de la modification d'une connexion Telnet.

Option	Description
Nom	Le nom de la connexion.
Adresse	L'adresse IP du système distant.
Port	Le port à utiliser sur le système distant.
Couleur du premier plan	La couleur de premier plan.
Couleur de l'arrière-plan	La couleur de l'arrière-plan.
Police	Les options valides sont les suivantes : **7X14**, **5X7**, **5X8**, **6X9**, **6X12**, **6X13**, **7X13**, **8X13**, **8X16**, **9X15**, **10X20** et **12X24**.

Avancé

REMARQUE : Reportez-vous à la section Paramètres de connexion avancés à la page 11 pour plus d'informations sur les paramètres disponibles dans la catégorie Avancé lors de la modification d'une connexion.

Personnalisée

Pour installer une application Linux® personnalisée, vous pouvez utiliser la connexion Personnalisée, qui vous permettra d'ouvrir cette application via le gestionnaire de connexion.

REMARQUE : Ces paramètres affectent uniquement la connexion que vous configurez.

Configuration

Le tableau suivant décrit les paramètres disponibles sous la catégorie Configuration lors de la modification d'une connexion Personnalisée.

Option	Description
Nom	Le nom de la connexion.
Entrer une commande pour exécuter	La commande à exécuter pour établir la connexion distante.

Avancé

REMARQUE : Reportez-vous à la section Paramètres de connexion avancés à la page 11 pour plus d'informations sur les paramètres disponibles dans la catégorie Avancé lors de la modification d'une connexion.

6 HP True Graphics

HP True Graphics décharge un contenu multimédia enrichi à l'unité de traitement graphique du client léger, en fournissant des images à faute fréquence et en améliorant l'efficacité.

Configuration requise côté serveur

Reportez-vous au tableau suivant pour obtenir la liste des produits pris en charge côté serveur de l'éditeur de logiciels indépendant (ISV) que vous utilisez pour votre infrastructure de bureau virtuel (VDI).

ISV	Produits pris en charge
Citrix®	XenApp®/XenDesktop® 7.0 ou plus récent **IMPORTANT :** Le serveur Citrix doit prendre en charge l'envoi des données de session dans le format H.264 (une technologie Citrix connue comme SuperCodec). H.264 est activé par défaut et est traité à l'aide de l'encodeur DeepCompressionV2, un algorithme de compression basé sur un processeur.
VMware®	VMware Horizon™ 6.0 et plus récent VMware Horizon View™ 5.2 et 5.3 VMware View® 5.1

Configuration requise côté client

Reportez-vous au tableau suivant pour une liste des systèmes d'exploitation de client léger pris en charge et de logiciel client pris en charge depuis l'ISV que vous utilisez pour vos VDI.

REMARQUE : HP true Graphics ne sont pas disponibles avec une licence ThinPro d'essai.

Systèmes d'exploitation pris en charge	Clients Citrix pris en charge	Clients VMware pris en charge
HP ThinPro 5.0 et plus récent	Citrix Receiver 13.1.1 et plus récent **REMARQUE :** Une version de Citrix Receiver qui prend en charge HP True Graphics est préinstallée à partir de HP ThinPro 5.2 et est disponible en tant qu'extension pour HP ThinPro 5.0 et 5.1.	VMware Horizon Client 4.0 et plus récent (en utilisant le protocole Blast)

Configuration côté client

REMARQUE : Les informations de ce chapitre ne concernent que Citrix. Pour VMware, il suffit d'utiliser le protocole Blast pour activer HP True Graphics.

Paramètres de compression

Pour activer HP True Graphics sur HP ThinPro :

▲ Sélectionnez les paramètres généraux **Activer la compression H264** pour les connexions Citrix.

REMARQUE : Certaines données de l'écran, tels que les données textes, peuvent être envoyées à l'aide de méthodes différentes de H.264. En général, il est préférable de conserver cette fonction activée, mais pour la résolution des problèmes ou des cas d'utilisation spécifiques, les clés de registre suivantes peuvent être définies à **0** pour désactiver cette fonction :

- **root/ConnectionType/xen/general/enableTextTracking**
- **root/ConnectionType/xen/general/enableSmallFrames**

Paramètres Windowns

Pour forcer les applications à distance à s'exécuter en mode fenêtré :

▲ Définissez les paramètres généraux **Mode TWI** pour les connexions Citrix sur **Forcer l'arrêt du plein écran**.

Surveillez les restrictions de disposition et de matériel

Notez les restrictions suivantes sur la disposition du moniteur :

- La plupart des configurations avec un maximum de deux écrans d'une résolution de 1920 ×1200 sont prises en charge.
- HP t420 Thin Client : En raison de sa configuration BIOS par défaut, ce modèle utilise par défaut HP True Graphics pour un écran uniquement. Pour plus d'informations, reportez-vous à la section Activation de HP True Graphics pour plusieurs écrans sur le HP t420 à la page 42.
- HP t630 Thin Client : Ce modèle prend en charge un maximum de deux écrans d'une résolution de 1920 × 1200 ou un seul écran avec une résolution de 3840 × 2160.
- HP t730 Thin Client : Ce modèle prend en charge un maximum de trois écrans d'une résolution de 1920 × 1200.
- Des écrans rotatifs risquent de ne pas s'afficher correctement.
- Si vous utilisez HP True Graphics avec deux écrans et essayez de lire une vidéo en utilisant HDX MediaStream, la vidéo va échouer car H.264 ne supporte que deux sessions de décodage matériel, qui sont actuellement utilisées par les écrans.

  REMARQUE : HDX MediaStream essaie aussi de profiter du décodage matériel local H.264, ce qui provoque le problème.

Activation de HP True Graphics pour plusieurs écrans sur le HP t420

Pour activer HP True Graphics pour plusieurs écrans sur le HP t420 :

1. Redémarrez le client léger, puis appuyez sur la touche F10 pour accéder au BIOS.
2. Sélectionnez **Advanced**(Avancé) ► **Integrated Graphics** (Carte Graphique Intégrée).
3. Régler **Integrated Graphics** (Carte Graphique Intégrée) sur **Force** (Force).
4. Définir la **UMA Frame Buffer Size** (taille de mémoire tampon pour le cadre UMA) sur **512 M**

Une fois ces opérations effectuées, la quantité de mémoire disponible pour les graphiques est développée, et HP True Graphics peut être utilisé pour deux écrans.

CONSEIL : Ces paramètres peuvent également être configurés via HPDM ou via les outils BIOS fournis avec HP ThinPro.

Conseils & pratiques recommandées

Notez ce qui suit lors de l'utilisation de HP True Graphics :

- Après s'être connecté à un bureau distant, vous pouvez utiliser le Citrix HDX Monitor pour déterminer quel encodeur est utilisé pour la session en examinant la valeur de **Component_Encoder** dans la section **Graphique - Thinwire avancé**. Si la valeur lit **DeepCompressionV2Encoder** ou **DeepCompressionEncoder**, alors le serveur envoie correctement les données dans un format qui est accéléré par HP True Graphics.

  REMARQUE : Si des cartes graphiques héritées sont forcées par une stratégie de serveur, comme CompatibilityEncoder ou LegacyEncoder, le serveur compresse les cartes graphiques selon une méthode qui est compatible avec les anciennes versions de clients Citrix et vous ne pourrez pas bénéficier des performances améliorées de HP True Graphics.

- HP True Graphics peut apporter certains avantages pour les anciennes versions de XenDesktop si vous utilisez HDX 3D Pro. Aucune amélioration des performances n'est fournie si HDX Pro 3D est utilisé avec la qualité visuelle définie sur **Always Lossless**, car, dans ce cas, les informations graphiques ne sont pas envoyées au client léger en format H.264.

7 Intégration d'Active Directory

En utilisant l'intégration d'Active Directory, vous pouvez obliger les utilisateurs à se connecter au client léger à l'aide d'informations d'authentification de domaine. Facultativement, ces informations d'authentification peuvent être cryptées et stockées, puis fournies ultérieurement au démarrage des connexions distantes, processus connu sous le nom d'authentification unique.

REMARQUE : L'activation de l'authentification ne nécessite pas d'autorisations spéciales sur le domaine.

L'intégration d'Active Directory peut s'opérer selon deux méthodes. En activant simplement d'authentification par rapport au domaine, les informations d'authentification du domaine peuvent être utilisées pour les opérations suivantes :

- Connexion au client léger
- Démarrage d'une connexion en utilisant l'authentification unique
- Passage au mode Administrateur en utilisant les informations d'authentification administrative
- Déverrouillage d'un écran bloqué en utilisant les informations d'authentification de connexion
- Neutraliser un écran bloqué en utilisant les informations d'authentification administrative

Le client léger peut également être formellement lié au domaine. Le client léger est alors ajouté à la base de données du domaine et peut activer le DNS dynamique, où le client léger informe le serveur DNS des modifications de son adresse IP ou de son association de nom d'hôte. Contrairement à l'authentification de domaine, un lien formel nécessite les informations d'authentification d'un utilisateur du domaine autorisé à y ajouter des clients. La liaison au domaine est facultative. Toutes les fonctions de domaine à l'exception du DNS dynamique sont disponibles sans liaison.

Écran de connexion

Lorsque l'authentification de domaine est activée, ThinPro affiche au démarrage un écran de connexion au domaine. L'écran de connexion inclut également des options qui peuvent être nécessaires à la configuration avant connexion.

La disposition du bureau en arrière-plan, le style de la boîte de dialogue de connexion, le texte de la boîte de dialogue de connexion et les boutons disponibles peuvent tous être ajustés via les paramètres du registre et/ou les paramètres du fichier de configuration. Pour plus d'informations à ce sujet, consultez le livre blanc HP ThinPro *Login Screen Customization* (disponible en anglais uniquement).

Si le système détecte que l'utilisateur a tenté de se connecter avec des informations d'authentification périmées, ce dernier est invité à les actualiser.

Authentification unique

Après la connexion d'un utilisateur du domaine, les informations d'authentification utilisées peuvent également être présentées au démarrage à toute connexion configurée pour les utiliser. L'utilisateur peut ainsi se connecter au client léger et démarrer les sessions Citrix, VMware Horizon View et RDP sans devoir saisir à nouveau ses informations d'authentification, aussi longtemps qu'il est connecté au client léger.

Bureau

Une fois l'utilisateur correctement connecté à l'aide des informations d'authentification du domaine, un icône Active Directory est disponible dans la barre de tâches. L'utilisateur peut sélectionner l'icône pour effectuer les fonctions suivantes :

- Afficher qui est connecté dans le système
- Verrouiller l'écran
- Changer le mot de passe du domaine

Verrouillage d'écran

L'écran peut être verrouillé en raison d'une temporisation d'inactivité ou par verrouillage manuel. Si l'écran a été verrouillé par un utilisateur du domaine, la boîte de dialogue de déverrouillage attend de l'utilisateur qu'il fournisse le même mot de passe de domaine que celui utilisé pour se connecter. Comme la boîte de dialogue, des options sont présentées, ainsi qu'une fonction supplémentaire : déverrouillage de l'écran. Lorsque le bouton de déverrouillage d'écran est sélectionné, le déverrouillage d'écran requiert à la place le mot de passe racine (administrateur) ou un ensemble quelconque d'informations d'authentification de domaine dans le groupe d'administration du domaine, désigné lors de la configuration de l'authentification du domaine. Lorsque l'utilisateur fournit des informations d'authentification neutralisantes, l'écran ne revient pas au bureau ; il retourne à la place à l'écran d'accueil.

Mode Administrateur

En plus de la méthode conventionnelle d'utilisation du mot de passe racine pour accéder au mode Administrateur, les informations d'authentification de domaine d'un utilisateur dans le groupe d'administrateurs de domaine désigné peuvent être utilisées pour passer en mode Administrateur.

Paramètres et utilisateur du domaine

Lorsqu'un utilisateur de domaine est connecté, toutes les modifications de paramètres sont enregistrées dans une couche du registre concernant uniquement cet utilisateur. Ces modifications comprennent les connexions nouvellement créées.

Si l'utilisateur n'a pas apporté de modifications aux paramètres du système ou aux connexions, les valeurs par défaut du système s'appliquent.

Lorsque le système est passé en mode Administrateur, les modifications de paramètres et de connexion ne sont plus effectuées dans la couche du registre spécifique à l'utilisateur. En revanche, en mode Administrateur, toutes les modifications s'appliquent au registre du niveau de base. Ainsi, une modification de paramètre en mode Administrateur s'applique à tous les utilisateurs, sauf en cas de paramètre personnalisé spécifique à un utilisateur déjà spécifié.

8 menu Démarrer

▲ Pour ouvrir le menu Démarrer, sélectionnez **Démarrer** .

Gestion des connexions

Le menu répertorie toutes les connexions disponibles. Cliquez avec le bouton droit sur le nom de la connexion pour gérer cette connexion ou la sélectionner pour lancer la connexion. Si la connexion est en cours d'exécution, le fait de la sélectionner interrompt la connexion. Pour de plus amples informations sur la gestion des connexions, voir Gestion des connexions de bureau à la page 9.

Basculer en administrateur/Basculer en utilisateur

Cette option vous permet de basculer entre le mode utilisateur et le mode administrateur.

System Information (Informations système)

Cette option démarre l'application System Information. Pour plus d'informations, voir System Information (Informations système) à la page 68.

Panneau de configuration

Cette option lance le Panneau de configuration. Pour plus d'informations, voir Panneau de configuration à la page 48.

Outils

Il existe de nombreux outils système fournis, dont un pour lancer des programmes, tel qu'un terminal de traitement de texte, ou pour exécuter l'Assistant de configuration initiale une deuxième fois. Si vous êtes connecté en tant qu'utilisateur, seuls les outils autorisés s'affichent. Si cette liste est vide, l'entrée de menu Outils est masquée.

Option de menu	Description
X Terminal (Terminal X)	Vous permet d'exécuter les commandes Linux.
Statistiques sans fil	Vous permet d'afficher des informations sur les points d'accès sans fil.
Vérifier les mises à jour	Recherche des mises à jour à partir du serveur.
Text Editor (Éditeur de texte)	Ouvre un éditeur de texte de base pour l'affichage et la modification des fichiers texte.
Gestionnaire des tâches	Vous permet de surveiller l'utilisation du processeur et l'historique d'utilisation de CPU pour le client léger.
Outil de découpe	Vous permet de prendre un instantané d'une sélection rectangulaires de l'écran, une fenêtre spécifique ou tout l'écran.

Option de menu	Description
Éditeur de registre	Ouvre l'éditeur de registre ThinPro.
Assistant de configuration initiale	Lance l'assistant de configuration initiale.
Vérification de la compatibilité	Exécute l'outil de vérification de la compatibilité ThinPro, qui évalue la convenance du système pour l'exécution de ThinPro.

Alimentation

Ces options vous permettent de vous connecter, d'éteindre l'ordinateur, de redémarrer l'ordinateur ou d'activer l'état de veille.

Un administrateur peut limiter la visibilité des options à un utilisateur à l'aide de l'outil Power Manager (Gestionnaire d'alimentation). Reportez-vous à la section Système à la page 48.

Recherche

Lorsque vous tapez dans la zone de recherche, une série de correspondances possibles pour votre recherche s'affichent de la plus probable à la moins probable. La recherche inclut les noms de contrôles, d'outils et de connexions visibles, ainsi que les alias et synonymes associés. Par exemple, en mode Administrateur, taper `encryption` (chiffrement) affiche les options de Sécurité parce que ces options proposent des paramètres de chiffrement.

Pour voir toutes les options disponibles, saisissez un espace dans la boîte de recherche ou sélectionnez l'icône de la loupe.

La recherche renvoie également des options permettant de créer de nouvelles connexions de tous les types disponibles. Elle peut être utilisée pour gérer les connexions.

9 Panneau de configuration

Le Panneau de configuration vous permet de modifier la configuration du système.

Pour ouvrir le Panneau de configuration :

▲ Sélectionnez **Démarrer**, puis **Panneau de configuration**.

REMARQUE : Vous pouvez également rechercher une fonction spécifique du Panneau de configuration à l'aide de la zone de recherche du menu Démarrer.

REMARQUE : Tous les éléments du Panneau de configuration accessibles en mode Administrateur. En mode Utilisateur, seuls les éléments du Panneau de configuration autorisés par l'administrateur pour une utilisation par les utilisateurs sont accessibles.

CONSEIL : Pour déterminer les éléments du Panneau de configuration auxquels peuvent accéder les utilisateurs, ouvrez **Appearance** (Apparence), sélectionnez **Customization Center** (Centre de personnalisation), puis sélectionnez ou désélectionnez les éléments dans la liste **Applications**.

Système

Option de menu	Description
Date et heure	Vous permet de configurer le fuseau horaire, ainsi que les options de date et d'heure.
Réseau	Vous permet de configurer les paramètres réseau. Pour plus d'informations, reportez-vous à la section Paramètres réseau à la page 49.
Options DHCP	Vous permet de configurer les options DHCP. Pour plus d'informations, reportez-vous à la section Options DHCP à la page 53.
Power Manager (Gestionnaire d'alimentation)	Permet de configurer les paramètres de gestion de l'alimentation, tels que l'économiseur d'écran et le verrouillage d'écran, les paramètres de l'UC, quand éteindre l'écran et quand activer le mode veille. En mode Administrateur, vous pouvez restreindre l'accès aux options liées à l'alimentation (telles que Redémarrer) à l'échelle du système.
Configuration Imprivata	Vous permet d'activer Imprivata Appliance Mode et de spécifier un serveur Imprivata.
Gestionnaire de composants	Vous permet de supprimer des composants du système. Pour plus d'informations, reportez-vous à la section Gestionnaire de composant à la page 53.
Réinitalisation des paramètres d'usine	Vous permet de rétablir le client léger dans sa configuration d'usine par défaut.
Instantanés	Vous permet de restaurer le client léger à un état antérieur ou de rétablir sa configuration d'usine par défaut.

Paramètres réseau

Les paramètres réseau peuvent être configurés dans le gestionnaire réseau. Pour ouvrir le gestionnaire réseau :

▲ Sélectionnez **Système**, puis **Réseau** dans le Panneau de configuration.

Reportez-vous aux sections suivantes pour plus d'informations sur les différents onglets du gestionnaire réseau :

- Paramètres du réseau filaire
- Paramètres du réseau sans fil
- Paramètres DNS
- Règles IPSec
- Configuration des paramètres VPN

Paramètres du réseau filaire

Le tableau suivant décrit les options disponibles dans l'onglet **Wired** (Filaire) du gestionnaire réseau.

Option	Description
Activer IPv6	Active le protocole IPv6. IPv4 est utilisé par défaut et les deux protocoles ne peuvent pas être utilisés en même temps.
Vitesse Ethernet	Vous permet de définir la vitesse Ethernet. Si votre commutateur ou concentrateur n'a pas d'exigences spécifiques, conservez la valeur par défaut, **Automatique**.
Méthode de connexion	Vous permet de choisir entre **Automatique** et **Statique**. Si votre environnement réseau utilise DHCP, l'option **Automatique** devrait fonctionner sans autre configuration supplémentaire. Si **Statique** est sélectionné, les paramètres de **Configuration d'adresse statique** apparaissent. Tenez compte du protocole utilisé (IPv4 ou IPv6) lorsque vous entrez ces valeurs.
MTU	Vous permet d'entrer l'unité de transmission maximum (en octets).
Paramètres de sécurité	Vous permet de définir le paramètre d'authentification sur l'une des valeurs suivantes : • Aucun • 802.1X-TTLS • 802.1X-PEAP • 802.1X-TLS Notez les points suivants concernant TTLS et PEAP : • L'option **Authentification interne** doit être configurée, quelles que soient les spécifications de votre serveur. • Le paramètre **Certificat d'autorité de certification** doit pointer vers le certificat du serveur sur le client léger local. • **Nom d'utilisateur** et **Mot de passe** correspondent aux informations d'authentification de l'utilisateur. Notez les points suivants concernant TLS : • Le paramètre **Certificat d'autorité de certification** doit pointer vers le certificat du serveur sur le client léger local. • Si votre fichier de **Clé privée** est .p12 ou .pfx, le paramètre **Certificat d'utilisateur** peut être laissé vide.

Option	Description
	• Le paramètre **Identité** doit correspondre au nom d'utilisateur du certificat de l'utilisateur. • Le paramètre **Mot de passe de clé privée** correspond au mot de passe du fichier de clé privée de l'utilisateur.

Paramètres du réseau sans fil

Utilisez cet onglet pour ajouter, modifier et supprimer des profils de réseau sans fil qui correspondent à des réseaux sans fil.

Les tableaux suivants décrivent les options disponibles lors de l'ajout ou de l'édition d'un profil de réseau sans fil.

REMARQUE : Cet onglet est disponible uniquement si le client léger dispose d'un adaptateur sans fil.

CONSEIL : Vous pouvez également accéder à ces paramètres en sélectionnant l'icône d'état du réseau dans la barre des tâches.

Utilisez l'onglet **Wireless** (Sans fil) pour configurer les paramètres généraux.

Option	Description
Scan AP (Rechercher un point d'accès)	Recherche les réseaux sans fil disponibles.
SSID	Utilisez ce champ pour entrer manuellement le SSID du réseau sans fil si ce dernier n'est pas détecté par la recherche.
Bande sans fil	Sélectionnez **Auto** (Automatique), **2,4 GHz**, ou **5 GHz**.
SSID Hidden (SSID masqué)	Activez cette option si le SSID du réseau sans fil est configuré pour être masqué (pas de diffusion).
Activer IPv6	Active IPv6. IPv4 est utilisé par défaut et les deux protocoles ne peuvent pas être utilisés en même temps.
Enable Power Management (Activer la gestion de l'alimentation)	Active la fonction de gestion de l'alimentation de l'adaptateur sans fil.
Méthode de connexion	Vous permet de choisir entre **Automatique** et **Statique**. Si votre environnement réseau utilise DHCP, l'option **Automatique** devrait fonctionner sans autre configuration supplémentaire. Si **Statique** est sélectionné, les paramètres de **Configuration d'adresses statiques** apparaissent. Tenez compte du protocole utilisé (IPv4 ou IPv6) lorsque vous entrez ces valeurs.
Paramètres de sécurité	Vous permet de définir le paramètre d'authentification sur l'un des paramètres suivants : • Aucun • WEP • WPA/WPA2-PSK • 802.1X-TTLS • 802.1X-PEAP • 802.1X-TLS • EAP-FAST Pour WEP et WPA/WPA2-PSK, vous devez simplement entrer la clé de réseau et sélectionner **OK**.

Option	Description
	Pour EAP-FAST, définissez **Identité anonyme**, **Nom d'utilisateur**, **Mot de passe** et **Méthode d'approvisionnement**. Vous n'avez pas besoin de modifier les paramètres du fichier PAC. Reportez-vous à la section Paramètres du réseau filaire à la page 49 pour plus d'informations sur TTLS, PEAP et TLS.
Connexion automatique	Cette option est réservée pour une utilisation future.
Activer la fonctionnalité sans fil	Activer l'adaptateur sans fil.

Utilisez l'onglet **IPv4** pour configurer les paramètres de la connexion IPv4.

Option	Description
IPv4 activé	Active IPv4.
Méthode IPv4	Vous permet de choisir entre **Automatic** et **Static**. Si votre environnement réseau utilise DHCP, l'option **Automatic** devrait fonctionner sans autre configuration supplémentaire. Si **Static** est sélectionné, les paramètres **Static Address Configuration** (Configuration d'adresse statique) s'affichent et vous devez saisir les paramètres IPv4.

Utilisez l'onglet **IPv6** pour configurer les paramètres de la connexion IPv6.

Option	Description
IPv6 activé	Active l'utilisation d'une adresse globale IPv6. **REMARQUE :** HP ThinPro tente d'obtenir une adresse globale IPv6 par les annonces de routage ou DHCPv6.
Méthode IPv6	Vous permet de choisir entre **Automatic** et **Static**. Si votre environnement réseau utilise DHCP, l'option **Automatic** devrait fonctionner sans autre configuration supplémentaire. Si **Static** est sélectionné, les paramètres **Static Address Configuration** (Configuration d'adresse statique) s'affichent et vous devez saisir les paramètres IPv6.

Utilisez l'onglet **Security** (Sécurité) pour configurer les paramètres de sécurité de la connexion.

Option	Description
Authentification	Vous permet de définir le paramètre d'authentification sur l'un des paramètres suivants : • Aucun • WEP • WPA/WPA2-PSK • WPA/WPA2 Enterprise-TTLS • WPA/WPA2 Enterprise-PEAP • WPA/WPA2 Enterprise-TLS • EAP-FAST Pour WEP et WPA/WPA2-PSK, vous devez simplement entrer la clé de réseau et sélectionner **OK**.

Option	Description
	Pour EAP-FAST, définissez **Identité anonyme**, **Nom d'utilisateur**, **Mot de passe** et **Méthode d'approvisionnement**. Vous n'avez pas besoin de modifier les paramètres du fichier PAC. Reportez-vous à la section Paramètres du réseau filaire à la page 49 pour plus d'informations sur TTLS, PEAP et TLS.

Paramètres DNS

Le tableau suivant décrit les options disponibles dans l'onglet **DNS** du gestionnaire réseau.

Option	Description
Nom d'hôte	Il est généré automatiquement en fonction de l'adresse MAC du client léger. Vous pouvez également définir un nom d'hôte personnalisé.
Serveur DNS	Utilisez ce champ pour définir des informations de serveur DNS personnalisées.
Domaines de recherche	Utilisez ce champ pour limiter les domaines de recherche.
Proxy HTTP Proxy FTP Proxy HTTPs	Utilisez ces champs pour définir les informations du serveur proxy en utilisant le format suivant : `http://<adresse>:<port>` HP vous recommande d'utiliser le préfixe `http://` pour les trois paramètres de proxy, car il est mieux pris en charge. **REMARQUE :** Les paramètres de proxy sont définis sur les variables d'environnement **http_proxy**, **ftp_proxy** et **https_proxy** pour le système.

Règles IPSec

Utilisez cet onglet pour ajouter, modifier et supprimer des règles IPSec. Une règle IPSec doit être identique pour chacun des systèmes qui utilise IPSec pour communiquer.

Lors de la configuration d'une règle IPSec, utilisez l'onglet **Général** pour définir les informations, adresses et méthode d'authentification de la règle. Le paramètre **Adresse source** correspond à l'adresse IP du client léger et l'adresse de destination correspond à l'adresse IP du système avec lequel le client va communiquer.

REMARQUE : Seuls les types d'authentification **PSK** et **Certificat** sont pris en charge. L'authentification Kerberos n'est pas prise en charge.

Utilisez l'onglet **Tunnel** pour configurer les paramètres du mode tunnel.

Utilisez les onglets **Phase I** et **Phase II** pour configurer les paramètres avancés de sécurité. Les paramètres doivent être identiques pour tous les systèmes homologues qui communiquent entre eux.

REMARQUE : Une règle IPSec peut également être utilisée pour communiquer avec un ordinateur sous Windows.

Configuration des paramètres VPN

HP ThinPro prend en charge deux types de VPN :

- Cisco
- PPTP

Activez l'option **Démarrage automatique** pour démarrer automatiquement le VPN.

Notez les points suivants sur la création d'un VPN avec Cisco :

- Le paramètre **Passerelle** correspond à l'adresse IP ou au nom d'hôte de la passerelle.
- Les paramètres **Nom du groupe** et **Mot de passe de groupe** correspondent à l'identifiant IPSec et au mot de passe IPSec.
- Le paramètre **Domaine** est facultatif.
- Les paramètres **Nom d'utilisateur** et **Mot de passe d'utilisateur** correspondent aux informations d'authentification des utilisateurs autorisés à créer une connexion VPN côté serveur.
- Le paramètre **Type de sécurité** doit être identique à celui configuré côté serveur.
- L'option **Parcours NAT** doit être configurée en fonction de votre environnement VPN.
- L'option **Groupe DH IKE** définit le groupe Diffie-Hellman à utiliser pour le VPN.
- L'option **Groupe DH IKE** définit le groupe Diffie-Hellman à utiliser pour PFS (Perfect Forward Secrecy).

Notez les points suivants sur la création d'un VPN avec le protocole PPTP :

- Le paramètre **Passerelle** correspond à l'adresse IP ou au nom d'hôte de la passerelle.
- Le paramètre **Domaine NT** est facultatif.
- Les paramètres **Nom d'utilisateur** et **Mot de passe utilisateur** correspondent aux informations d'authentification des utilisateurs autorisés à créer une connexion VPN côté serveur.

Options DHCP

Pour ouvrir le gestionnaire d'options DHCP :

▲ Sélectionnez **Système** puis sélectionnez **Options DHCP** dans le Panneau de configuration.

Le gestionnaire d'options DHCP affiche les informations détaillées des options DHCP qui sont demandées par le client léger.

CONSEIL : La liste déroulante vous permet de filtrer les étiquettes DHCP à afficher.

Pour que le client demande ou ignore certaines options DHCP spécifiques, procédez comme suit :

▲ Cochez ou décochez les cases dans la colonne **Demandé**.

Si un crayon apparaît dans la colonne **Code DHCP**, le numéro de code peut être modifié en cas de conflit sur votre serveur DHCP à propos d'un numéro de code spécifique.

Pour modifier un code DHCP :

▲ Double-cliquez sur le code DHCP et entrez un nouveau numéro.

REMARQUE : Les codes DHCP modifiables peuvent uniquement être modifiés lorsque cette option DHCP est activée dans la colonne **Requis**.

Pour en savoir plus sur l'utilisation de l'option DHCP sur le client léger et sur le serveur DHCP :

▲ Sélectionnez l'icône dans la colonne **Info** de cette option.

Gestionnaire de composant

Component Manager (Gestionnaire de composant) vous permet de supprimer des composants système qui ne sont pas utilisés dans votre environnement, ce qui peut être souhaitable afin de réduire la taille de l'image ou

optimiser la sécurité. Par exemple, si les connexions Citrix ne servent jamais dans votre environnement, vous pourriez vouloir supprimer le composant de Citrix.

Lorsque les composants sont supprimés, la nouvelle configuration peut être testée avant que vous n'appliquiez les modifications définitivement. Vous pouvez également annuler les modifications qui ont été faites, si elles n'ont pas encore été appliquées définitivement.

IMPORTANT : Une fois la nouvelle configuration appliquée définitivement, toutes les images instantanées individuelles sont supprimées et un nouvel instantané de paramètres d'usine est créé. Les composants supprimés ne peuvent pas être restaurés après ce point.

REMARQUE : Le retrait de composants peut ne pas réduire l'utilisation de l'espace disque local, mais il peut réduire la taille de toutes les images disque créées à partir du système local.

Pour ouvrir le gestionnaire de composants :

▲ Sélectionnez **Système** puis sélectionnez **Component Manager** dans le Panneau de configuration.

Suppression des composants

Pour supprimer des composants :

1. Dans le gestionnaire de composants, sélectionnez les composants de votre choix.

   CONSEIL : Pour sélectionner plusieurs composants, utilisez Ctrl ou Shift.

2. Sélectionnez **Remove Component(s)** (Retirer Component(s)).
3. Si la boîte de dialogue de confirmation s'affiche, sélectionnez **OK**.
4. Une fois les composants supprimés, testez la nouvelle configuration.

Annuler une modification

Vous pouvez annuler chaque modification, une à la fois, si les modifications n'ont pas encore été appliquées définitivement. Un redémarrage du client léger est requis après chaque annulation.

Pour annuler une modification effectuée avec le gestionnaire de composant :

1. Dans le gestionnaire de composant, sélectionnez **Revert Last Change** (Annuler dernière modification).
2. Sélectionnez **Yes** (Oui) pour redémarrer le client léger.

Répétez cette procédure pour toutes les modifications que vous souhaitez annuler.

IMPORTANT : Si vous prenez un instantané de l'image lors du test d'une nouvelle configuration, vous ne pouvez pas annuler les modifications via le gestionnaire de composants. Ces modifications peuvent être annulées uniquement en rétablissant un instantané précédent via l'outil Snapshots (Instantanés). Cependant, il ne fonctionne pas si les modifications ont déjà été appliquées définitivement, car la fonction choisie supprime toutes les images instantanées individuelles existantes. Si les modifications ont déjà été appliquées définitivement, vous devez réinstaller le système d'exploitation pour restaurer la plupart des composants supprimés. Certains composants (par exemple, Citrix, RDP et VMware Horizon View) peuvent être disponibles en tant que modules complémentaires sur le web et peuvent être restaurés en les réinstallant.

Appliquer les modifications définitivement

Pour appliquer définitivement les modifications apportées avec le gestionnaire de composants :

IMPORTANT : Une fois la nouvelle configuration appliquée définitivement, tous les instantanés sont supprimés et un nouvel instantané de paramètres d'usine est créé. Les composants supprimés ne peuvent pas être restaurés après ce point.

1. Dans le gestionnaire de composants, sélectionnez **Apply Component Configuration** (Appliquer la Configuration de composant).
2. Sélectionnez **Yes** (Oui).

Sécurité

Option de menu	Description
Sécurité	Pour plus d'informations, reportez-vous à la section Paramètres de sécurité à la page 55.
Changer le mot de passe du domaine	Si un domaine est en cours d'utilisation, vous permet de modifier le mot de passe du domaine.
certificats	Ouvre Certificate Manager (Gestionnaire de certificats), qui vous permet d'importer, d'afficher ou de supprimer des certificats en toute simplicité. Pour plus d'informations, voir Gestionnaire de certificats à la page 57.
Gestionnaire du Pare-feu	Permet de configurer les paramètres du pare-feu.
Gestionnaire SCEP	Permet d'effectuer une gestion des certificats en réseau.

Paramètres de sécurité

Les paramètres de sécurité peuvent être configurés avec Security Manager. Pour ouvrir Security Manager, sélectionnez **Sécurité**, puis sélectionnez **Sécurité** dans le Panneau de configuration.

Consultez les sections suivantes pour des informations plus détaillées sur les différents onglets de Security Manager.

- Comptes locaux à la page 55
- Cryptage à la page 56
- Options à la page 56

Comptes locaux

Vous pouvez utiliser l'onglet Comptes locaux pour changer les mots de passe racine local et du compte utilisateur ou pour désactiver l'authentification en utilisant ces comptes.

ATTENTION : La désactivation des comptes racine et/ou utilisateur peuvent rendre votre système inutilisable si l'authentification Active Directory n'est pas activée. Par exemple, si le compte racine est désactivé, vous ne pourrez passer en mode Administrateur qu'en utilisant les informations d'authentification de domaine d'un administrateur. En revanche, la désactivation des comptes locaux peut améliorer la sécurité lorsqu'une authentification Active Directory est activée, car vous n'êtes plus dans l'obligation de maintenir et d'actualiser un secret partagé comme le mot de passe racine du client léger.

Si l'authentification Active Directory a été utilisée alors qu'il existe des données en cache pour les utilisateurs du domaine sur le client léger, vous pouvez également supprimer les données en cache de l'utilisateur depuis cet onglet.

REMARQUE : Si l'utilisateur s'est connecté en utilisant un compte de domaine, vous ne pouvez pas supprimer les données de son propre compte, car cela laisserait le système dans un état indéterminé.

Cryptage

Les informations d'authentification Active Directory et autres secrets peuvent être hachés pour des fonctions comme le déverrouillage d'écran et/ou cryptées et stockées dans le système pour l'authentification unique.

L'algorithme de hachage pour créer un hachage de mot de passe peut être sélectionné dans ce menu. L'option par défaut, scrypt, est une fonction de dérivation de clé bien acceptée. Argon2, une autre fonction de dérivation de clé, est également disponible, ainsi que les hachages conventionnels SHA-256 et SHA-512. L'avantage d'une telle fonction réside dans le fait qu'il est coûteux sur le plan du calcul de calculer une table arc-en-ciel correspondant aux mots de passe en texte simple en valeurs hachées pré-calculées, alors que les hachages conventionnels sont conçus pour s'exécuter aussi rapidement que possible. Tous les hachages sont stockés en 128 bits aléatoires ou plus de grains de sel, qui changent à chaque fois que le hachage de mot de passe est calculé et stocké.

Les mots de passe cryptés sont utilisés dans les cas où ils peuvent être inversés et fournis au démarrage des connexions (authentification unique). L'algorithme de cryptage peut être sélectionné ici parmi un large éventail compatible avec OpenSSL. Sauf s'il existe une bonne raison de sélectionner une valeur différente, HP recommande d'utiliser l'algorithme de cryptage par défaut, qui est généralement considéré comme moderne et sûr par la communauté sécuritaire. Le nombre de bits de grains de sel et de bits clés varie selon l'algorithme. Vous pouvez obtenir des détails en appuyant sur le bouton info en regard du sélecteur d'algorithme. Les clés de cryptage sont uniques pour chaque client léger et sont stockées dans un emplacement que seuls les administrateurs peuvent lire. En outre, seules certaines applications autorisées sur le système peuvent décrypter.

Les hachages comme les secrets cryptés peuvent être configurés avec un délai de péremption. Si la durée entre le moment où le secret a été haché ou crypté et celui où il est utilisé ou décrypté dépasse le délai de péremption, la correspondance de hashage ou le décryptage échoue.

Par défaut, le mot de passe unique de connexion n'est utilisable que pour une seule journée, mais tous les mots de passe stockés avec les paramètres réseau ou de connexion peuvent être utilisés indéfiniment.

Options

L'utilisateur local doit se connecter : Lorsque cette option est sélectionnée alors que l'authentification Active Directory est désactivée, l'écran de connexion s'affiche toujours au démarrage et à la déconnexion. Dans ce cas, les informations d'authentification racine ou de l'utilisateur local doivent être utilisées pour accéder au système.

Activer l'aperçu des données secrètes : Lorsque cette option est activée, la plupart des champs de saisie de mot de passe et de secret affichent sur la droite une petite icône représentant un œil. En sélectionnant cette icône en maintenant le bouton gauche de la souris enfoncé, le secret est affiché en texte simple tant que le bouton de la souris est maintenu enfoncé. Dès que le bouton est relâché, le secret est à nouveau masqué.

Utiliser la saisie de texte du domaine : Lorsque cette option est activée, un champ de saisie de domaine distinct est présenté pour le nom de domaine, le cas échéant. Lorsqu'elle est désactivée, le domaine est déterminé par la valeur saisie dans le champ Utilisateur. Par exemple, si le champ Utilisateur contient « mike@mycorp@», le domaine est supposé être « mycorp ». Si le champ utilisateur est « graycorp\mary » le domaine est supposé être « graycorp ».

Autoriser les administrateurs à neutraliser le verrouillage de l'écran : Lorsque l'option est activée, vous pouvez neutraliser un écran verrouillé et le ramener à l'écran de connexion ou au bureau ThinPro, exactement comme si l'utilisateur s'était déconnecté manuellement du client léger.

Certificats

REMARQUE : Pour plus d'informations sur l'utilisation des certificats dans Linux, consultez https://www.openssl.org/docs/.

Gestionnaire de certificats

Pour ouvrir Certificate Manager :

▲ Sélectionnez **Sécurité**, puis **Certificats** dans le Panneau de configuration.

Utilisez Certificate Manager pour installer manuellement un certificat en provenance d'une autorité de certification. Cette action copie le certificat vers le magasin de certificats local de l'utilisateur (/usr/local/share/ca-certificates) et configure OpenSSL afin que le certificat soit utilisé pour vérifier la connexion.

Si vous le souhaitez, utilisez Profile Editor pour associer le certificat à un profil, comme décrit dans la section Ajout de certificats à un profil de client à la page 76.

REMARQUE : Généralement, un certificat auto-signé fonctionnera tant qu'il est valide d'après ses spécifications et qu'il peut être vérifié par OpenSSL.

Gestionnaire SCEP

Pour ouvrir le gestionnaire SCEP :

▲ Sélectionnez **Sécurité**, puis sélectionnez **SCEP Manager** dans le Panneau de configuration.

Utilisez le gestionnaire SCEP lorsque vous souhaitez inscrire ou renouveler des certificats côté client en provenance d'une autorité de certification.

Lors d'une inscription ou d'un renouvellement, le gestionnaire SCEP génère la clé privée et la demande de certificat du client, puis envoie la demande à l'autorité de certification sur le serveur SCEP. Lorsque l'autorité de certification émet le certificat, ce dernier est renvoyé et placé dans le magasin de certificats du client léger. OpenSSL utilise le certificat pour vérifier la connexion.

REMARQUE : Avant l'inscription, assurez-vous que le serveur SCEP est configuré correctement.

Si vous le souhaitez, entrez les informations relatives à l'utilisateur dans l'onglet **Identification** du gestionnaire SCEP.

REMARQUE : Le paramètre **Common Name** (Nom commun) est obligatoire et correspond au nom de domaine complet totalement qualifié (FQDN) du client léger par défaut. Toutes les autres informations sont facultatives. Le paramètre **Country or Region** (Pays ou région) doit être entré sous la forme deux lettres, par exemple US pour les États-Unis et CN pour la Chine.

Utilisez l'onglet **Serveurs** du gestionnaire SCEP pour ajouter des serveurs SCEP et inscrire ou renouveler des certificats.

CONSEIL : Lors de la saisie d'un nouveau serveur SCEP, commencez par enregistrer les informations du serveur, puis utilisez le bouton **Paramètres** pour revenir en arrière et procéder à l'inscription.

Simplicité de gestion

Option de menu	Description
Active Directory	Pour plus d'informations, reportez-vous à la section Configuration d'Active Directory à la page 58.
Mise à jour automatique	Vous permet de configurer manuellement le serveur de mise à jour automatique. Pour plus d'informations, reportez-vous à la section HP Smart Client Services à la page 69.
Easy Update	Lance HP Easy Tools.

Option de menu	Description
	Pour plus d'informations, reportez-vous à la section du manuel de l'utilisateur pour HP Easy Tools.
HPDM Agent	Vous permet de configurer l'agent HP Device Manager (HPDM). Pour plus d'informations, consultez le *Manuel de l'administrateur* HPDM.
Gestionnaire SSHD	Permet l'accès via un shell sécurisé.
ThinState	HP ThinState vous permet d'effectuer une copie ou une restauration de l'image complète du système d'exploitation ou de ses paramètres de configuration. Pour plus d'informations, reportez-vous à la section HP ThinState à la page 59.
Contrôle à distance (VNC)	Vous permet de configurer les options de Contrôle à distance (VNC). Pour plus d'informations, reportez-vous à la section Utilisation de VNC Shadow à la page 63.

Configuration d'Active Directory

Onglet État

Cette commande permet d'activer ou de désactiver l'authentification par rapport à un domaine, ainsi que différentes options associées au domaine.

Après avoir modifié les paramètres de domaine dans l'onglet État, la page affiche une action en attente et vous devez sélectionner **Appliquer** pour que cette action intervienne. Lier ou délier le domaine nécessite des informations d'authentification avec autorisations pour effectuer cette opération. Après avoir activé l'authentification ou lié le domaine, certains paramètres secondaires peuvent être marqués en lecture seule, car il est impossible de les modifier à ce moment. Vous devez plutôt délier ou désactiver complètement l'authentification puis appliquer les modifications. Vous pouvez ensuite réactiver l'authentification ou la liaison avec les paramètres secondaires modifiés.

Option	Description
Nom de domaine	Si le client léger est en mesure de déterminer le nom de domaine à l'aide des options DHCP, il est affiché ici. Sinon, vous devez saisir manuellement le nom de domaine pleinement qualifié.
Authentification par rapport au domaine	Lorsque cette option est activée, les informations d'authentification du domaine peuvent être utilisées, comme indiqué dans la section Intégration d'Active Directory du présent guide.
Exiger la connexion du client léger	Cette option est activée par défaut et elle a pour effet de démarrer le système dans l'écran de connexion au domaine. Lorsqu'elle est désactivée, les informations d'authentification du domaine peuvent toujours être utilisées pour passer en mode administrateur ou pour neutraliser un écran verrouillé, mais l'authentification unique n'est pas disponible.
Groupe de travail	Il est généralement détecté automatiquement à partir des informations fournies par les serveurs réseau mais vous pouvez utiliser cette option comme neutralisation manuelle en cas de topologie inhabituelle du réseau.
Contrôleurs de domaine	Ils sont généralement détectés en utilisant les recherches DNS mais vous pouvez les spécifier manuellement si votre réseau ne fournit pas cette information.

Option	Description
Lier le client léger au domaine	Comme exposé au chapitre sur l'intégration d'Active Directory, cette option permet d'ajouter formellement le client léger aux bases de données d'Active Directory.
Unité organisationnelle (UO)	Le client léger est généralement ajouté à l'UO « Ordinateurs » de la base de données mais vous pouvez saisir manuellement une valeur différente si le schéma de votre base de données l'exige.
DNS dynamique	Lorsque cette option est activée, le client léger tente d'actualiser le serveur DNS lorsque son association adresse IP/nom d'hôte change.

Onglet Options

Option	Description
Activer l'authentification unique	Lorsque cette option est activée, un mot de passe fourni à la connexion est crypté et enregistré dans le système. Lorsqu'une connexion commence avec des informations d'authentification SSO configurées, elle peut décrypter le mot de passe et le transmettre à la connexion afin de l'utiliser pour la connexion distante.
Groupe de connexion au domaine	Si cette option est activée, la connexion est limitée aux utilisateurs du groupe de domaine indiqué.
Groupe d'administration de domaine	Si cette option est activée, la progression vers le mode Administrateur et la neutralisation du verrouillage d'écran sont limitées aux membres du groupe de domaine indiqué.
Activer la connexion au domaine en cache	Lorsque cette option est activée, un hashage du mot de passe utilisateur est enregistré dans le système et peut être utilisé pour la connexion lorsque le serveur Active Directory est inaccessible.
Conserver les préférences de l'utilisateur à la déconnexion	Lorsque cette option est activée, toutes les modifications de paramètre effectuées par un utilisateur du domaine sont stockées dans un emplacement où ces paramètres sont appliqués uniquement à cet utilisateur. Lorsqu'elle est désactivée, de telles modifications spécifiques à l'utilisateur sont éliminées lorsque l'utilisateur se déconnecte.
Autoriser les modifications de mot de passe de domaine	Lorsque cette option est activée, les mots de passe expirés produisent une invite qui permet à l'utilisateur d'actualiser son mot de passe. Il peut également actualiser son mot de passe manuellement à l'aide de l'icône utilisateur de la barre de tâches.

HP ThinState

HP ThinState vous permet de capturer et de déployer une image ou configuration (profil) HP ThinPro sur un autre client léger de modèle ou matériel compatible.

Gestion d'une image HP ThinPro

Capture d'une image HP ThinPro sur un serveur FTP

Pour capturer une image HP ThinPro sur un serveur FTP :

IMPORTANT : Le répertoire du serveur FTP où vous envisagez d'enregistrer l'image capturée doit exister avant de démarrer la capture.

1. Sélectionnez **Gestion > ThinState** dans le Panneau de configuration.
2. Sélectionnez **l'image HP ThinPro**, puis **Suivant**.
3. Sélectionnez **copier l'image HP ThinPro** , puis **Suivant**.

4. Sélectionnez **sur un serveur FTP**, puis **Suivant**.
5. Entrez les informations du serveur FTP dans les champs.

   REMARQUE : Par défaut, le nom du fichier image correspond au nom d'hôte du client léger.

   Sélectionnez **Compresser l'image** si vous souhaitez compresser l'image capturée.

   REMARQUE : Le fichier image HP ThinPro est un simple vidage sur disque. La taille décompressée est d'environ 1 Go et une image compressée sans module est d'environ 500 Mo.

6. Sélectionnez **Terminer**.

   Lorsque la capture d'image commence, toutes les applications s'arrêtent et une nouvelle fenêtre s'affiche pour montrer la progression. En cas de problème, sélectionnez **Détails** pour plus d'informations. Le bureau réapparaît à la fin de la capture.

Déploiement d'une image HP ThinPro avec le protocole FTP ou HTTP

IMPORTANT : Si vous abandonnez un déploiement avant la fin, l'image précédente ne sera pas restaurée et le contenu de l'unité flash USB du client léger sera corrompu.

Pour déployer une image HP ThinPro avec le protocole FTP ou HTTP :

1. Sélectionnez **Gestion > ThinState** dans le Panneau de configuration.
2. Sélectionnez **l'image HP ThinPro**, puis **Suivant**.
3. Sélectionnez **restaurer une image HP ThinPro**, puis **Suivant**.
4. Sélectionnez le protocole HTTP ou FTP, puis entrez les informations du serveur dans les champs.

   REMARQUE : Les champs **Username** (Nom d'utilisateur) et **Password** (Mot de passe) sont facultatifs si vous utilisez le protocole HTTP.

5. Si vous souhaitez conserver les paramètres précédemment configurés, cochez **Conserver la configuration de HP ThinPro**.
6. Sélectionnez **Terminer**.

   Lorsque le déploiement d'image commence, toutes les applications s'arrêtent et une nouvelle fenêtre s'affiche pour montrer la progression. En cas de problème, sélectionnez **Détails** pour plus d'informations. Le bureau réapparaît à la fin du déploiement.

   REMARQUE : Une vérification MD5sum est effectuée uniquement si le fichier MD5 est présent sur le serveur.

Capture d'une image HP ThinPro sur une unité flash USB

Pour capturer une image HP ThinPro sur une unité flash USB :

IMPORTANT : Sauvegardez toutes les données sur un lecteur flash USB avant de démarrer. HP ThinState formate automatiquement l'unité flash USB pour créer une unité flash USB amorçable. Cette opération efface toutes les données actuellement sur l'unité flash USB.

1. Sélectionnez **Gestion > ThinState** dans le Panneau de configuration.
2. Sélectionnez **l'image HP ThinPro**, puis **Suivant**.
3. Sélectionnez **copier l'image HP ThinPro**, puis **Suivant**.

4. Sélectionnez **créer une clé USB amorçable**, puis **Suivant**.

   Le client léger redémarre et puis vous invite à entrer un lecteur flash USB.

5. Insérez une clé USB dans un port USB du client léger.

6. Sélectionnez une unité flash USB amorçable, puis **Terminer**.

   Une nouvelle fenêtre affiche la progression. En cas de problème, sélectionnez **Details** (Détails) pour plus d'informations. Le bureau réapparaît à la fin de la capture.

Déploiement d'une image HP ThinPro avec une unité flash USB

Pour déployer une image HP ThinPro avec une unité flash USB :

IMPORTANT : Si vous abandonnez un déploiement avant la fin, l'image précédente ne sera pas restaurée et le contenu de l'unité flash USB du client léger sera corrompu. Dans cet État, le client léger doit être ré-imagé à l'aide d'une unité flash USB.

1. Mettez hors tension le client léger cible.

2. Insérez l'unité flash USB.

3. Mettez le client léger sous tension.

REMARQUE : L'écran reste noir pendant 10 à 15 secondes pendant que le client léger détecte l'unité flash USB et démarre à partir de cette dernière. Si le client léger ne parvient pas à démarrer à partir de l'unité flash USB, essayez de débrancher tous les autres périphériques USB et répétez cette procédure.

Gestion d'un profil de client

Un profil de client contient les connexions, les paramètres et les personnalisations de l'avancée qui ont été configurées à l'aide du gestionnaire de connexion et du Panneau de configuration. Un profil est enregistré dans un fichier de configuration qui est spécifique à la version de HP ThinPro dans laquelle il a été créé.

REMARQUE : Un profil de client peut également être préconfiguré et déployé à l'aide de Profil Editor et de Automatic Update (reportez-vous aux sections Profile Editor à la page 74 et HP Smart Client Services à la page 69 pour plus d'informations).

Enregistrement d'un profil de client sur un serveur FTP

Pour enregistrer un profil de client sur un serveur FTP :

IMPORTANT : Le répertoire du serveur FTP où vous envisagez d'enregistrer le profil doit exister avant de démarrer l'enregistrement.

1. Sélectionnez **Gestion > ThinState** dans le Panneau de configuration.

2. Sélectionnez **la configuration HP ThinPro**, puis **Suivant**.

3. Sélectionnez **Enregistrer la configuration**, puis **Suivant**.

4. Sélectionnez **sur un serveur FTP**, puis **Suivant**.

5. Entrez les informations du serveur FTP dans les champs.

6. Sélectionnez **Terminer**.

Restauration d'un profil de client avec le protocole FTP ou HTTP

Pour restaurer un profil de client avec le protocole FTP ou HTTP :

1. Sélectionnez **Gestion > ThinState** dans le Panneau de configuration.
2. Sélectionnez **la configuration HP ThinPro**, puis **Suivant**.
3. Sélectionnez **Restaurer une configuration**, puis sélectionnez **Suivant**.
4. Sélectionnez **sur un serveur distant**, puis **Suivant**.
5. Sélectionnez le protocole HTTP ou FTP, puis entrez les informations du serveur dans les champs.

   REMARQUE : Les champs **Nom d'utilisateur** et **Mot de passe** sont facultatifs si vous utilisez le protocole HTTP.

6. Sélectionnez **Terminer**.

Enregistrement d'un profil de client sur une unité flash USB

Pour enregistrer un profil de client sur une unité flash USB :

1. Insérez une clé USB dans un port USB du client léger.
2. Sélectionnez **Gestion > ThinState** dans le Panneau de configuration.
3. Sélectionnez **la configuration HP ThinPro**, puis **Suivant**.
4. Sélectionnez **Enregistrer la configuration**, puis **Suivant**.
5. Sélectionnez **sur une clé USB**, puis **Suivant**.
6. Sélectionnez l'unité flash USB.
7. Sélectionnez **Parcourir**.
8. Accédez à l'emplacement souhaité dans l'unité flash USB, puis attribuez un nom de fichier au profil.
9. Sélectionnez **Enregistrer**.
10. Sélectionnez **Terminer**.

Restauration d'un profil de client à partir d'une unité flash USB

Pour restaurer un profil de client à partir d'une unité flash USB :

1. Insérez l'unité flash USB contenant le profil dans un port USB du client léger cible.
2. Sélectionnez **Gestion > ThinState** dans le Panneau de configuration.
3. Sélectionnez **la configuration HP ThinPro**, puis **Suivant**.
4. Sélectionnez **Restaurer une configuration**, puis sélectionnez **Suivant**.
5. Sélectionnez **sur une clé USB**, puis **Suivant**.
6. Sélectionnez la clé USB.
7. Sélectionnez **Parcourir**.
8. Double-cliquez sur le fichier de configuration de votre choix sur la clé USB.
9. Sélectionnez **Terminer**.

Utilisation de VNC Shadow

Virtual Network Computing (VNC) est un protocole de commande à distance qui vous permet de consulter le bureau d'un ordinateur distant et de le contrôler avec votre souris et clavier locaux.

Pour augmenter la sécurité, HP recommande de laisser VNC désactivé, à moins que cela ne soit nécessaire pour le diagnostic à distance. Ensuite, désactivez VNC lorsque l'accès distant vers le client léger n'est plus nécessaire.

Pour accéder à l'outil VNC Shadow :

▲ Sélectionnez **Manageability**, puis sélectionnez **VNC Shadow** dans le Panneau de configuration.

REMARQUE : Vous devez redémarrer le client léger pour que les changements apportés aux options de Contrôle à distance (VNC) puissent s'appliquer.

Le tableau suivant décrit les options disponibles dans l'outil Contrôle à distance (VNC).

Option	Description
Activer le contrôle à distance	Active le contrôle à distance VNC.
Lecture seule	Configure la session VNC en lecture seule.
Utiliser un mot de passe	Exige la saisie d'un mot de passe pour accéder au client léger avec VNC. Sélectionnez **Définir le mot de passe** pour définir le mot de passe.
Afficher le bouton « Arrêt du contrôle à distance »	Lorsque cette option est activée, un bouton **Arrêt du contrôle à distance** s'affiche dans le coin supérieur gauche du système distant. Il stoppe le contrôle à distance VNC lorsqu'il est enfoncé.
Autoriser bouclage VNC uniquement	Si cette option est activée, vous pouvez vous connecter au serveur VNC uniquement à partir de ce client léger qui est identifié par l'adresse de bouclage.
Délais pour que l'utilisateur accepte la prise de contrôle	Active une boîte de dialogue de notification sur le système distant qui informe l'utilisateur distant lorsqu'une personne utilise VNC pour accéder au client léger. L'utilisateur peut refuser ou autoriser l'accès.
Fermer automatiquement la notification après (secondes)	Ferme le message de notification utilisateur après x secondes.
Message de notification	Vous permet d'afficher un message dans la boîte de dialogue de notification à destination de l'utilisateur distant.
À défaut, refuser les connexions	Si cette option est activée, la connexion VNC est refusée par défaut à l'expiration du délai.
Redémarrer le serveur VNC maintenant	Réinitialise le serveur VNC après l'application des nouveaux paramètres.

Périphériques d'entrée

Option de menu	Description
Clavier	Vous permet de modifier la disposition du clavier pour l'adapter à la langue utilisée pour le clavier principal et le clavier secondaire.
Raccourcis clavier	Vous permet de créer, modifier et supprimer des raccourcis clavier.
Souris	Vous permet de définir la vitesse de la souris et de spécifier si la souris est configurée pour un droitier ou un gaucher.

Option de menu	Description
	Clients légers avec un pavé tactile, cette option de menu vous permet également de désactiver ou d'activer le pavé tactile.
Écran tactile	Vous permet de configurer les options de l'écran tactile.
Ibus	Vous permet de configurer Ibus (intelligent Input Bus) pour une entrée multilingue. Ibus n'est pas activé par défaut. Pour activer Ibus : **Panneau de configuration > Périphériques d'entrée > Méthode d'entrée Ibus > Démarrer IBUS au démarrage** Il est également possible de modifier ou de restaurer les paramètres d'usine du fichier de configuration Ibus à partir du panneau de configuration par défaut. Après le redémarrage, l'icône de la barre Ibus apparaît. Sélectionnez l'icône pour sélectionner une langue. Cliquez avec le bouton droit sur l'icône pour plus d'options de configuration. **REMARQUE :** Ibus dans ThinPro est préchargé avec des langues chinoises, japonaises et coréennes. Pour ajouter des langues supplémentaires : 1. Cliquez avec le bouton droit sur l'icône de la barre système Ibus. 2. Sélectionnez l'onglet **Méthode d'entrée**. 3. Sélectionnez **Ajouter**.

Matériel

Option de menu	Description
Affichage	Permet de configurer et de tester les options d'affichage. Pour plus d'informations, reportez-vous à la section Gestionnaire d'affichage à la page 64.
Son	Vous permet de contrôler la lecture, les périphériques d'entrée et les niveaux d'entrée audio.
Gestionnaire USB	Vous permet de configurer les options de redirection des périphériques USB. Pour plus d'informations, reportez-vous à la section Redirection des périphériques USB à la page 65.
Gestionnaire séquentiel	Vous permet de configurer les périphériques série.
Imprimantes	Vous permet de configurer des imprimantes locales et réseau. Les imprimantes locales peuvent être partagées sur le réseau. Pour plus d'informations, reportez-vous à la section Configuration des imprimantes à la page 65.

Gestionnaire d'affichage

Le Gestionnaire d'affichage vous permet de configurer les paramètres de l'écran et d'appliquer ces modifications à la session. Pour ouvrir le gestionnaire d'affichage :

Panneau de configuration > Matériel > Gestionnaire d'affichage.

Redirection des périphériques USB

Pour rediriger des périphérique USB :

1. Dans le Panneau de configuration, sélectionnez **Matériel**, puis sélectionnez **Gestionnaire USB**.
2. Sur la page **Protocole**, sélectionnez un protocole distant.

   Si le paramètre est **Local**, vous pouvez également spécifier les options **autoriser le montage des périphériques** et **périphériques montés en lecture seule**.
3. Sur la page **Périphériques**, vous pouvez activer ou désactiver la redirection de chacun des périphériques si nécessaire.
4. Sur la page de **Classes**, vous pouvez sélectionner les classes de périphériques spécifiques à rediriger vers des sessions à distance.
5. Lorsque vous avez terminé, cliquez sur **Appliquer**.

Configuration des imprimantes

Pour configurer une imprimante :

1. Sélectionnez **Matériel**, puis **Imprimantes** dans le Panneau de configuration.
2. Dans la boîte de dialogue **Printing** (Impression), sélectionnez **Add** (Ajouter).
3. Dans la boîte de dialogue **New Printer** (Nouvelle imprimante), sélectionnez l'imprimante à configurer, puis sélectionnez **Forward** (Continuer).

   REMARQUE : Si vous sélectionnez une imprimante série, veillez à entrer les bons paramètres sur le côté droit de la boîte de dialogue. Dans le cas contraire, l'imprimante est susceptible de ne pas fonctionner correctement.
4. Sélectionnez la marque de l'imprimante. En cas de doute, sélectionnez l'option **Generic (recommended)** (Générique - recommandé), puis sélectionnez **Forward** (Continuer).
5. Sélectionnez le modèle et le pilote de l'imprimante, puis sélectionnez **Forward** (Continuer).

   REMARQUE : Si vous ne savez pas quel modèle d'imprimante ou pilote utiliser, ou si le modèle de votre imprimante ne figure pas dans la liste, sélectionnez **Back** (Retour) et essayez d'utiliser l'option **Generic (recommended)** (Générique - recommandé) lors de la sélection de la marque de l'imprimante.

   Si vous utilisez **Generic (recommended)** (Générique - recommandé), assurez-vous de sélectionner **text-only (recommended)** (Texte seul - recommandé) pour le modèle et **Generic text-only printer [en] (recommended)** (Imprimante texte seul générique [en] - recommandé) pour le pilote.
6. Remplissez les informations facultatives sur l'imprimante, telles que son nom et son emplacement.

   REMARQUE : HP vous recommande d'entrer le nom du pilote approprié dans la zone **Windows Driver** (Pilote Windows). Le pilote doit également être installé sur le serveur Windows pour que l'imprimante fonctionne correctement. Si un pilote n'est pas spécifié, un pilote Postscript générique est utilisé. L'utilisation d'un pilote Windows spécifique peut permettre plus de fonctions pour l'imprimante.
7. Sélectionnez **Apply** (Appliquer), puis imprimez une page de test si vous le souhaitez.

Répétez cette procédure pour configurer des imprimantes supplémentaires si nécessaire.

CONSEIL : L'utilisation d'un mauvais pilote pour l'imprimante est le problème le plus courant. Pour modifier le pilote, cliquez avec le bouton droit sur l'imprimante et sélectionnez **Properties** (Propriétés), puis changez la marque et le modèle.

Apparence

Option de menu	Description
Gestionnaire d'image de fond	Permet de configurer le thème d'arrière-plan et d'afficher de façon dynamique les informations sur le système (telles que le nom d'hôte, l'adresse IP, le modèle du matériel et l'adresse MAC du client léger) en arrière-plan. Pour plus d'informations à ce sujet, consultez le livre blanc HP ThinPro *Login Screen Customization* (disponible en anglais uniquement).
Centre de personnalisation	Vous permet d'effectuer l'une des opérations suivantes : • Basculer entre les configurations ThinPro et Smart Zero • Configurer les options du bureau et de la barre des tâches • Sélectionnez les types de connexions et les éléments du Panneau de configuration auxquels les utilisateurs ont accès. Pour plus d'informations, reportez-vous à la section Centre de personnalisation à la page 66.
Langue	Vous permet d'afficher l'interface HP ThinPro dans une autre langue.

Centre de personnalisation

Pour ouvrir Customization Center (Centre de personnalisation) :

▲ Sélectionnez **Appearance** (Apparence), puis sélectionnez **Customization Center** (Centre de personnalisation) dans le Panneau de configuration.

Le bouton en haut de la page **Bureau** permet de basculer entre les configurations ThinPro et Smart Zero. Reportez-vous à la section Choix d'une configuration OS à la page 1 pour plus d'informations sur les différences entre les deux configurations.

REMARQUE : Lors du passage entre ThinPro et Smart Zero, la connexion Smart Zero est automatiquement utilisée si vous n'avez configuré qu'une seule connexion. Si vous avez configuré plusieurs connexions, vous êtes invité à sélectionner la connexion à utiliser.

Avant de passer en mode Smart Zero, la fonction d'authentification du domaine sur le client léger doit être désactivée. L'authentification du domaine et le mode Smart Zero sont incompatibles.

Le tableau suivant décrit les autres options disponibles sur la page **Bureau**.

Option	Description
Lancer le Gestionnaire de connexions au démarrage	Lorsque cette option est activée, le gestionnaire de connexion se lance automatiquement au démarrage du système.
Activer le menu contextuel	Désactivez cette option pour désactiver le menu contextuel qui s'affiche lorsque vous effectuez un clic droit sur le bureau.

Option	Description
Activer la sécurité du contrôle d'accès du serveur X	Lorsque cette option est activée, seuls les systèmes répertoriés sous **Liste de contrôle d'accès XHost** sont autorisés à contrôler le client léger à distance.
Activer la mise à jour USB	Permet l'installation des mises à jour à partir d'une unité flash USB. Pour plus d'informations, reportez-vous à la section Mises à jour USB à la page 82.
Certifier la mise à jour USB	Désactivez cette option pour autoriser les utilisateurs standard à installer les mises à jour via USB.
Autoriser l'utilisateur à passer en mode administrateur	Désactivez cette option pour retirer l'option **Commutation mode administrateur/utilisateur** du Panneau de configuration en mode Utilisateur.
Délai avant annulation du mode Administrateur	Spécifie la temporisation d'attente (en minutes) après laquelle le mode Administrateur se termine. Si la valeur est égale ou inférieure à 0, le mode Administrateur ne se termine jamais.

Utilisez les pages **Connexions** et **Applications** pour sélectionner les types de connexions et les applications du Panneau de configuration disponibles en mode Utilisateur.

Utilisez la page **Barre des tâches** pour configurer la barre des tâches.

10 System Information (Informations système)

Dans le menu Démarrer, sélectionnez **Informations système** pour afficher les informations sur le système, le réseau et les logiciels. Le tableau suivant décrit les informations qui s'affichent dans chaque panneau.

Panneau	Description
Général	Affiche des informations sur le BIOS, le système d'exploitation, le processeur et la mémoire.
Réseau	Affiche des informations sur l'interface réseau, la passerelle et les paramètres DNS.
Outils réseau	Fournit les outils suivants à des fins de contrôle et de dépannage : • **Ping** : Spécifiez l'adresse IP d'un autre périphérique du réseau pour essayer d'établir un contact. • **Recherche DNS** : Utilisez cet outil pour résoudre un nom de domaine en adresse IP. • **Trace Route** : Utilisez cet outil pour suivre le chemin pris par un paquet réseau d'un appareil à un autre.
Informations logicielles	Affiche une liste des modules complémentaires installés sur l'onglet **Service Packs** et des informations de version du logiciel sur l'onglet **Logiciels installés**. **CONSEIL :** Vous pouvez également accéder au manuel de l'administrateur (ce document) depuis cet écran.
Licence officielle	Affiche le contrat de licence pour le système d'exploitation HP ThinPro et, s'il n'est pas sous licence automatique, des informations sur les licences ThinPro sur le système.
Journaux système	Affiche les journaux suivants : • Autorisation et sécurité • Gestionnaire de connexion • Baux DHCP • Journal du système général • Noyau • Gestionnaire de réseau • Services Smart Client • Serveur X • OneSign En mode Administrateur, le niveau de débogage peut être modifié pour afficher des informations supplémentaires qui pourront être demandées par l'assistance HP à des fins de dépannage. Sélectionnez **Diagnostic** pour enregistrer un fichier de diagnostic. Pour plus d'informations, reportez-vous à la section Utilisation des diagnostics système à des fins de résolution des problèmes à la page 80.

REMARQUE : Reportez-vous à la section SystemInfo à la page 158 pour plus d'informations sur les clés de registre qui permettent de masquer les écrans des informations système.

11 HP Smart Client Services

HP Smart Client Services est un ensemble d'outils serveur qui vous permettent de configurer des profils client qui peuvent être distribués vers un grand nombre de clients légers. Cette fonction est appelée la mise à jour automatique.

HP ThinPro détecte un serveur de mise à jour automatique au démarrage et effectue leur propre configuration en conséquence. L'installation et la maintenance des périphérique s'en trouvent simplifiées.

Système d'exploitation pris en charge

HP Smart Client Services prend en charge les systèmes d'exploitation suivants :

- Windows Server® 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows 7
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2003
- Windows Vista®
- Windows XP

REMARQUE : Le programme d'installation est uniquement de type 32 bits, mais il est pris en charge à la fois par les versions 32 bits et 64 bits du système d'exploitation Windows.

Configuration requise pour HP Smart Client Services

Avant d'installer HP Smart Client Services, vérifiez la configuration et l'installation des composants suivants :

- **Internet Information Services (IIS)**
- **.NET Framework 3.5**

Pour en savoir plus sur l'installation ou l'activation de ces composants sur le système d'exploitation que vous utilisez pour le serveur, rendez-vous sur http://www.microsoft.com.

Obtention de HP Smart Client Services

Pour obtenir HP Smart Client Services, accédez à ftp://ftp.hp.com/pub/tcdebian/SmartClientServices/.

Consultation du site Web d'Automatic Update (Mise à jour automatique)

1. Sur le bureau du serveur, sélectionnez **Démarrer > Panneau de configuration**, puis **Outils d'administration**.
2. Double-cliquez sur **Gestionnaire des services Internet (IIS)**.
3. Dans le volet gauche du gestionnaire IIS, développez les éléments suivants :

   « Nom du serveur » > Sites > Mise à jour automatique HP > auto-update

REMARQUE : L'emplacement physique dans lequel les fichiers d'Automatic Update seront stockés est :

```
C:\Program Files (x86)\HP\HP Smart Client Service\auto-update
```

Création d'un profil Automatic Update (Mise à jour automatique)

Automatic Update utilise des profils pour déployer une configuration sur des clients légers. Par défaut, lorsque vous créez un profil à l'aide de Profile Editor (consultez la section Profile Editor à la page 74), cet outil vous permet de l'enregistrer dans le dossier suivant :

```
C:\Program Files (x86)\HP\HP Smart Client Service\auto-update
\PersistentProfile\
```

Vous pouvez également exporter un profil existant à partir d'un client léger avec HP ThinState, puis copier le profil à cet emplacement.

Lors de la recherche de mises à jour, HP ThinPro examine ce dossier et applique le profil qui y est enregistré. Cela permet de s'assurer que tous les clients légers utilisent la même configuration.

Profils spécifiques à une adresse MAC

Les profils Automatic Update peuvent être créés pour une adresse MAC unique. Cela peut s'avérer utile lorsque certains clients légers nécessitent une configuration différente.

Les profils pour une adresse MAC unique doivent être stockés sur le serveur Automatic Update, dans le dossier suivant :

```
C:\Program Files (x86)\HP\HP Smart Client Service\auto-update
\PersistentProfile\MAC\
```

Lors de la recherche de mises à jour, HP ThinPro recherche d'abord le profil générique, puis un profil spécifique à une adresse MAC. Ces profils sont fusionnés et installés sur le client léger. Le profil spécifique à une adresse MAC prévaut sur les autres profils. Autrement dit, si la même clé de registre est associée à des valeurs différentes dans les deux fichiers, c'est la valeur du profil spécifique à l'adresse MAC qui est utilisée.

Cela permet de s'assurer qu'une configuration partagée peut être fournie à tous les clients légers, mais une personnalisation spécifique peut être ajoutée, si nécessaire.

Cette section décrit comment créer un profil Automatic Update pour une adresse MAC.

1. Obtenir l'adresse MAC du client léger à l'aide des infos sur le système. Par exemple, la procédure suivante utilise l' adresse MAC `00fcab8522ac`.
2. Utilisez Profile Editor pour créer ou modifier un profil de client (reportez-vous à la section Profile Editor à la page 74), puis enregistrez le profil de client lorsque vous êtes prêt.
3. Dans **Profile Editor**, sélectionnez **Terminer** dans le panneau de gauche pour accéder au panneau **Profil actuel**.
4. Sélectionnez **Enregistrer le profil sous** pour enregistrer le profil du client comme suit :

   ```
   C:\Program Files (x86)\HP\HP Smart Client Service\auto-update
   \PersistentProfile\MAC\00fcab8522ac.xml
   ```

5. Sélectionnez le bouton **Terminer** dans le panneau **Profil actuel** pour quitter Profile Editor.
6. Redémarrez le client léger qui utilise l'adresse MAC spécifiée pour lancer le processus de mise à jour automatique.

Mise à jour de clients légers

Utiliser la méthode de mise à jour par diffusion

Pour effectuer une mise à jour par diffusion, branchez le client sur le même réseau que le serveur de mise à jour. Une mise à jour par diffusion repose sur HP Smart Client Services, qui fonctionne avec IIS pour transmettre automatiquement les mises à jour au client léger.

REMARQUE : Les mises à jour par diffusion fonctionnent uniquement si le client léger se trouve sur le même sous-réseau que le serveur.

CONSEIL : Pour vérifier que les mises à jour par diffusion fonctionnent, exécutez Profile Editor et effectuez quelques modifications. Connectez le client léger et vérifiez qu'il a téléchargé le nouveau profil. Dans le cas contraire, reportez-vous à la section Dépannage à la page 79.

Utilisation de la méthode de mise à jour par balisage DHCP

Sur les systèmes Windows Server, le balisage DHCP permet à un client léger de se mettre à jour. Utilisez cette méthode pour mettre à jour des clients légers spécifiques ; Cependant, si vous n'avez qu'un ou deux clients à mettre à jour, envisagez plutôt d'utiliser la méthode de mise à jour manuelle. Dans le cas contraire, HP recommande la méthode de mise à jour par diffusion.

Exemple de balisage DHCP

L'exemple de cette section montre comment effectuer un balisage DHCP sur un serveur Windows 2008 R2 Server.

REMARQUE : Pour utiliser le balisage DHCP, reportez-vous à la documentation de votre serveur DHCP.

1. Sur le bureau du serveur, sélectionnez **Démarrer** > **Outils d'administration** > **DHCP**.
2. Dans le panneau gauche de l'écran **DHCP**, sélectionnez sur le domaine où les clients légers sont connectés.
3. Dans le panneau droit de l'écran **DHCP**, développez la section **IPv4** et cliquez avec le bouton droit, puis sélectionnez **Set Predefined Options** (Configurer les options prédéfinies).
4. Dans la boîte de dialogue **Predefined Options and Values** (Options et valeurs prédéfinies), sélectionnez **Add** (Ajouter).

5. Dans la zone **Option Type** (Type d'option), configurez les options comme indiqué dans le tableau ci-dessous.

Champ	Entrée
Name (Nom)	Saisissez `auto-update`.
Data type (Type de données)	Sélectionnez **String** (Chaîne).
Code	Saisissez `137`.
Description	Saisissez `HP Automatic Update`.

6. Sélectionnez **OK**.
7. Dans la boîte de dialogue **Predefined Options and Values** (Options et valeurs prédéfinies), sous **Value (Valeur) > String (Chaîne)**, saisissez l'adresse du serveur de mise à jour en utilisant le format suivant :

   `http://auto-update.dominio.com:18287/auto-update`

8. Pour terminer la configuration, sélectionnez **OK**. Le balayage DHCP est maintenant prêt à mettre à jour des clients légers spécifiques.

Utilisation de la méthode de mise à jour dite DNS

Au cours du démarrage du système, Automatic Update tente de résoudre l' **l'auto-update** par alias DNS. Si ce nom d'hôte est résolu, il tente de vérifier la présence de mises à jour sur **http://auto-update: 18287**. Cette méthode de mise à jour permet aux clients légers d'accéder à un serveur de mise à jour unique à travers l'ensemble du domaine, en simplifiant ainsi la gestion des déploiements avec de nombreux sous-réseaux et serveurs DHCP.

Pour configurer la méthode de mise à jour par alias DNS :

▲ Modifiez le nom d'hôte du serveur hébergeant HP Smart Client Services en le remplaçant par **auto-update** ou créez un alias DNS de **auto-update** pour ce serveur.

Utilisation de la méthode de mise à jour manuelle

Utilisez la méthode de mise à jour manuelle pour connecter un client léger à un serveur spécifique pour une mise à jour. En outre, utilisez cette méthode si vous souhaitez tester une mise à jour sur un seul client léger avant de la distribuer à de nombreux clients légers, ou si vous avez des mises à jour spécifiques à installer sur seulement un ou deux clients légers.

REMARQUE : Assurez-vous d'avoir spécifié le nom d'hôte du serveur manuel dans le profil vers lequel s'effectue la mise à jour. Sinon, les paramètres automatiques sont rétablis lors du téléchargement du profil. Utilisez **Profile Editor** pour modifier ces paramètres à la racine/auto-update.

REMARQUE : Si plusieurs clients légers nécessitent des mises à jour particulières, servez-vous de la méthode de balisage DHCP.

Si aucune discrimination n'est nécessaire pour la mise à jour, utilisez la méthode de mise à jour Broadcast.

Mise à jour manuelle

1. Sélectionnez **Administration > Mise à jour automatique** dans le Panneau de configuration.
2. Sélectionnez **Activer la configuration manuelle**.
3. Définissez l'option **Protocole** sur **http**.

4. Dans le champ **Serveur**, saisissez le nom d'hôte et le port du serveur de mise à jour dans ce format :

   `<Nom hôte>:18287`

5. Dans le champ **Chemin**, saisissez ce qui suit :

   `auto-update`

6. Si vous souhaitez conserver les paramètres précédemment configurés, cochez **Conserver la configuration du client léger**.

7. Sélectionnez **OK** pour que le client léger extraie les mises à jour.

12 Profile Editor

HP Smart Client Services contient Profil Editor, qui permet aux administrateurs de créer des profils client et de les télécharger sur le serveur de mise à jour automatique.

CONSEIL : En plus de créer un nouveau profil de client, vous pouvez modifier un profil existant ayant été exporté à l'aide de HP ThinState.

Un profil de client contient les connexions, les paramètres et les personnalisations de l'avancée qui ont été configurées à l'aide du gestionnaire de connexion et divers éléments du Panneau de configuration. Un profil de client est enregistré dans un fichier de configuration qui est spécifique à la version de HP ThinPro dans laquelle il a été créé.

Ouverture de Profile Editor

▲ Sélectionnez **Start** (Démarrer), sélectionnez **All Programs** (Tous les programmes), sélectionnez **HP**, sélectionnez **HP Automatic Update Server** (Serveur de mise à jour automatique HP), puis sélectionnez **Profile Editor**.

Chargement d'un profil de client

Le nom du profil de client actuellement chargé est indiqué sur l'écran initial de Profile Editor.

Pour charger un autre profil de client :

1. Dans l'écran initial de Profile Editor, sélectionnez le lien qui affiche le nom du profil de client actuellement chargé.
2. Accédez à un profil de client, puis sélectionnez **Open** (Ouvrir).

Personnalisation d'un profil de client

Sélection de la plateforme pour un profil de client

Utilisez l'écran de la **plateforme** dans Profile Editor pour effectuer les opérations suivantes :

- Sélectionnez la version d'image HP ThinPro souhaitée qui est compatible avec votre matériel
- Choix entre ThinPro et Smart Zero
- Affichez les kits clients installés qui fournissent des paramètres de registre supplémentaires

REMARQUE : Les kits clients doivent être placés dans le répertoire suivant :

`C:\Program Files (x86)\HP\HP Smart Client Service\auto-update\Packages`

Pour configurer les paramètres de la plate-forme d'un profil de client :

1. Sur l'écran de la **plateforme** dans Profile Editor, sélectionnez un **ID de version du système d'exploitation** qui correspond à la version d'image souhaitée.

IMPORTANT : N'oubliez pas de créer un profil de client différent pour chaque type de matériel.

REMARQUE : Si un kit client est installé, il s'affiche automatiquement dans la zone de Kits Client, et des paramètres de Registre supplémentaires seront disponibles sur l'écran de registre.

2. Définissez la configuration sur **Standard** (ThinPro) ou sur **Zero** (Smart Zero).

REMARQUE : Pour des versions plus anciennes de l'image, ce paramètre est grisé et défini automatiquement sur Zéro.

Configuration d'une connexion par défaut pour un profil de client

Pour configurer une connexion par défaut pour un profil de client :

1. Sur l'écran de **connexion** dans Profile Editor, sélectionnez le type de connexion souhaitée dans la liste déroulante de **Type**.

REMARQUE : Les types de connexion disponibles varient selon que vous avez choisi ThinPro ou Smart Zero dans l'écran de la plateforme.

2. Dans le champ **Server** (Serveur), saisissez le nom ou l'adresse IP du serveur.

Modification des paramètres de registre d'un profil de client

Pour modifier les paramètres de registre par défaut pour un profil de client :

1. Sur l'écran de **Registry** (Registry) de Profile Editor, développez les dossiers de l'arborescence des **paramètres de registre** pour localiser le paramètre de registre que vous souhaitez modifier.
2. Sélectionnez la clé de Registre et puis saisissez la valeur désirée dans le champ **Value** (Valeur).

REMARQUE : Reportez-vous à l'annexe Clés de registre à la page 85 pour obtenir la liste complète et la description des clés de registre.

Ajout de fichiers à un profil de client

Utilisez l'écran **Files** (Fichiers) dans Profile Editor pour ajouter des fichiers de configuration qui seront installés sur le client léger automatiquement lorsque le profil de client sera installé. Cette option est généralement utilisée pour les raisons suivantes :

- Ajouter des certificats
- Modifier des paramètres de périphérique lorsque les paramètres de registre concernés sont indisponibles
- Modifier le comportement du système en insérant des scripts personnalisés ou en modifiant des scripts existants

Vous pouvez également spécifier un lien symbolique qui pointe vers un fichier déjà installé sur le client léger. Utilisez cette option lorsque le fichier doit être accessible depuis plusieurs répertoires différents.

Ajout d'un fichier de configuration à un profil de client

1. Dans l'écran **Files** (Fichiers) de Profile Editor, sélectionnez **Add a file** (Ajouter un fichier).
2. Sélectionnez **Import File** (Importer un Fichier), localisez le fichier à importer et sélectionnez **Open** (Ouvrir).

REMARQUE : Les fichiers peuvent également être exportés à l'aide du bouton **Export file** (Exporter le fichier), si des informations plus détaillées sur ceux-ci sont nécessaires.

3. Dans le champ **Path** (Chemin d'accès), entrez le chemin d'accès où le fichier sera installé sur le client léger.

4. Dans la section **File details** (Détails sur le fichier), définir les champs **Owner** (Propriétaire), **Group** (Groupe) et **Permissions** (Autorisations) pour les valeurs appropriées.

   REMARQUE : En général, la définition du propriétaire et du groupe en tant que **root** et des autorisations en tant que **644** est satisfaisante. Si un propriétaire, un groupe ou des autorisations spéciales sont nécessaires, reportez-vous aux autorisations de fichier Unix® standard pour obtenir des consignes concernant la modifications des détails relatifs aux fichiers.

5. Sélectionnez **Save** (Enregistrer) pour terminer l'ajout du fichier de configuration au profil de client.

REMARQUE : Un fichier installé dans le cadre d'un profil écrasera automatiquement tout fichier existant sur le système de fichiers dans le chemin de destination. En outre, un second profil pour lequel le fichier n'est pas associé ne pourra pas rétablir les fichiers précédemment associés. Tous les fichiers qui ont été installés en étant associés à un profil sont permanents et doivent être rétablis manuellement ou via une réinitialisation des paramètres d'usine.

Ajout de certificats à un profil de client

Les profils des clients incluent systématiquement les certificats qui sont importés vers un magasin de certificats client standard pour les applications suivantes :

- VMware Horizon View, Citrix, RDP
- Mise à jour automatique
- HP Smart Client Services
- Boutiques sur navigateur Web

Pour importer d'autres certificats vers un profil de client :

1. Dans l'écran **Files** (Fichiers) de Profile Editor, sélectionnez **Add a file** (Ajouter un fichier).
2. Sélectionnez **Import File** (Importer Fichier), recherchez le certificat, puis cliquez sur **Open** (Ouvrir).

   REMARQUE : Le certificat doit être au format de fichier `.pem` ou `.crt`.

3. Dans le champ **Path** (Chemin d'accès), définissez le chemin d'accès suivant :

   `/usr/local/share/ca-certificates`

4. Cliquez sur **Save** (Enregistrer) pour finir d'ajouter le certificat au profil de client.
5. Après avoir installé le profil de client, utilisez **Certificate Manager** (Gestionnaire de certificats) pour confirmer que le certificat a été importé correctement.

Ajout d'un lien symbolique à un profil de client

1. Dans l'écran **Files** (Fichiers) de Profile Editor, sélectionnez **Add a file** (Ajouter un fichier).
2. Dans la liste déroulante **Type**, sélectionnez **Link** (Lien).
3. Dans la section **Symbolic link details** (Détails du lien symbolique), définissez le champ **Link** (Lien) au chemin d'accès du fichier souhaité déjà installé sur le client léger.
4. Cliquer **Save** (Enregistrer) pour terminer l'ajout du lien symbolique.

Enregistrement de profil de client

1. Dans **Profile Editor**, sélectionnez **Finish** (Terminer) dans le panneau gauche pour accéder à l'écran **Current profile** (Profil actuel).
2. Sélectionnez **Save Profile** (Enregistrer le profil) pour enregistrer le profil de client actuel ou sélectionnez **Save Profile As** (Enregistrer le profil sous) pour l'enregistrer sous forme de nouveau profil de client.

   REMARQUE : Si **Save Profile** (Enregistrer le profil) est désactivé, votre profil de client n'a pas changé depuis la dernière connexion où il a été enregistré.

3. Sélectionnez le bouton **Finish** (Terminer) dans l'écran **Current Profile** (Profil actuel) pour quitter Profile Editor.

Configuration d'une imprimante série ou parallèle

Vous pouvez utiliser Profile Editor pour configurer les ports d'imprimante série ou parallèle. Une imprimante USB est automatiquement mappée lors de sa connexion.

Obtention des paramètres de l'imprimante

Avant de configurer les ports de l'imprimante, obtenez les paramètres de l'imprimante. Si elle est disponible, consultez la documentation de l'imprimante avant de poursuivre. Si ce n'est pas le cas, procédez comme suit :

1. Pour la plupart des imprimantes, maintenez enfoncé le bouton d'**Alimentation** tout en allumant l'appareil.
2. Après quelques secondes, relâchez le bouton d'**Alimentation**. Ceci permet à l'imprimante de passer en mode de test et d'imprimer les informations requises.

   CONSEIL : Il se peut que vous ayez à mettre l'imprimante hors tension pour annuler le mode de test ou à appuyer de nouveau sur **Alimentation** pour imprimer une page de diagnostic.

Configuration des ports de l'imprimante

1. Dans **Profile Editor**, sélectionnez **Registre** puis cochez la case **Afficher tous les paramètres**.
2. Activez le mappage de port de l'imprimante correspondant à votre type de connexion :
   - Citrix : Aucune action n'est requise.
   - RDP : Accédez à **root > ConnectionType > freerdp**. Cliquez avec le bouton droit sur le dossier **connections**, sélectionnez **New connection** (Nouvelle connexion), puis **OK**. Définissez la clé de registre **portMapping** sur `1` pour activer le mappage de port d'imprimante.
   - VMware Horizon View : Accédez à **root > ConnectionType > view**. Cliquez avec le bouton droit sur le dossier **connections**, sélectionnez **New connection** (Nouvelle connexion), puis **OK**. Sous le dossier **xfreerdpOptions**, définissez la clé de registre **portMapping** sur `1` pour activer le mappage de port d'imprimante.
3. Accédez à **root > Serial**. Cliquez avec le bouton droit sur le dossier **Serial**, sélectionnez **New UUID** (Nouveau UUID), puis sélectionnez **OK**.
4. Sous le nouveau répertoire, définissez les valeurs **baud**, **dataBits**, **flow** et **parity** sur les valeurs obtenues dans la section Obtention des paramètres de l'imprimante à la page 77.

   Définissez la valeur de **device** sur le port auquel l'imprimante sera branchée. Par exemple, le premier port série serait `/dev/ttyS0`, le deuxième port série serait `/dev/ttyS1` et ainsi de suite. Pour les

imprimantes série USB, utilisez le format `/std/ttyUSB #`, où # correspond au numéro du port, en commençant par 0.

Installation d'imprimantes sur le serveur

1. Sur le bureau Windows, sélectionnez **Démarrer** > **Imprimantes et télécopieurs**.
2. Sélectionnez **Ajouter une imprimante**, puis **Suivant**.
3. Sélectionnez **Local Printer attached to this Computer** (Imprimante locale connectée à cet ordinateur) et, si nécessaire, désélectionnez **Automatically detect and install my Plug and Play printer** (Détection et installation automatique de l'imprimante Plug-and-Play).
4. Lorsque vous avez terminé, sélectionnez **Suivant**.
5. Dans le menu, sélectionnez un port.

REMARQUE : Le port dont vous avez besoin se trouve dans la section de ports intitulée **TS###**, où ### est un nombre compris entre 000-009 ou 033-044. Le port approprié dépend de votre nom d'hôte et de l'imprimante que vous souhaitez installer. Par exemple, si vous avez ZTAHENAKOS comme nom d'hôte et une imprimante série, sélectionnez le port avec **(ZTAHENAKOS:COM1)**. Pour une imprimante parallèle, sélectionnez **(ZTAHENAKOS:LPT1)**. Le champ **TS###** est attribué par le serveur, il ne portera donc pas le même nom à chaque fois.

6. Sélectionnez le fabricant et le pilote de votre imprimante.

CONSEIL : Si vous le souhaitez, utilisez le disque de pilotes **Windows Update** pour installer le pilote.

REMARQUE : Pour des impressions simples ou de test, le type d'imprimante **Generic Manufacturer** (Fabricant générique) ou **Generic/Text Only** (Générique/Texte uniquement) est habituellement suffisant.

7. Si vous êtes invité à conserver le pilote existant et s'il est connu pour fonctionner, conservez-le, puis sélectionnez **Suivant**.
8. Donnez un nom à l'imprimante. Pour l'utiliser comme imprimante par défaut, sélectionnez **Oui**, puis **Suivant**.
9. Pour partager l'imprimante, sélectionnez **Nom de partage** et donnez-lui un nom de partage. Sinon, sélectionnez **Suivant**.
10. À la page suivante, vous pouvez demander l'impression d'une page de test. HP le recommande, car cela vous permettra de vérifier si l'imprimante a été configurée correctement. Si ce n'est pas le cas, vérifiez les paramètres et réessayez.

REMARQUE : Si le client léger se déconnecte du serveur, l'imprimante devra être reconfigurée la prochaine fois que le client léger se connectera.

13 Dépannage

Résolution des problèmes de connectivité réseau

1. Envoyez une commande ping au serveur en procédant comme suit :
   a. Sélectionnez le bouton des informations système dans la barre des tâches, puis sélectionnez l'onglet **Outils Net**.
   b. Sous **Sélectionner un outil**, sélectionnez **Ping**.
   c. Dans la zone **Hôte cible**, saisissez l'adresse du serveur, puis sélectionnez **Démarrer le processus**.

   En cas de succès de la commande ping, le système affiche la sortie suivante :

   ```
   Ping 10.30.8.52 (10.30.8.52) 56 (84) octets de données.
   ```

   ```
   64 octets à partir de 10.30.8.52:icmp_seq-1 ttl=64 time=0.81 5 ms 64
   octets à partir de 10.30.8.52:icmp_seq=2 ttl=64 time=0.735 ms
   ```

   Si la commande ping échoue, le client léger peut être déconnecté du réseau et connaître un long moment sans émission du système.
2. Si le client léger ne répond pas à la commande ping, effectuez les opérations suivantes :
   a. Vérifiez le câble réseau, ainsi que les paramètres réseau dans le Panneau de configuration.
   b. Essayez d'envoyer une commande ping à d'autres serveurs ou clients légers.
   c. Si vous pouvez accéder à d'autres clients légers, vérifiez que vous avez saisi l'adresse correcte du serveur.
   d. Envoyez une commande ping au serveur en utilisant l'adresse IP au lieu du nom de domaine ou vice-versa.
3. Vérifiez les journaux système en procédant comme suit :
   a. Sélectionnez le bouton des informations système dans la barre des tâches, puis sélectionnez l'onglet **Journaux système**.
   b. Recherchez d'éventuelles erreurs dans les journaux.
   c. En cas d'erreur, la notification **Server is not set up** (Le serveur n'est pas configuré) s'affiche. Vérifiez que le serveur est correctement configuré et que HP Smart Client Services est en cours d'exécution.

Résolution du problème d'expiration du mot de passe Citrix

Si les utilisateurs ne sont pas invités à modifier les mots de passe Citrix expirés, assurez-vous alors que le site XenApp Services (site PNAgent) dispose de la méthode d'authentification **Prompt** définie pour permettre aux utilisateurs de modifier les mots de passe expirés. Si vous autorisez les utilisateurs à changer leur mot de passe en se connectant directement au contrôleur du domaine, assurez-vous alors du moment où le client léger est synchronisé avec le contrôleur de domaine et utilisez le nom de domaine complet (par exemple, `domain_name.com`) lors de la saisie les informations d'authentification de connexion de Citrix. Pour plus d'informations, reportez-vous à la documentation Citrix.

Utilisation des diagnostics système à des fins de résolution des problèmes

Le diagnostic système prend un instantané du client léger qui peut être utilisé pour aider à résoudre les problèmes sans accéder physiquement au dit client léger. Cet instantané contient des fichiers journaux tirés des informations du BIOS et les processus actifs au moment où les diagnostics système ont été exécutés.

CONSEIL : Vous pouvez modifier le paramètre de **Niveau de débogage** dans l'onglet **Journaux système** de la fenêtre **Informations système** pour spécifier la quantité d'informations à inclure dans le rapport de diagnostic. Ces informations peuvent être requises par HP pour la résolution des problèmes. Étant donné que le système réinitialise les fichiers journaux lorsqu'il redémarre, veillez à capturer les fichiers journaux avant un redémarrage.

Pour les journaux les plus utiles, réglez le niveau pour capturer un haut niveau de détail avant de reproduire le problème et de créer un rapport de diagnostic.

Enregistrement des données des diagnostics système

1. Insérez une clé USB dans un port USB du client léger.
2. Sélectionnez le bouton des informations système dans la barre des tâches, puis sélectionnez l'onglet **Journaux système**.
3. Sélectionnez **Diagnostic** et enregistrez le fichier de diagnostic compressé **Diagnostic.tgz** sur l'unité flash USB.

Décompression des fichiers de diagnostic système

Le fichier de diagnostic système **Diagnostic.tgz** est compressé et doit être décompressé pour que vous puissiez consulter les fichiers de diagnostic.

Décompression des fichiers de diagnostic système avec les systèmes fonctionnant sous Windows

1. Téléchargez et installez une copie de la version Windows de **7-Zip**.

   REMARQUE : Vous pouvez obtenir une copie gratuite de 7-Zip pour Windows à l'adresse http://www.7-zip.org/download.html.

2. Insérez la clé USB qui contient le fichier de diagnostic système enregistré, puis copiez **Diagnostic.tgz** sur le bureau.
3. Cliquez avec le bouton droit de la souris sur **Diagnostic.tgz** et sélectionnez **7-zip > Extract files** (Extraire les fichiers...).
4. Ouvrez le nouveau dossier intitulé **Diagnostic** et répétez l'étape 3 avec **Diagnostic.tar**.

Décompression des fichiers de diagnostic système avec les systèmes fonctionnant sous Linux ou Unix

1. Insérez la clé USB qui contient le fichier de diagnostic système enregistré, puis copiez **Diagnostic.tgz** dans votre répertoire personnel.
2. Ouvrez une fenêtre de terminal et accédez à votre répertoire personnel.
3. Sur la ligne de commande, insérez `tar xvfz Diagnostic.tgz`.

Consultation des fichiers de diagnostic système

Les fichiers de diagnostic système sont répartis entre les dossiers **Commands** (Commandes), **/var/log** et **/etc**.

Consultation des fichiers du dossier Commands

Ce tableau décrit les fichiers à rechercher dans le dossier **Commands** (Commandes).

Fichier	Description
demidecode.txt	Ce fichier contient des informations sur les composants graphiques et le BIOS du système.
dpkg_--list.txt	Ce fichier répertorie les packages installés au moment où les diagnostics système ont été exécutés.
ps_-ef.txt	Ce fichier répertorie les processus actifs au moment où les diagnostics système ont été exécutés.

Consultation des fichiers du dossier /var/log

Le fichier utile dans le dossier **/var/log** est **Xorg.0.log**.

Consultation des fichiers du dossier /etc

Le dossier **/etc** contient le système de fichiers présent au moment où les diagnostics système ont été exécutés.

A Mises à jour USB

Lorsque les mises à jour USB sont activées (reportez-vous à la section Centre de personnalisation à la page 66), vous pouvez utiliser une unité flash USB pour installer simultanément plusieurs certificats et modules complémentaires et déployer un profil.

Pour effectuer des mises à jour USB :

1. Placez les fichiers souhaités sur une unité flash USB.

   REMARQUE : Les fichiers peuvent être placés dans le répertoire racine ou dans des sous-dossiers.

2. Connectez l'unité flash USB au client léger.

   Les mises à jour sont détectées automatiquement et affichées dans la boîte de dialogue **Mise à jour USB**, qui vous permet de rechercher et d'afficher des détails sur les mises à jour détectées.

3. Cochez les cases en regard des mises à jour que vous souhaitez installer, puis sélectionnez **Installer**.

4. Après l'installation, redémarrez le client léger si le système vous y invite.

HP ThinUpdate

HP ThinUpdate vous permet de télécharger les images et les modules complémentaires HP et de créer des unités flash USB amorçables pour le déploiement d'images. Pour plus d'informations, consultez le *Manuel de l'administrateur* HP ThinUpdate.

B Outils BIOS (clients légers de bureau uniquement)

Il existe deux types d'outils BIOS pour HP ThinPro :

- Outil des paramètres du BIOS : Utilisé pour récupérer ou modifier les paramètres du BIOS
- Outil de flashage du BIOS : Utilisé pour mettre à jour le BIOS

Ces outils peuvent être exécutés via un terminal X.

Outil des paramètres du BIOS

Le tableau suivant décrit la syntaxe de l'outil des paramètres du BIOS.

REMARQUE : Les modifications apportées prennent effet au redémarrage suivant.

Syntaxe	Description
`hptc-bios-cfg -G <nom fichier>`	Récupère les paramètres actuels du BIOS et les enregistre dans le fichier spécifié afin qu'ils puissent être consultés ou modifiés (CPQSETUP.TXT par défaut).
`hptc-bios-cfg -S <nom fichier>`	Écrit les paramètres du BIOS à partir du fichier spécifié (CPQSETUP.TXT par défaut) dans le BIOS.
`hptc-bios-cfg -h`	Affiche une liste d'options.

Outil de flashage du BIOS

Le tableau suivant décrit la syntaxe de l'outil de flashage du BIOS.

REMARQUE : Les modifications apportées prennent effet au redémarrage suivant.

Syntaxe	Description
`hptc-bios-flash <nom image>`	Prépare le système à la mise à jour du BIOS lors du redémarrage suivant. Cette commande copie automatiquement les fichiers à l'emplacement approprié et vous invite à redémarrer le client léger. **REMARQUE :** Cette commande nécessite que l'option **Tool-less update** du BIOS soit définie sur **Auto**.
`hptc-bios-flash -h`	Affiche une liste d'options.

C Redimensionnement de la partition de l'unité flash

IMPORTANT : Les clients légers HP livrés depuis usine avec HP ThinPro utilisent l'intégralité du lecteur flash. Les méthodes de capture d'image capturent l'image la plus petite possible, ce qui permet de déployer des images à partir d'unités flash plus grande sur des unités flash plus petites disposant de suffisamment d'espace pour l'image capturée. Plus aucun redimensionnement de la partition de l'unité flash ne devrait être nécessaire pour les clients légers HP livrés depuis l'usine avec HP ThinPro. Pour les clients légers avec HP ThinPro qui n'utilisent pas l'intégralité du lecteur flash pour une raison quelconque, consultez les informations suivantes.

Pour utiliser la totalité de l'espace de l'unité flash, vous devez modifier la taille de la partition et développer le système de fichiers pour occuper cet espace supplémentaire. Cette opération peut être effectuée en utilisant le script `resize-image` via un terminal X.

REMARQUE : Lorsqu'une image est déployée via HPDM, HP ThinState ou Automatic Update (Mise à jour automatique), le système de fichiers est automatiquement redimensionné pour utiliser tout l'espace disponible sur l'unité flash.

Le tableau suivant décrit la syntaxe du script `resize-image`.

Syntaxe	Description
`resize-image`	Lorsqu'il est appelé avec aucun paramètre, le script affiche la taille actuelle de la partition et la quantité d'espace disponible sur l'unité flash. Le script vous invite à entrer la taille de la partition cible et à confirmer la modification. La modification prend effet au prochain redémarrage du client léger. **REMARQUE :** Il n'est pas possible de réduire la taille de la partition. La valeur entrée doit être supérieure à la taille actuelle de la partition.
`resize-image --size <taille en Mo>` Par exemple : `resize-image --size 1024`	Avec cette syntaxe, vous pouvez spécifier la taille de la partition cible en mégaoctets (MO) comme paramètre, puis confirmer la modification.

`resize-image --no-prompt`
–ou–
`resize-image --no-prompt --size <taille en Mo>`
Par exemple : `resize-image --no-prompt --size 1024`
	Avec cette syntaxe, le script s'exécute automatiquement sans qu'aucune intervention de l'utilisateur ne soit nécessaire.
	Si aucune taille spécifique n'est donnée simultanément comme paramètre, la taille de la partition est augmentée au maximum.
	CONSEIL : Ce mode sans interaction de l'utilisateur est utile pour scripter et effectuer cette opération à partir d'un outil d'administration à distance tel que HP Device Manager.

D Clés de registre

Les clés de registre HP ThinPro sont regroupées dans des dossiers et peuvent être modifiées de différentes façons :

- Avec une tâche **_File and Registry** dans HPDM.
- Avec le composant Registry Editor de Profile Editor, puis en déployant le nouveau profil.
- À l'aide de Registry Editor (Éditeur du registre) dans l'interface utilisateur HP ThinPro, qui est disponible dans le menu Outils en mode administrateur.

Chaque section de niveau supérieur dans cette annexe correspond à un des dossiers de niveau supérieur du registre.

REMARQUE : Certaines clés de registre peuvent s'appliquer uniquement à ThinPro ou Smart Zero.

Audio

Clé de registre	Description
`root/Audio/AdjustSoundPath`	Définit le chemin d'accès complet du son joué lorsque le volume de lecture est modifié via les commandes de volume.
`root/Audio/JackRetask`	Cette clé de registre ne concerne que les clients légers dotés de prises ré-affectables. Pour le port inférieur avant du t730 : • 0/1 : Sans modification / casque • 2 : Microphone Pour le port arrière du t630 : • 0 : Sans modification / entrée audio • 1 : Casque / sortie audio Vous devez redémarrer le client léger après avoir modifié ces paramètres.
`root/Audio/OutputMute`	Si la valeur est définie sur 1, le son des haut-parleurs internes et de la prise casque est désactivé.
`root/Audio/OutputScale`	Permet de régler l'échelle du volume des haut-parleurs internes et de la prise casque, allant de 1 à 400.
`root/Audio/OutputScaleAuto`	Si définie sur 1, la valeur de `OutputScale` sera définie automatiquement en fonction du modèle de client léger.
`root/Audio/OutputVolume`	Permet de régler le volume des haut-parleurs internes et de la prise casque, allant de 1 à 100.
`root/Audio/PlaybackDevice`	Définit le périphérique à utiliser pour la lecture.
`root/Audio/PulseBuffer`	La plage recommandée pour cette valeur se situe entre 1024 et 8192. Une valeur trop élevée peut provoquer des saccades de lecture, alors qu'une valeur trop faible peut causer le crash du client léger.

Clé de registre	Description
root/Audio/RecordDevice	Définit le périphérique à utiliser pour la capture.
root/Audio/RecordMute	Si la valeur est définie sur 1, le son de la prise microphone est désactivé.
root/Audio/RecordScale	Définit l'échelle du volume de la prise microphone, allant de 1 à 400.
root/Audio/RecordScaleAuto	Si définie sur 1, la valeur de RecordScale sera définie automatiquement en fonction du modèle de client léger.
root/Audio/RecordVolume	Permet de régler le volume de la prise microphone, allant de 1 à 100.
root/Audio/VisibleInSystray	Si la valeur est définie sur 1, une icône de haut-parleur est visible dans la barre d'état système.
root/Audio/shortcutPassThrough	Définit les applications qui permettent de passer les raccourcis audio à l'aide d'une liste séparée par un espace. Les options disponibles sont freerdp, view, et xen.

CertMgr

Cette catégorie d'enregistrement est utilisée en interne et n'a pas d'entrées définies par l'utilisateur.

ComponentMgr

Clé de registre	Description
root/ComponentMgr/NotShowDeleteSnapshotWarning	Si la valeur est définie sur 1, les informations d'avertissement ne figurent pas lors de la suppression d'un instantané.

ConnectionManager

Clé de registre	Description
root/ConnectionManager/createSampleConnections	Si défini sur 1, des icônes de connexion d'exemple modifiable par l'utilisateur sont créées sur le bureau au premier démarrage.
root/ConnectionManager/customLogoPath	
root/ConnectionManager/defaultConnection	La valeur doit indiquer une connexion valide utilisant le format <saisir>:<étiquette> pour qu'une connexion se lance correctement au démarrage. Par exemple, xen:Default Connection
root/ConnectionManager/minHeight	
root/ConnectionManager/minWidth	
root/ConnectionManager/splashLogoPath	Définit le chemin d'accès à l'image qui s'affiche pendant le chargement d'une connexion.

Clé de registre	Description
root/ConnectionManager/useKioskMode	
root/ConnectionManager/useSplashOnConnectionStartup	Si la valeur est définie sur 1, l'image définie par splashLogoPath est activée. Par défaut, elle est activée pour ThinPro et désactivée dans Smart Zero.

ConnectionType

custom

Clé de registre	Description
root/ConnectionType/custom/authorizations/user/add	Si la clé est définie sur 1, un utilisateur final est autorisé à ajouter une nouvelle connexion de ce type à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/custom/authorizations/user/general	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres généraux de ce type de connexion à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/custom/connections/<UUID>/afterStartedCommand	Permet de régler la commande à exécuter après le démarrage de la connexion.
root/ConnectionType/custom/connections/<UUID>/afterStoppedCommand	Permet de régler la commande à exécuter une fois que la connexion a été arrêtée.
root/ConnectionType/custom/connections/<UUID>/authorizations/user/edit	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres de la connexion pour cette connexion.
root/ConnectionType/custom/connections/<UUID>/authorizations/user/execution	Si la clé est définie sur 1, un utilisateur final est autorisé à exécuter cette connexion.
root/ConnectionType/custom/connections/<UUID>/autoReconnect	Si la valeur est définie sur 1, la connexion redémarre lorsqu'elle est fermée ou déconnectée.
root/ConnectionType/custom/connections/<UUID>/autoReconnectDelay	Définit le temps d'attente en secondes avant la reconnexion de la session. La valeur par défaut de 0 entraîne la reconnexion immédiate de la connexion. Ce paramètre ne prend effet que lorsque autoReconnect est définie sur 1.
root/ConnectionType/custom/connections/<UUID>/autostart	Si définie sur une valeur de 1 à 5, la connexion se lancera automatiquement après le démarrage du système, la valeur de 1 ayant la priorité la plus élevée.
root/ConnectionType/custom/connections/<UUID>/beforeStartingCommand	Définit la commande à exécuter avant le démarrage de la connexion.
root/ConnectionType/custom/connections/<UUID>/command	Définit la commande principale pour l'exécution de la connexion Custom.
root/ConnectionType/custom/connections/<UUID>/connectionEndAction	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/custom/connections/<UUID>/coord	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/custom/connections/<UUID>/dependConnectionId	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.

Clé de registre	Description
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/key	Définit le nom d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/custom/connections/<UUID>/extraEnvValues/<UUID>/value	Définit la valeur d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/custom/connections/<UUID>/fallBackConnection	Permet de régler la connexion de secours via son UUID.
root/ConnectionType/custom/connections/<UUID>/hasDesktopIcon	Si la valeur est définie sur 1, l'icône du Bureau pour cette connexion est activée. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/custom/connections/<UUID>/iconPosition	Définit les coordonnées x,y d'une icône de bureau fixée. Si aucune valeur n'est spécifiée, l'icône est flottante.
root/ConnectionType/custom/connections/<UUID>/label	Définit le nom de connexion qui s'affiche dans l'interface utilisateur. Sur Smart Zero, ce paramètre est normalement défini sur `Default Connection` et ne s'affiche pas dans l'interface utilisateur.
root/ConnectionType/custom/connections/<UUID>/startMode	Si la valeur par défaut `focus` est définie et que la connexion a déjà démarré, la connexion est mise en avant. Sinon, une erreur est renvoyée indiquant que la connexion est déjà démarrée.
root/ConnectionType/custom/connections/<UUID>/waitForNetwork	Si la valeur est définie sur 1, la connexion n'est pas lancée tant que le réseau n'est pas disponible. Ce paramètre permet de s'assurer que, sur un réseau lent, la connexion ne se lance pas avant que le réseau soit disponible, ce qui pourrait entraîner un échec.
root/ConnectionType/custom/coreSettings/USBrelevant	Spécifie si ce type de connexion est conforme à l'USB. Si c'est le cas, il peut y avoir une connexion de USB pour rediriger les périphériques USB.
root/ConnectionType/custom/coreSettings/appName	Définit le nom de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/custom/coreSettings/className	Définit la classe de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/custom/coreSettings/editor	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de connexion s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/custom/coreSettings/generalSettingsEditor	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de paramètres généraux s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/custom/coreSettings/icon	Spécifie l'icône à partir du thème d'icône défini à utiliser pour cette connexion.
root/ConnectionType/custom/coreSettings/icon16Path	Définit le chemin d'accès à l'icône 16 x 16 pixels représentant cette application.
root/ConnectionType/custom/coreSettings/icon32Path	Définit le chemin d'accès à l'icône 32 x 32 pixels représentant cette application.
root/ConnectionType/custom/coreSettings/icon48Path	Définit le chemin d'accès à l'icône 48 x 48 pixels représentant cette application.
root/ConnectionType/custom/coreSettings/iconActive	Réservé à une utilisation ultérieure.
root/ConnectionType/custom/coreSettings/label	Définit le nom à afficher pour ce type de connexion dans l'interface utilisateur.

Clé de registre	Description
`root/ConnectionType/custom/coreSettings/priorityInConnectionLists`	Définit la priorité de ce type de connexion lorsqu'elle s'affiche dans le gestionnaire de connexion et dans l'assistant de configuration qui s'affiche pendant l'installation initiale. Une valeur supérieure déplace le type de connexion vers le haut de la liste. Lorsqu'elle est définie sur 0, le type de connexion est masqué à l'assistant de configuration et figure en dernière place dans le gestionnaire de connexion. Les types de connexion de priorité identique sont répertoriés dans l'ordre alphabétique.
`root/ConnectionType/custom/coreSettings/serverRequired`	Définit si un nom ou une adresse de serveur est `unused`, `optional` ou `required` pour ce type de connexion.
`root/ConnectionType/custom/coreSettings/stopProcess`	Définit le comportement attendu lorsque la commande `connexion-mgr stop` est appelée sur cette connexion. Par défaut, il s'agit de `close`, qui provoque l'envoi d'un signal « kill » standard au processus. Si la valeur est définie sur `kill`, le processus spécifié par `appName` est tué de force. Si la valeur est définie sur `custom`, un script d'exécution personnalisé spécifié par `wrapperScript` sera exécuté avec l'argument `stop` pour mettre fin au processus normalement.
`root/ConnectionType/custom/coreSettings/tier`	Indique l'importance relative de ce type de connexion et l'ordre dans lequel elle est répertoriée dans le menu Créer.
`root/ConnectionType/custom/coreSettings/watchPid`	Si la valeur est définie sur 1, la connexion est contrôlée sous le nom spécifié par `appName`. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/custom/coreSettings/wrapperScript`	Définit le nom du script ou du fichier binaire à exécuter au lancement de ce type de connexion. Il s'agit du script principal gérant tous les paramètres de connexion et les arguments de ligne de commande de la connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/custom/gui/CustomManager/name`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/custom/gui/CustomManager/status`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/custom/gui/CustomManager/title`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/custom/gui/CustomManager/widgets/autoReconnect`	Contrôle l'état du widget **Reconnexion automatique** dans le gestionnaire de connexion Personnalisée. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/custom/gui/CustomManager/widgets/autostart`	Contrôle l'état du widget **Priorité du démarrage automatique** dans le gestionnaire de connexion Custom. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/custom/gui/CustomManager/widgets/command`	Contrôle l'état du widget **Entrer une commande pour exécuter** dans le gestionnaire de connexion Custom. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.

Clé de registre	Description
`root/ConnectionType/custom/gui/CustomManager/widgets/fallBackConnection`	Contrôle l'état du widget **Connexion de repli** dans le gestionnaire de connexion Custom. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/custom/gui/CustomManager/widgets/hasDesktopIcon`	Contrôle l'état du widget **Afficher l'icône sur le Bureau** dans le gestionnaire de connexion Custom. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/custom/gui/CustomManager/widgets/label`	Contrôle l'état du widget **Nom** dans le gestionnaire de connexion Custom. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/custom/gui/CustomManager/widgets/waitForNetwork`	Contrôle l'état du widget **Attente du réseau avant connexion** dans le gestionnaire de connexion Custom. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.

firefox

Clé de registre	Description
`root/ConnectionType/firefox/authorizations/user/add`	Si la clé est définie sur 1, un utilisateur final est autorisé à ajouter une nouvelle connexion de ce type à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
`root/ConnectionType/firefox/connections/<UUID>/address`	Définit l'adresse URL ou IP à laquelle se connecter.
`root/ConnectionType/firefox/connections/<UUID>/afterStartedCommand`	Permet de régler la commande à exécuter après le démarrage de la connexion.
`root/ConnectionType/firefox/connections/<UUID>/afterStoppedCommand`	Permet de régler la commande à exécuter une fois que la connexion a été arrêtée.
`root/ConnectionType/firefox/connections/<UUID>/authorizations/user/edit`	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres de la connexion pour cette connexion.
`root/ConnectionType/firefox/connections/<UUID>/authorizations/user/execution`	Si la clé est définie sur 1, un utilisateur final est autorisé à exécuter cette connexion.
`root/ConnectionType/firefox/connections/<UUID>/autoReconnect`	Si la valeur est définie sur 1, la connexion redémarre lorsqu'elle est fermée ou déconnectée.
`root/ConnectionType/firefox/connections/<UUID>/autoReconnectDelay`	Définit le temps d'attente en secondes avant la reconnexion de la session. La valeur par défaut de 0 entraîne la reconnexion immédiate de la connexion. Ce paramètre ne prend effet que lorsque `autoReconnect` est définie sur 1.
`root/ConnectionType/firefox/connections/<UUID>/autostart`	Si définie sur une valeur de 1 à 5, la connexion se lancera automatiquement après le démarrage du système, la valeur de 1 ayant la priorité la plus élevée.

Clé de registre	Description
root/ConnectionType/firefox/connections/<UUID>/autostartDelay	Réservé à une utilisation ultérieure.
root/ConnectionType/firefox/connections/<UUID>/beforeStartingCommand	Définit la commande à exécuter avant le démarrage de la connexion.
root/ConnectionType/firefox/connections/<UUID>/connectionEndAction	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/firefox/connections/<UUID>/coord	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/firefox/connections/<UUID>/dependConnectionId	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/firefox/connections/<UUID>/enablePrintDialog	Si la valeur est définie sur 1, la boîte de dialogue d'impression du navigateur Web peut être utilisée.
root/ConnectionType/firefox/connections/<UUID>/enableSmartCard	Si la clé est définie sur 1, la connexion de Smart Card est autorisée pour les connexions Citrix créées via le navigateur Internet.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/key	Définit le nom d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/firefox/connections/<UUID>/extraEnvValues/<UUID>/value	Définit la valeur d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/firefox/connections/<UUID>/fallBackConnection	Permet de régler la connexion de secours via son UUID.
root/ConnectionType/firefox/connections/<UUID>/forbiddenFiles	Cette clé de registre ne fonctionne que lorsque la fonction **Permettre aux connexions de gérer leurs propres paramètres** est sélectionnée dans le gestionnaire de paramètres généraux de connexion du navigateur web. Les fichiers répertoriés dans la valeur de cette clé de registre sont supprimées à la fin d'une connexion de navigateur web. Les noms de fichier doivent être séparés par une virgule et un caractère générique est pris en charge. Par exemple : `*.rdf,cookies.sqlite`
root/ConnectionType/firefox/connections/<UUID>/fullscreen	Si la valeur est définie sur 1, le navigateur Web démarrera en plein écran. Si `kioskMode` est désactivé, l'interface utilisateur du navigateur est accessible en mode plein écran.
root/ConnectionType/firefox/connections/<UUID>/hasDesktopIcon	Si la valeur est définie sur 1, l'icône du Bureau pour cette connexion est activée. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/firefox/connections/<UUID>/iconPosition	Définit les coordonnées x,y d'une icône de bureau fixée. Si aucune valeur n'est spécifiée, l'icône est flottante.
root/ConnectionType/firefox/connections/<UUID>/intendedUse	Définit l'utilisation prévue de cette connexion Web Browser à `Citrix`, `RDP`ou à `Internet`.
root/ConnectionType/firefox/connections/<UUID>/kioskMode	Si la valeur est définie sur 1, le Web Browser se lance en Mode kiosque, ce qui signifie que le Web Browser démarrera en plein écran (même si `fullscreen` est sur 0) et que l'interface utilisateur du navigateur est inaccessible.
root/ConnectionType/firefox/connections/<UUID>/label	Définit le nom de connexion qui s'affiche dans l'interface utilisateur. Sur Smart Zero, ce paramètre est normalement défini sur `Default Connection` et ne s'affiche pas dans l'interface utilisateur.
root/ConnectionType/firefox/connections/<UUID>/manageOwnPrefs	Si elle est définie sur 1, la connexion gère ses propres préférences et les stocke dans l'emplacement suivant : `/etc/firefox/`

Clé de registre	Description
	<UUID>. Si elle est définie sur 0, la connexion utilise les préférences partagées.
root/ConnectionType/firefox/connections/<UUID>/showBackForwardButton	Si définie sur 1, les boutons Back (Retour) et Forward (Suivant) du navigateur Internet sont affichés lorsque le mode kiosque est activé.
root/ConnectionType/firefox/connections/<UUID>/showHomeButton	Si la clé est définie sur 1, le bouton d'accueil du navigateur Internet est affiché lorsque le mode kiosque est activé.
root/ConnectionType/firefox/connections/<UUID>/showSearchBar	Si la clé est définie sur 1, la barre de recherche du navigateur Internet est affichée lorsque le mode kiosque est activé.
root/ConnectionType/firefox/connections/<UUID>/showTabsBar	Si la clé est définie sur 1, les onglets du navigateur Internet sont affichés lorsque le mode kiosque est activé.
root/ConnectionType/firefox/connections/<UUID>/showTaskBar	Si la clé est définie sur 1, la barre des tâches du navigateur Internet est affichée lorsque le mode kiosque est activé.
root/ConnectionType/firefox/connections/<UUID>/showUrlBarRefreshButton	Si la clé est définie sur 1, la barre de saisie d'URL et le bouton Refresh (Rafraîchir) sont affichés lorsque le mode kiosque est activé.
root/ConnectionType/firefox/connections/<UUID>/startMode	Si la valeur par défaut focus est définie et que la connexion a déjà démarré, la connexion est mise en avant. Sinon, une erreur est renvoyée indiquant que la connexion est déjà démarrée.
root/ConnectionType/firefox/connections/<UUID>/waitForNetwork	Si la valeur est définie sur 1, la connexion n'est pas lancée tant que le réseau n'est pas disponible. Ce paramètre permet de s'assurer que, sur un réseau lent, la connexion ne se lance pas avant que le réseau soit disponible, ce qui pourrait entraîner un échec.
root/ConnectionType/firefox/coreSettings/USBrelevant	Spécifie si ce type de connexion est conforme à l'USB. Si c'est le cas, il peut y avoir une connexion de USB pour rediriger les périphériques USB.
root/ConnectionType/firefox/coreSettings/appName	Définit le nom de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/firefox/coreSettings/className	Définit la classe de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/firefox/coreSettings/editor	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de connexion s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/firefox/coreSettings/icon	Spécifie l'icône à partir du thème d'icône défini à utiliser pour cette connexion.
root/ConnectionType/firefox/coreSettings/icon16Path	Définit le chemin d'accès à l'icône 16 x 16 pixels représentant cette application.
root/ConnectionType/firefox/coreSettings/icon32Path	Définit le chemin d'accès à l'icône 32 x 32 pixels représentant cette application.
root/ConnectionType/firefox/coreSettings/icon48Path	Définit le chemin d'accès à l'icône 48 x 48 pixels représentant cette application.
root/ConnectionType/firefox/coreSettings/iconActive	Réservé à une utilisation ultérieure.
root/ConnectionType/firefox/coreSettings/label	Définit le nom à afficher pour ce type de connexion dans l'interface utilisateur.

Clé de registre	Description
`root/ConnectionType/firefox/coreSettings/priorityInConnectionLists`	Définit la priorité de ce type de connexion lorsqu'elle s'affiche dans le gestionnaire de connexion et dans l'assistant de configuration qui s'affiche pendant l'installation initiale. Une valeur supérieure déplacera ce type de connexion vers le haut de la liste. Si la clé est définie sur 0, ce type de connexion est masqué pour l'assistant de configuration et figure en dernière place dans le gestionnaire de connexion. Les types de connexions avec la même priorité sont répertoriés dans l'ordre alphabétique.
`root/ConnectionType/firefox/coreSettings/restartIdleTime`	Définit la durée en minutes avant que le navigateur Web ne redémarre lorsque le système ne reçoit pas de saisie de l'utilisateur. Si la valeur est définie sur 0, le redémarrage est désactivé.
`root/ConnectionType/firefox/coreSettings/serverRequired`	Définit si un nom ou une adresse de serveur est `unused`, `optional` ou `required` pour ce type de connexion.
`root/ConnectionType/firefox/coreSettings/stopProcess`	Définit le comportement attendu lorsque la commande `connexion-mgr stop` est appelée sur cette connexion. Par défaut, il s'agit de `close`, qui provoque l'envoi d'un signal « kill » standard au processus. Si la valeur est définie sur `kill`, le processus spécifié par `appName` est tué de force. Si la valeur est définie sur `custom`, un script d'exécution personnalisé spécifié par `wrapperScript` sera exécuté avec l'argument `stop` pour mettre fin au processus normalement.
`root/ConnectionType/firefox/coreSettings/tier`	Indique l'importance relative de ce type de connexion et l'ordre dans lequel elle est répertoriée dans le menu Créer.
`root/ConnectionType/firefox/coreSettings/wrapperScript`	Définit le nom du script ou du fichier binaire à exécuter au lancement de ce type de connexion. C'est le script principal gérant tous les paramètres de connexion et arguments de ligne de commande pour la connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/firefox/general/enableUserChanges`	Si la valeur est définie sur 1, les paramètres configurés dans la boîte de dialogue Préférences de Firefox sont enregistrés après chaque session.
`root/ConnectionType/firefox/gui/FirefoxManager/name`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/firefox/gui/FirefoxManager/status`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/firefox/gui/FirefoxManager/title`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/address`	Contrôle l'état du widget **URL** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/autoReconnect`	Contrôle l'état du widget **Reconnexion automatique** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/autostart`	Contrôle l'état du widget **Priorité du démarrage automatique** dans le gestionnaire de connexion Web Browser. Si la clé est

Clé de registre	Description
	définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/enablePrintDialog`	Contrôle l'état du widget **Activer la boîte de dialogue d'impression** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/fallBackConnection`	Contrôle l'état du widget **Connexion de repli** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/hasDesktopIcon`	Contrôle l'état du widget **Afficher l'icône sur le Bureau** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/kioskMode`	Contrôle l'état du widget **Activer le mode kiosque** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/label`	Contrôle l'état du widget **Nom** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/showBackForwardButton`	Contrôle l'état du widget **Afficher les boutons Retour et Suivant** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/showHomeButton`	Contrôle l'état du widget **Afficher le bouton d'accueil** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/showSearchBar`	Contrôle l'état du widget **Afficher la barre de recherche** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/firefox/gui/FirefoxManager/widgets/showTabsBar`	Contrôle l'état du widget **Afficher la barre d'onglets** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur

Clé de registre	Description
	active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/showTaskBar	Contrôle l'état du widget **Afficher la barre d'état** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/showUrlBarRefreshButton	Contrôle l'état du widget **Afficher la barre de saisie d'URL et le bouton Rafraîchir** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/startMode	Contrôle l'état du widget **Activer le plein écran** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.
root/ConnectionType/firefox/gui/FirefoxManager/widgets/waitForNetwork	Contrôle l'état du widget **Attendre le réseau avant connexion** dans le gestionnaire de connexion Web Browser. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.

freerdp

Clé de registre	Description
root/ConnectionType/freerdp/authorizations/user/add	Si la clé est définie sur 1, un utilisateur final est autorisé à ajouter une nouvelle connexion de ce type à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/ExtraArgs	Spécifie des arguments supplémentaires pour le client xfreerdp. Exécutez xfreerdp —help à partir d'un terminal X pour afficher tous les arguments disponibles.
root/ConnectionType/freerdp/connections/<UUID>/SingleSignOn	Si cette option est activée, l'utilisateur, le domaine et la combinaison de mot de passe pour la connexion RDP sont sauvegardés pour déverrouiller l'économiseur d'écran.
root/ConnectionType/freerdp/connections/<UUID>/address	Définit le nom d'hôte ou l'adresse IP auquel se connecter. Le numéro de port peut être ajouté à la fin après deux points. Par exemple : ServerName:3389
root/ConnectionType/freerdp/connections/<UUID>/afterStoppedCommand	Permet de régler la commande à exécuter une fois que la connexion a été arrêtée.
root/ConnectionType/freerdp/connections/<UUID>/application	Spécifie un autre shell ou une autre application à exécuter.

Clé de registre	Description
root/ConnectionType/freerdp/connections/<UUID>/attachToConsole	
root/ConnectionType/freerdp/connections/<UUID>/audioLatency	Définit la durée moyenne en millisecondes du décalage entre le flux audio et l'affichage des images vidéo correspondantes après décodage.
root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/edit	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres de la connexion pour cette connexion.
root/ConnectionType/freerdp/connections/<UUID>/authorizations/user/execution	Si la clé est définie sur 1, un utilisateur final est autorisé à exécuter cette connexion.
root/ConnectionType/freerdp/connections/<UUID>/autoReconnect	Si la valeur est définie sur 1, la connexion redémarre lorsqu'elle est fermée ou déconnectée.
root/ConnectionType/freerdp/connections/<UUID>/autoReconnectDelay	Définit le temps d'attente en secondes avant la reconnexion de la session. La valeur par défaut de 0 entraîne la reconnexion immédiate de la connexion. Ce paramètre ne prend effet que lorsque autoReconnect est définie sur 1.
root/ConnectionType/freerdp/connections/<UUID>/autostart	Si définie sur une valeur de 1 à 5, la connexion se lancera automatiquement après le démarrage du système, la valeur de 1 ayant la priorité la plus élevée.
root/ConnectionType/freerdp/connections/<UUID>/bandwidthLimitation	Si la clé est définie sur une valeur supérieure à 0, la valeur représente une limitation approximative de la bande passante pour le téléchargement depuis et vers le serveur en kilo-octets par seconde. Si cette clé est définie sur 0 valeur par défaut), aucune limitation ne s'applique.
root/ConnectionType/freerdp/connections/<UUID>/beforeStartingCommand	Définit la commande à exécuter avant le démarrage de la connexion.
root/ConnectionType/freerdp/connections/<UUID>/clipboardExtension	Si la valeur est définie sur 1, la fonctionnalité de presse-papiers est activée entre différentes sessions RDP et entre les sessions RDP et le système local.
root/ConnectionType/freerdp/connections/<UUID>/compression	Si la valeur est définie sur 1, la compression des données RDP entre le client et le serveur est activée.
root/ConnectionType/freerdp/connections/<UUID>/credentialsType	Spécifie le type d'informations d'authentification parmi sso (authentification unique), startup (les informations d'authentification sont demandées au démarrage), password (mot de passe utilisateur/domaine préconfiguré), ou smartcard (carte à puce préconfigurée).
root/ConnectionType/freerdp/connections/<UUID>/dependConnectionId	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/freerdp/connections/<UUID>/directory	Spécifie le répertoire de démarrage où une autre application shell est exécutée.
root/ConnectionType/freerdp/connections/<UUID>/disableMMRwithRFX	Si la valeur est définie sur 1, la redirection multimédia est désactivée si une session RemoteFX valide est établie.
root/ConnectionType/freerdp/connections/<UUID>/domain	Définit le nom de domaine par défaut à fournir à l'hôte distant lors de l'ouverture de session. Si aucun domaine n'est spécifié, le domaine par défaut de l'hôte distant est utilisé.
root/ConnectionType/freerdp/connections/<UUID>/enableMMR	Si la valeur est définie sur 1, l'extension Redirection multimédia est activée, ce qui entraîne la redirection vers le client des codecs compatibles lus dans Windows Media Player.

Clé de registre	Description
root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/key	Définit le nom d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/freerdp/connections/<UUID>/extraEnvValues/<UUID>/value	Définit la valeur d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/freerdp/connections/<UUID>/fallBackConnection	Permet de régler la connexion de secours via son UUID.
root/ConnectionType/freerdp/connections/<UUID>/frameAcknowledgeCount	Définit le nombre d'images vidéo que le serveur peut envoyer sans attendre d'accusé de réception de la part du client. Des valeurs plus faibles donnent lieu à un bureau plus réactif, mais réduisent le nombre d'images par seconde. Si la valeur est définie sur 0, les interactions client-serveur portant sur les images se font sans accusé de réception.
root/ConnectionType/freerdp/connections/<UUID>/gatewayAddress	Définit le nom de serveur ou l'adresse de la passerelle RD.
root/ConnectionType/freerdp/connections/<UUID>/gatewayCredentialsType	Spécifie le type d'informations d'authentification en déterminant si elles doivent être fournies par `sso` (authentification unique), `startup` (les informations d'authentification sont demandées au démarrage), ou `password` (mot de passe utilisateur/domaine préconfiguré).
root/ConnectionType/freerdp/connections/<UUID>/gatewayDomain	Définit le nom de domaine par défaut à fournir à la passerelle RD lors de l'ouverture de session. En général, ce paramètre est utilisé avec les applications de style kiosque dans lesquelles un nom d'utilisateur générique est utilisé pour l'ouverture de session. Si `gatewayUsesSameCredentials` est défini sur 1, cette valeur est désactivée.
root/ConnectionType/freerdp/connections/<UUID>/gatewayEnabled	Si la valeur est définie sur 1, l'utilisation de la passerelle RD est prévue.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPassword	Définit le mot de passe par défaut à fournir à la passerelle RD lors de l'ouverture de session. Cette valeur est généralement cryptée. En général, ce paramètre est utilisé avec les applications de style kiosque dans lesquelles un nom d'utilisateur générique est utilisé pour l'ouverture de session. Si `gatewayUsesSameCredentials` est défini sur 1, cette valeur est désactivée.
root/ConnectionType/freerdp/connections/<UUID>/gatewayPort	Définit le numéro de port à utiliser pour contacter le serveur RDP. Cette valeur peut être laissée vide. La valeur la plus courante est 443.
root/ConnectionType/freerdp/connections/<UUID>/gatewayUser	Définit le nom d'utilisateur par défaut à fournir à la passerelle RD lors de l'ouverture de session. En général, ce paramètre est utilisé avec les applications de style kiosque dans lesquelles un nom d'utilisateur générique est utilisé pour l'ouverture de session. Si `gatewayUsesSameCredentials` est défini sur 1, cette valeur est désactivée.
root/ConnectionType/freerdp/connections/<UUID>/gatewayUsesSameCredentials	Si la valeur est définie sur 1, les informations d'authentification utilisées pour la connexion à la passerelle RD sont les mêmes que celles utilisées pour la connexion au serveur final.
root/ConnectionType/freerdp/connections/<UUID>/hasDesktopIcon	Si la valeur est définie sur 1, l'icône du Bureau pour cette connexion est activée. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/freerdp/connections/<UUID>/hostnameType	Si la valeur hostname est définie, le nom d'hôte du système est envoyé à l'hôte distant. Ce paramétrage est généralement utilisé pour identifier le client léger, associé à une session RDP donnée.

Clé de registre	Description
	Le nom d'hôte envoyé peut être remplacé à l'aide de `sendHostname` dans les paramètres spécifiques à la connexion. Si la valeur est définie sur mac, l'adresse MAC du premier adaptateur réseau disponible est envoyée à la place du nom d'hôte.
`root/ConnectionType/freerdp/connections/<UUID>/iconPosition`	Définit les coordonnées x,y d'une icône de bureau fixée. Si aucune valeur n'est spécifiée, l'icône est flottante.
`root/ConnectionType/freerdp/connections/<UUID>/label`	Définit le nom de connexion qui s'affiche dans l'interface utilisateur. Sur Smart Zero, ce paramètre est normalement défini sur `Default Connection` et ne s'affiche pas dans l'interface utilisateur.
`root/ConnectionType/freerdp/connections/<UUID>/loadBalanceInfo`	Cette valeur est le cookie d'équilibrage de charge envoyé à des fins de brokering au serveur lors de la connexion et correspond au champ `loadbalanceinfo` du fichier .rdp. Par défaut, la valeur est vide.
`root/ConnectionType/freerdp/connections/<UUID>/localPartitionRedirection`	Si la valeur est définie sur 1, les partitions de stockage non-USB locales sont redirigées vers l'hôte distant via l'extension `Storage`. Si définie sur 0, l'extension est désactivée pour les partitions de stockage non-USB qui ne sont pas utilisées par HP ThinPro.
`root/ConnectionType/freerdp/connections/<UUID>/loginfields/domain`	Si la valeur est définie sur 1, le champ **Domaine** est affiché dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, le champ est affiché puis désactivé. Si la valeur est définie sur 0, le champ est masqué.
`root/ConnectionType/freerdp/connections/<UUID>/loginfields/password`	Si la valeur est définie sur 1, le champ **Mot de passe** est affiché dans la boîte de dialogue ouverture de session pour la connexion. Si la valeur est définie sur 2, le champ est affiché puis désactivé. Si la valeur est définie sur 0, le champ est masqué.
`root/ConnectionType/freerdp/connections/<UUID>/loginfields/rememberme`	Lorsqu'elle est définie sur 1, la case **Se souvenir de moi** figure dans la boîte de dialogue d'ouverture de session pour la connexion. Lorsqu'elle est définie sur 2, la case est affichée mais désactivée. Lorsqu'elle est définie sur 0, la case est masquée.
`root/ConnectionType/freerdp/connections/<UUID>/loginfields/server`	Si elle est définie sur 1, la case **Serveur** est affichée dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, la case est affichée puis désactivée. Si la valeur est réglée sur 0, la case est masquée. Si la valeur est définie sur 3, les paramètres du système sont utilisés.
`root/ConnectionType/freerdp/connections/<UUID>/loginfields/showpassword`	Lorsqu'elle est définie sur 1, la case à cocher **Afficher le mot de passe** figure dans la boîte de dialogue d'ouverture de session pour la connexion. Lorsqu'elle est définie sur 2, la case est affichée mais désactivée. Lorsqu'elle est définie sur 0, la case est masquée.
`root/ConnectionType/freerdp/connections/<UUID>/loginfields/smartcard`	Lorsqu'elle est définie sur 1, la case **Connexion carte à puce** figure dans la boîte de dialogue d'ouverture de session pour la connexion. Lorsqu'elle est définie sur 2, la case est affichée mais désactivée. Lorsqu'elle est définie sur 0, la case est masquée. Cette case peut ne pas figurer si aucune carte à puce n'est détectée, même si cette option est activée.
`root/ConnectionType/freerdp/connections/<UUID>/loginfields/username`	Si la valeur est définie sur 1, le champ **Nom d'utilisateur** apparaît dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, le champ est affiché puis désactivé. Si la valeur est définie sur 0, le champ est masqué.

Clé de registre	Description
root/ConnectionType/freerdp/connections/<UUID>/mouseMotionEvents	Si la valeur est définie sur 0, les évènements de déplacement de la souris ne sont pas envoyés au serveur. Ce paramétrage peut empêcher certaines interactions de l'utilisateur, comme les info-bulles, de fonctionner correctement.
root/ConnectionType/freerdp/connections/<UUID>/offScreenBitmaps	Si la valeur est définie sur 0, les images bitmaps hors écran sont désactivées. Cela peut augmenter légèrement les performances, mais provoquera une mise à jour asynchrone de certains blocs de l'écran, ce qui entraine des actualisations d'écran non-uniformes.
root/ConnectionType/freerdp/connections/<UUID>/password	Définit le mot de passe par défaut à fournir à l'hôte distant lors de l'ouverture de session. Cette valeur est cryptée. En général, ce paramètre est utilisé avec les applications de style kiosque dans lesquelles un mot de passe générique est utilisé pour l'ouverture de session.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagDesktopComposition	Si la valeur est définie sur 1, cette clé permet la composition du bureau, par exemple des bordures translucides, lorsque cette fonction est prise en charge par le serveur. La désactivation de ce paramètre peut améliorer les performances sur les connexions à faible bande passante. En général, ce paramètre affecte uniquement RemoteFX. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagFontSmoothing	Si la valeur est définie sur 1, cette clé permet le lissage de police lorsque cette fonction est prise en charge par le serveur et activée. La désactivation de ce paramètre peut améliorer les performances sur les connexions à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorSettings	Si la valeur est définie sur 1, le clignotement de curseur est désactivé, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoCursorShadow	Si la valeur est définie sur 1, les ombres de curseur sont désactivées, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoMenuAnimations	Si la valeur est définie sur 1, les animations de menu sont désactivées, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoTheming	Si la valeur est définie sur 1, les thèmes d'interface utilisateur sont désactivés, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWallpaper	Si la valeur est définie sur 1, le papier peint du bureau est désactivé, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
root/ConnectionType/freerdp/connections/<UUID>/perfFlagNoWindowDrag	Si la valeur est définie sur 1, le glissement de fenêtre intégral est désactivé, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Le contour de la fenêtre est utilisé à la place. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.

Clé de registre	Description
root/ConnectionType/freerdp/connections/<UUID>/portMapping	Si la valeur est définie sur 1, tous les ports séries et parallèles sont redirigés vers l'hôte distant via l'extension Ports. Si la valeur est définie sur 0, l'extension est désactivée.
root/ConnectionType/freerdp/connections/<UUID>/printerMapping	Si la clé est définie sur 1, toutes les imprimantes définies localement via CUPS sont redirigées vers l'hôte distant via l'extension Printers (Imprimantes). Si la clé est définie sur 0, l'extension est désactivée. Si la clé est définie sur 2, les imprimantes USB sont redirigées selon la configuration définie dans le gestionnaire USB.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/autoDisconnectTimeout	Définit le nombre de minutes pendant lesquelles il peut n'y avoir aucune ressource RemoteApp et Desktop exécutée avant la coupure automatique de la connexion. Le décompte du temps est affiché au cours des 20 dernières secondes si l'utilisateur a la possibilité de désarmer la minuterie. Si la clé est définie sur 0, la minuterie est désactivée.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/autoStartSingleResource	Si la valeur est définie sur 1, et si le serveur ne renvoie qu'une seule ressource publiée (programme RemoteApp ou bureau virtuel), cette ressource est lancée automatiquement.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/filter/<UUID>/alias	Spécifie l'alias de ressource pour le filtre de ressource. Des RemoteApp et Ressources Bureau avec un alias de compatibilité seront disponibles pour les utilisateurs.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/filter/<UUID>/name	Spécifie le nom d'une ressource pour le filtre de ressource. Des RemoteApp et Ressources Bureau avec un nom compatible seront disponibles pour les utilisateurs.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/keepResourcesWindowOpened	Si la valeur est définie sur 0, la fenêtre de sélection de ressource est automatiquement fermée après qu'une ressource a démarré. Si la valeur est 1, la fenêtre de sélection de ressources est conservée ouverte après le démarrage de ressources. Cela permet à un utilisateur de démarrer plusieurs ressources avant de fermer la fenêtre de sélection de ressource.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/trustedPublisherSha1Thumbprints	Spécifie une liste d'empreintes numériques SHA1, séparées par des virgules, des éditeurs de ressources certifiées. Notez qu'un certificat qui correspond à l'une de ces empreintes n'est pas vérifié. Importez l'autorité de certification (CA) racine de l'éditeur pour plus de sécurité. Examinez également la clé de registre verifyPublisherSignature et Certificate Manager (Gestionnaire de certificats) dans le Panneau de configuration.
root/ConnectionType/freerdp/connections/<UUID>/rdWebFeed/verifyPublisherSignature	Si la clé est définie sur 1, la signature de l'éditeur est vérifiée lorsqu'elle devient disponible dans les fichiers .rdp publiés. Seules les ressources possédant une signature valide d'un éditeur certifié peuvent être exécutées. Si la clé est définie sur 0, aucune vérification de la signature n'est effectuée. Examinez également la clé de registre trustedPublisherSha1Thumbprints.
root/ConnectionType/freerdp/connections/<UUID>/rdp6Buffering	Si la valeur est définie sur 1, les performances graphiques non-RemoteFX, sont augmentées au coût de mises à jour d'écran moins fréquentes.
root/ConnectionType/freerdp/connections/<UUID>/rdp8Codecs	Si la valeur est définie sur 1, des codecs RDP 8 sont utilisés s'ils sont disponibles. Ce paramètre doit être désactivé uniquement dans le cas d'un défaut spécifique aux codecs RDP 8. La désactivation de ce paramètre peut également désactiver des codecs plus avancés.
root/ConnectionType/freerdp/connections/<UUID>/rdpEncryption	Si la valeur est définie sur 1, un cryptage RDP standard est utilisé pour crypter toutes les données entre le client et le serveur.

Clé de registre	Description
root/ConnectionType/freerdp/connections/<UUID>/rdpH264Codec	Si la valeur est définie sur 1, des codecs RDP 8 H.264 sont utilisés s'ils sont disponibles. Ce paramètre a des erreurs visuelles connues, en particulier dans des configurations à plusieurs écrans et il doit être considéré comme expérimental et non pris en charge. L'activation de ce paramètre informe simplement le serveur que le client léger prend en charge les H.264 pour l'affichage du bureau. Le serveur doit également prendre en charge les H.264, et le serveur prend la décision finale sur les codecs à utiliser. Ce paramètre affecte uniquement les codecs bureau. Il n'affecte pas les codecs de redirection multimédia.
root/ConnectionType/freerdp/connections/<UUID>/rdpProgressiveCodec	Si la valeur est définie sur 1, des codecs progressifs RDP 8 sont utilisés s'ils sont disponibles. Ce paramètre doit être désactivé uniquement dans le cas d'un défaut spécifique aux codecs progressif RDP 8. La désactivation de ce paramètre peut également désactiver des codecs plus avancés.
root/ConnectionType/freerdp/connections/<UUID>/redirectPreference	Pour la redirection, le client RDP se voit proposer plusieurs destinations possibles. Il les essaie toutes, dans l'ordre suivant : FQDN, IP principale, liste d'IP, NetBIOS. Si FQDN n'est pas souhaité, une des autres alternatives peut être tentée en premier en définissant cette clé de registre. Si la méthode spécifiée ne fonctionne pas, le client RDP reprend l'ordre d'origine. Le paramétrage sur `auto` force l'ordre d'origine.
root/ConnectionType/freerdp/connections/<UUID>/remoteApp	Définit le nom d'une application disponible à exécuter en mode RAIL (Remote Application Integrated Locally).
root/ConnectionType/freerdp/connections/<UUID>/remoteDesktopService	Si le paramètre est réglé sur `Remote computer`, une connexion RDP directe à un ordinateur distant est effectuée. Si l'ensemble `RD Web Access`, une connexion à un service d'accès à Internet RD est effectuée tout d'abord pour récupérer un flux de ressources d'applications distantes publiées.
root/ConnectionType/freerdp/connections/<UUID>/remoteFx	Si la valeur est définie sur 1, RemoteFX dans le style de RDP 7.1 est utilisé s'il est disponible. Ce paramètre est obsolète et peut disparaître dans une version ultérieure de HP ThinPro. Ce paramètre doit être désactivé uniquement dans le cas d'un défaut spécifique au protocole RemoteFX. La désactivation de ce paramètre peut également désactiver des codecs plus avancés.
root/ConnectionType/freerdp/connections/<UUID>/requireEncryptionOracleRemediation	Si défini sur 1, le client de bureau distant refuse de se connecter aux serveurs qui n'offrent pas de protection appropriée. Cela fait face à la vulnérabilité de sécurité Microsoft CVE-2018-0886.
root/ConnectionType/freerdp/connections/<UUID>/scCertificate	Lorsqu'une connexion avec carte à puce préconfigurée est sélectionnée, un identificateur correspondant au certificat sur cette carte à puce est produit pour l'utiliser pour l'authentification.
root/ConnectionType/freerdp/connections/<UUID>/scPin	Lorsqu'une connexion avec carte à puce préconfigurée est sélectionnée, le PIN ou le mot de passe de cette carte est fourni.
root/ConnectionType/freerdp/connections/<UUID>/scRedirection	Si défini sur 1, tous les lecteurs de carte à puce locaux sont redirigés vers l'hôte distant, mais ne sont pas utilisés pour l'authentification au niveau du réseau (NLA) de la session RDP. **REMARQUE :** Si `credentialsType` est défini sur `carte à puce` ou `carte à puce` est défini sur `1`, scRedirection est ignoré, selon la version de HP ThinPro. Dans cette configuration, les lecteurs de carte à puce sont toujours redirigés.
root/ConnectionType/freerdp/connections/<UUID>/seamlessWindow	Si la valeur est définie sur 1, les décorations des fenêtres sont désactivées. Ce paramétrage peut être souhaitable dans une

Clé de registre	Description
	configuration à plusieurs moniteurs afin de permettre que la connexion soit définie sur la taille du moniteur principal.
`root/ConnectionType/freerdp/connections/<UUID>/securityLevel`	Définit le niveau de sécurité du certificat. Si la valeur est définie sur 0, toutes les connexions sont autorisées. Lorsqu'elle est définie sur 1, les hôtes enregistrés sont sélectionnés et un message d'avertissement s'affiche si une vérification échoue. Lorsqu'elle est définie sur 2, les hôtes enregistrés ne sont pas sélectionnés et un message d'avertissement s'affiche si une vérification échoue. Si la valeur est définie sur 3, toutes les connexions non sécurisées sont refusées.
`root/ConnectionType/freerdp/connections/<UUID>/sendHostname`	Définit le nom d'hôte du client léger qui est envoyé à l'hôte distant. Si vide, le nom d'hôte du système est envoyé. La clé de registre `root/ConnectionType/freerdp/general/sendHostname` doit être définie sur `hostname` pour que cette clé soit utilisée.
`root/ConnectionType/freerdp/connections/<UUID>/showConnectionGraph`	Cette clé n'a pas de fonction diagnostique. Si la valeur est définie sur 1, au démarrage de la session, un programme séparé se lancera pour réaliser un graphique de l'état de santé de la connexion.
`root/ConnectionType/freerdp/connections/<UUID>/showRDPDashboard`	Si la clé est définie sur 1, lorsque la session démarre, une fenêtre distincte affiche les performances et l'état du protocole RDP.
`root/ConnectionType/freerdp/connections/<UUID>/smartcard`	Si la valeur est définie sur 1, l'authentification de la carte Smart Card à l'hôte distant est autorisée. Actuellement, cela désactivera l'authentification au niveau du réseau (NLA).
`root/ConnectionType/freerdp/connections/<UUID>/sound`	Si la clé est définie sur 1, les périphériques d'enregistrement et de lecture sont redirigés vers l'hôte distant via l'extension `Audio`. Si la clé est définie sur 0, l'extension est désactivée. Si la clé est définie sur 2, les périphériques audio USB sont redirigés selon la configuration définie dans le gestionnaire USB. En général, HP recommande de paramétrer cette valeur sur 1 afin d'utiliser une redirection audio de haut niveau. Ce paramétrage permet d'améliorer la qualité audio et de veiller à ce que le son du client redirigé par d'autres extensions (par exemple, la `Multimedia Redirection`) corresponde aux paramètres audio locaux.
`root/ConnectionType/freerdp/connections/<UUID>/startMode`	Si la valeur par défaut `focus` est définie et que la connexion a déjà démarré, la connexion est mise en avant. Sinon, une erreur est renvoyée indiquant que la connexion est déjà démarrée.
`root/ConnectionType/freerdp/connections/<UUID>/timeoutError`	Définit le nombre de millisecondes à attendre après une perte de connexion avant que toute tentative de reconnexion avec le serveur soit abandonnée. Si la valeur est définie sur 0, le nombre de tentatives de reconnexion est illimité.
`root/ConnectionType/freerdp/connections/<UUID>/timeoutRecovery`	Définit le nombre de millisecondes à attendre après une perte de connexion pour que le réseau soit restauré sans effectuer de tentative de reconnexion forcée.
`root/ConnectionType/freerdp/connections/<UUID>/timeoutWarning`	Le nombre de millisecondes à attendre après une perte de connexion avant d'avertir l'utilisateur que la connexion a été perdue.
`root/ConnectionType/freerdp/connections/<UUID>/timeoutWarningDialog`	Si la valeur est définie sur 1, lorsqu'une baisse de connexion de bout en bout est détectée, une boîte de dialogue s'affiche et l'écran passe en mode nuances de gris. Dans le cas contraire, des messages sont écrits dans le journal des connexions et la session se fige.

Clé de registre	Description
root/ConnectionType/freerdp/connections/<UUID>/timeoutsEnabled	Si la valeur est définie sur 1, des vérifications sont effectuées au niveau de la connexion de bout en bout.
root/ConnectionType/freerdp/connections/<UUID>/tlsVersion	Définit la version TLS (Transport Layer Security) à utiliser au cours des étapes initiales de négociation avec le serveur RDP. Définissez cette option sur la version TLS utilisée par votre serveur RDP ou essayez de la régler sur auto. **REMARQUE :** Il existe certains défauts côté serveur sur des serveurs RDP auxquels les correctifs n'ont pas été appliqués, susceptibles de provoquer l'échec de la valeur auto, c'est pourquoi il ne s'agit pas de la valeur par défaut.
root/ConnectionType/freerdp/connections/<UUID>/usbMiscRedirection	Si la clé est définie sur 0, la redirection est désactivée pour tous les périphériques USB autres que ceux gérés par sound, printerMapping, portMapping, usbStorageRedirection et localPartitionRedirection. Si la clé est définie sur 2, tous les autres périphériques USB sont redirigés vers l'hôte distant selon la configuration définie dans le gestionnaire USB.
root/ConnectionType/freerdp/connections/<UUID>/usbStorageRedirection	Si la clé est définie sur 1, les périphériques de stockage USB sont redirigés vers l'hôte distant via l'extension Storage. Si la clé est définie sur 0, l'extension est désactivée. Si la clé est définie sur 2, les périphériques de stockage USB sont redirigés selon ce qui est défini dans le gestionnaire USB.
root/ConnectionType/freerdp/connections/<UUID>/username	Définit le nom d'utilisateur par défaut à fournir à l'hôte distant lors de l'ouverture de session. En général, ce paramètre est utilisé avec les applications de style kiosque dans lesquelles un nom d'utilisateur générique est utilisé pour l'ouverture de session.
root/ConnectionType/freerdp/connections/<UUID>/waitForNetwork	Si la valeur est définie sur 1, la connexion n'est pas lancée tant que le réseau n'est pas disponible. Ce paramètre permet de s'assurer que, sur un réseau lent, la connexion ne se lance pas avant que le réseau soit disponible, ce qui pourrait entraîner un échec.
root/ConnectionType/freerdp/connections/<UUID>/windowMode	Si définie sur Remote Application, le RDP est exécuté en mode RAIL (Remote Application Integrated Locally). Ceci nécessite que le serveur d'application à distance permette à une application souhaitée de s'exécuter en tant qu'application distante. L'application sera affichée dans une fenêtre séparée dans l'environnement de bureau, donnant l'impression que l'application fait partie du système local. Reportez-vous également à la clé de registre remoteApp. Si définie sur Alternate Shell, un shell non standard est invoqué. Reportez-vous également aux clés de registre application et directory.
root/ConnectionType/freerdp/connections/<UUID>/windowSizeHeight	
root/ConnectionType/freerdp/connections/<UUID>/windowSizePercentage	
root/ConnectionType/freerdp/connections/<UUID>/windowSizeWidth	
root/ConnectionType/freerdp/connections/<UUID>/windowType	
root/ConnectionType/freerdp/connections/<UUID>/x11Capture	Cette clé n'a pas de fonction diagnostique. Si la clé est définie sur 1, les opérations X11 sont capturées pour une lecture ultérieure.

Clé de registre	Description
root/ConnectionType/freerdp/connections/<UUID>/x11CaptureDir	Cette clé n'a pas de fonction diagnostique. La valeur définit le répertoire pour les fichiers de capture X11.
root/ConnectionType/freerdp/connections/<UUID>/x11LogAutoflush	Cette clé n'a pas de fonction diagnostique. Si elle est définie sur 1, le fichier journal X11 est plus souvent mis à jour sur le disque.
root/ConnectionType/freerdp/connections/<UUID>/x11Logfile	Cette clé n'a pas de fonction diagnostique. La valeur définit le chemin d'accès au fichier journal X11.
root/ConnectionType/freerdp/connections/<UUID>/x11Logging	Cette clé n'a pas de fonction diagnostique. Si la clé est définie sur 1, les opérations X11 sont consignées.
root/ConnectionType/freerdp/connections/<UUID>/x11Synchronous	Cette clé n'a pas de fonction diagnostique. Si la clé est définie sur sur 1, les opérations X11 ne sont pas mises en cache.
root/ConnectionType/freerdp/connections/<UUID>/xkbLayoutId	Définit un identifiant de disposition XKB pour contourner le clavier du système. Pour accéder à la liste des identifiants disponibles, saisissez la commande suivante dans un terminal X : `xfreerdp --kbd-list`.
root/ConnectionType/freerdp/coreSettings/USBrelevant	Spécifie si ce type de connexion est conforme à l'USB. Si c'est le cas, il peut y avoir une connexion de USB pour rediriger les périphériques USB.
root/ConnectionType/freerdp/coreSettings/appName	Définit le nom de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/freerdp/coreSettings/className	Définit la classe de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/freerdp/coreSettings/disableLinkDropWarning	Si la valeur est définie sur 1, le système d'exploitation ne génère pas de boîte de dialogue indiquant que le réseau est hors tension, car le protocole de connexion sait gérer de telles situations.
root/ConnectionType/freerdp/coreSettings/editor	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de connexion s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/freerdp/coreSettings/icon	Spécifie l'icône à partir du thème d'icône défini à utiliser pour cette connexion.
root/ConnectionType/freerdp/coreSettings/icon16Path	Définit le chemin d'accès à l'icône 16 x 16 pixels représentant cette application.
root/ConnectionType/freerdp/coreSettings/icon32Path	Définit le chemin d'accès à l'icône 32 x 32 pixels représentant cette application.
root/ConnectionType/freerdp/coreSettings/icon48Path	Définit le chemin d'accès à l'icône 48 x 48 pixels représentant cette application.
root/ConnectionType/freerdp/coreSettings/iconActive	Réservé à une utilisation ultérieure.
root/ConnectionType/freerdp/coreSettings/initialConnectionTimeout	Définit le temps d'attente en secondes pour une première réponse du serveur RDP avant d'abandonner.
root/ConnectionType/freerdp/coreSettings/label	Définit le nom à afficher pour ce type de connexion dans l'interface utilisateur.
root/ConnectionType/freerdp/coreSettings/priorityInConnectionLists	Définit la priorité de ce type de connexion lorsqu'elle s'affiche dans le gestionnaire de connexion et dans l'assistant de configuration qui s'affiche pendant l'installation initiale. Une valeur supérieure déplacera ce type de connexion vers le haut de la liste. Si la clé est définie sur 0, ce type de connexion est masqué pour l'assistant de configuration et figure en dernière place dans

Clé de registre	Description
	le gestionnaire de connexion. Les types de connexions avec la même priorité sont répertoriés dans l'ordre alphabétique.
`root/ConnectionType/freerdp/coreSettings/stopProcess`	Définit le comportement attendu lorsque la commande `connexion-mgr stop` est appelée sur cette connexion. Par défaut, il s'agit de `close`, qui provoque l'envoi d'un signal « kill » standard au processus. Si la valeur est définie sur `kill`, le processus spécifié par `appName` est tué de force. Si la valeur est définie sur `custom`, un script d'exécution personnalisé spécifié par `wrapperScript` sera exécuté avec l'argument `stop` pour mettre fin au processus normalement.
`root/ConnectionType/freerdp/coreSettings/tier`	Indique l'importance relative de ce type de connexion et l'ordre dans lequel elle est répertoriée dans le menu Créer.
`root/ConnectionType/freerdp/coreSettings/watchPid`	Si la valeur est définie sur 1, la connexion est contrôlée sous le nom spécifié par `appName`. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/freerdp/coreSettings/wrapperScript`	Définit le nom du script ou du fichier binaire à exécuter au lancement de ce type de connexion. C'est le script principal gérant tous les paramètres de connexion et arguments de ligne de commande pour la connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/freerdp/coreSettings/wrapperScriptGeneration`	Indique au gestionnaire de connexion quel type de paramètres transmettre au script de la passerelle.
`root/ConnectionType/freerdp/general/autoReconnectDialogTimeout`	Si `autoReconnect` est activée, cette clé définit le nombre de secondes avant l'expiration du délai des boîtes de dialogues d'erreur pour la connexion. Si la valeur est définie sur 0, les boîtes de dialogues attendent indéfiniment une interaction de l'utilisateur.
`root/ConnectionType/freerdp/general/disablePasswordChange`	Lorsqu'une ouverture de session à distance échoue en raison d'informations d'authentification incorrectes, un bouton s'affiche à l'utilisateur pour ouvrir une boîte de dialogue de mise à jour de son mot de passe. Si cette clé est définie est 1, ce bouton et cette boîte de dialogue ne sont pas affichés.
`root/ConnectionType/freerdp/general/preferredAudio`	Définit le serveur audio principal par défaut sur une redirection audio de haut niveau (entrée et sortie).
`root/ConnectionType/freerdp/general/rdWebFeedUrlPattern`	Définit le motif utilisé pour l'URL d'accès Internet RD. L'hôte de l'URL, par ex., myserver.com, est remplacé par la valeur du champ **Adresse** de la connexion. Ce modèle n'est pas utilisé lorsque l'adresse est déjà une URL.
`root/ConnectionType/freerdp/general/serialPortsDriver`	Ce paramètre garantit une meilleure compatibilité avec le pilote Windows sous-jacent prévu SerCx2.sys, SerCx.sys ou Serial.sys.
`root/ConnectionType/freerdp/general/serialPortsPermissive`	Si la valeur est définie sur 1, les erreurs en matière de fonctionnalités non prises en charge sont ignorées.

ssh

Clé de registre	Description
`root/ConnectionType/ssh/authorizations/user/add`	Si la clé est définie sur 1, un utilisateur final est autorisé à ajouter une nouvelle connexion de ce type à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.

Clé de registre	Description
root/ConnectionType/ssh/authorizations/user/general	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres généraux de ce type de connexion à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/ssh/connections/<UUID>/address	Définit le nom d'hôte ou l'adresse IP auquel se connecter.
root/ConnectionType/ssh/connections/<UUID>/afterStartedCommand	Permet de régler la commande à exécuter après le démarrage de la connexion.
root/ConnectionType/ssh/connections/<UUID>/afterStoppedCommand	Permet de régler la commande à exécuter une fois que la connexion a été arrêtée.
root/ConnectionType/ssh/connections/<UUID>/application	Spécifie l'application à exécuter.
root/ConnectionType/ssh/connections/<UUID>/authorizations/user/edit	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres de la connexion pour cette connexion.
root/ConnectionType/ssh/connections/<UUID>/authorizations/user/execution	Si la clé est définie sur 1, un utilisateur final est autorisé à exécuter cette connexion.
root/ConnectionType/ssh/connections/<UUID>/autoReconnect	Si la valeur est définie sur 1, la connexion redémarre lorsqu'elle est fermée ou déconnectée.
root/ConnectionType/ssh/connections/<UUID>/autoReconnectDelay	Définit le temps d'attente en secondes avant la reconnexion de la session. La valeur par défaut de 0 entraîne la reconnexion immédiate de la connexion. Ce paramètre ne prend effet que lorsque autoReconnect est définie sur 1.
root/ConnectionType/ssh/connections/<UUID>/autostart	Si définie sur une valeur de 1 à 5, la connexion se lancera automatiquement après le démarrage du système, la valeur de 1 ayant la priorité la plus élevée.
root/ConnectionType/ssh/connections/<UUID>/backgroundColor	Définit la couleur d'arrière-plan de la connexion.
root/ConnectionType/ssh/connections/<UUID>/beforeStartingCommand	Définit la commande à exécuter avant le démarrage de la connexion.
root/ConnectionType/ssh/connections/<UUID>/compression	Autorise la compression pour une connexion SSH.
root/ConnectionType/ssh/connections/<UUID>/connectionEndAction	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/ssh/connections/<UUID>/coord	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/ssh/connections/<UUID>/dependConnectionId	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/key	Définit le nom d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/ssh/connections/<UUID>/extraEnvValues/<UUID>/value	Définit la valeur d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/ssh/connections/<UUID>/fallBackConnection	Permet de régler la connexion de secours via son UUID.
root/ConnectionType/ssh/connections/<UUID>/font	Définit la taille de police de la connexion.

Clé de registre	Description
root/ConnectionType/ssh/connections/<UUID>/foregroundColor	Définit la couleur de premier plan de la connexion.
root/ConnectionType/ssh/connections/<UUID>/fork	Si la valeur est définie sur 1, l'option **Envoi d'une commande en arrière-plan** est activée pour la connexion.
root/ConnectionType/ssh/connections/<UUID>/hasDesktopIcon	Si la valeur est définie sur 1, l'icône du Bureau pour cette connexion est activée. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/ssh/connections/<UUID>/iconPosition	Définit les coordonnées x,y d'une icône de bureau fixée. Si aucune valeur n'est spécifiée, l'icône est flottante.
root/ConnectionType/ssh/connections/<UUID>/isInMenu	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/ssh/connections/<UUID>/label	Définit le nom de connexion qui s'affiche dans l'interface utilisateur. Sur Smart Zero, ce paramètre est normalement défini sur `Default Connection` et ne s'affiche pas dans l'interface utilisateur.
root/ConnectionType/ssh/connections/<UUID>/loginfields/server	S'il est réglé sur 1, le champ **mot de passe** est affiché dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, la case est affichée puis désactivée. Si la valeur est réglée sur 0, la case est masquée. Si la valeur est définie sur 3, les paramètres du système sont utilisés.
root/ConnectionType/ssh/connections/<UUID>/loginfields/username	Si la valeur est réglée à 1, la case **User Name** (Nom d'utilisateur) apparaît dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, la case est affichée puis désactivée. Si la valeur est réglée sur 0, la case est masquée. Si la valeur est définie sur 3, les paramètres du système sont utilisés.
root/ConnectionType/ssh/connections/<UUID>/port	Définit le numéro de port à utiliser pour contacter le serveur SSH. La valeur par défaut est 22.
root/ConnectionType/ssh/connections/<UUID>/startMode	Si la valeur par défaut `focus` est définie et que la connexion a déjà démarré, la connexion est mise en avant. Sinon, une erreur est renvoyée indiquant que la connexion est déjà démarrée.
root/ConnectionType/ssh/connections/<UUID>/tty	Si la valeur est définie sur 1, l'option **Forcer l'allocation TTY** est activée pour la connexion.
root/ConnectionType/ssh/connections/<UUID>/username	Définit le nom d'utilisateur par défaut à fournir à l'hôte distant lors de l'ouverture de session. En général, ce paramètre est utilisé avec les applications de style kiosque dans lesquelles un nom d'utilisateur générique est utilisé pour l'ouverture de session.
root/ConnectionType/ssh/connections/<UUID>/waitForNetwork	Si la valeur est définie sur 1, la connexion n'est pas lancée tant que le réseau n'est pas disponible. Ce paramètre permet de s'assurer que, sur un réseau lent, la connexion ne se lance pas avant que le réseau soit disponible, ce qui pourrait entraîner un échec.
root/ConnectionType/ssh/connections/<UUID>/x11	Si la valeur est définie sur 1, l'option **Transfert de la connexion X11** est activée pour la connexion.
root/ConnectionType/ssh/coreSettings/USBrelevant	Spécifie si ce type de connexion est conforme à l'USB. Si c'est le cas, il peut y avoir une connexion USB pour rediriger les périphériques USB.
root/ConnectionType/ssh/coreSettings/appName	Définit le nom de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/ssh/coreSettings/className	Définit la classe de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.

Clé de registre	Description
`root/ConnectionType/ssh/coreSettings/editor`	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de connexion s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/ssh/coreSettings/icon`	Spécifie l'icône à partir du thème d'icône défini à utiliser pour cette connexion.
`root/ConnectionType/ssh/coreSettings/icon16Path`	Définit le chemin d'accès à l'icône 16 x 16 pixels représentant cette application.
`root/ConnectionType/ssh/coreSettings/icon32Path`	Définit le chemin d'accès à l'icône 32 x 32 pixels représentant cette application.
`root/ConnectionType/ssh/coreSettings/icon48Path`	Définit le chemin d'accès à l'icône 48 x 48 pixels représentant cette application.
`root/ConnectionType/ssh/coreSettings/iconActive`	Réservé à une utilisation ultérieure.
`root/ConnectionType/ssh/coreSettings/label`	Définit le nom à afficher pour ce type de connexion dans l'interface utilisateur.
`root/ConnectionType/ssh/coreSettings/priorityInConnectionLists`	Définit la priorité de ce type de connexion lorsqu'elle s'affiche dans le gestionnaire de connexion et dans l'assistant de configuration qui s'affiche pendant l'installation initiale. Une valeur supérieure déplacera ce type de connexion vers le haut de la liste. Si la clé est définie sur 0, ce type de connexion est masqué pour l'assistant de configuration et figure en dernière place dans le gestionnaire de connexion. Les types de connexions avec la même priorité sont répertoriés dans l'ordre alphabétique.
`root/ConnectionType/ssh/coreSettings/serverRequired`	Définit si un nom ou une adresse de serveur est `unused`, `optional` ou `required` pour ce type de connexion.
`root/ConnectionType/ssh/coreSettings/stopProcess`	Définit le comportement attendu lorsque la commande `connexion-mgr stop` est appelée sur cette connexion. Par défaut, il s'agit de `close`, qui provoque l'envoi d'un signal « kill » standard au processus. Si la valeur est définie sur `kill`, le processus spécifié par `appName` est tué de force. Si la valeur est définie sur `custom`, un script d'exécution personnalisé spécifié par `wrapperScript` sera exécuté avec l'argument `stop` pour mettre fin au processus normalement.
`root/ConnectionType/ssh/coreSettings/tier`	Indique l'importance relative de ce type de connexion et l'ordre dans lequel elle est répertoriée dans le menu Créer.
`root/ConnectionType/ssh/coreSettings/watchPid`	Si la valeur est définie sur 1, la connexion est contrôlée sous le nom spécifié par `appName`. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/ssh/coreSettings/wrapperScript`	Définit le nom du script ou du fichier binaire à exécuter au lancement de ce type de connexion. Il s'agit du script principal gérant tous les paramètres de connexion et les arguments de ligne de commande de la connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/ssh/gui/SshManager/name`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/ssh/gui/SshManager/status`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/ssh/gui/SshManager/title`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.

Clé de registre	Description
`root/ConnectionType/ssh/gui/SshManager/widgets/address`	Contrôle l'état du widget **Adresse** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/application`	Contrôle l'état du widget **Exécuter l'application** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/autoReconnect`	Contrôle l'état du widget **Reconnexion automatique** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/autostart`	Contrôle l'état du widget **Priorité du démarrage automatique** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/backgroundColor`	Contrôle l'état du widget **Couleur de l'arrière-plan** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/compression`	Contrôle l'état du widget **Compression** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/fallBackConnection`	Contrôle l'état du widget **Connexion de repli** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/font`	Contrôle l'état du widget **Police** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/foregroundColor`	Contrôle l'état du widget **Couleur du premier plan** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/fork`	Contrôle l'état du widget **Envoyer une commande en arrière-plan** dans le gestionnaire de connexion Secure Shell. Si la clé est

Clé de registre	Description
	définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/hasDesktopIcon`	Contrôle l'état du widget **Afficher l'icône sur le Bureau** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/isInMenu`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/ssh/gui/SshManager/widgets/label`	Contrôle l'état du widget **Nom** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/port`	Contrôle l'état du widget **Port** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/tty`	Contrôle l'état du widget **Forcer l'allocation TTY** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/username`	Contrôle l'état du widget **Nom d'utilisateur** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/waitForNetwork`	Contrôle l'état du widget **Attendre le réseau avant connexion** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/ssh/gui/SshManager/widgets/x11`	Contrôle l'état du widget **Transfert de la connexion X11** dans le gestionnaire de connexion Secure Shell. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.

telnet

Clé de registre	Description
root/ConnectionType/telnet/authorizations/user/add	Si la clé est définie sur 1, un utilisateur final est autorisé à ajouter une nouvelle connexion de ce type à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/telnet/authorizations/user/general	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres généraux de ce type de connexion à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/telnet/connections/<UUID>/address	Définit le nom d'hôte ou l'adresse IP auquel se connecter.
root/ConnectionType/telnet/connections/<UUID>/afterStartedCommand	Permet de régler la commande à exécuter après le démarrage de la connexion.
root/ConnectionType/telnet/connections/<UUID>/afterStoppedCommand	Permet de régler la commande à exécuter une fois que la connexion a été arrêtée.
root/ConnectionType/telnet/connections/<UUID>/authorizations/user/edit	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres de la connexion pour cette connexion.
root/ConnectionType/telnet/connections/<UUID>/authorizations/user/execution	Si la clé est définie sur 1, un utilisateur final est autorisé à exécuter cette connexion.
root/ConnectionType/telnet/connections/<UUID>/autoReconnect	Si la valeur est définie sur 1, la connexion redémarre lorsqu'elle est fermée ou déconnectée.
root/ConnectionType/telnet/connections/<UUID>/autostart	Si définie sur une valeur de 1 à 5, la connexion se lancera automatiquement après le démarrage du système, la valeur de 1 ayant la priorité la plus élevée.
root/ConnectionType/telnet/connections/<UUID>/backgroundColor	Définit la couleur d'arrière-plan de la connexion.
root/ConnectionType/telnet/connections/<UUID>/beforeStartingCommand	Définit la commande à exécuter avant le démarrage de la connexion.
root/ConnectionType/telnet/connections/<UUID>/connectionEndAction	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/telnet/connections/<UUID>/coord	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/telnet/connections/<UUID>/dependConnectionId	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/key	Définit le nom d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/telnet/connections/<UUID>/extraEnvValues/<UUID>/value	Définit la valeur d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/telnet/connections/<UUID>/fallBackConnection	Permet de régler la connexion de secours via son UUID.
root/ConnectionType/telnet/connections/<UUID>/font	Définit la taille de police de la connexion.
root/ConnectionType/telnet/connections/<UUID>/foregroundColor	Définit la couleur de premier plan de la connexion.
root/ConnectionType/telnet/connections/<UUID>/hasDesktopIcon	Si la valeur est définie sur 1, l'icône du Bureau pour cette connexion est activée. Cette clé n'a aucun effet sur Smart Zero.

Clé de registre	Description
`root/ConnectionType/telnet/connections/<UUID>/iconPosition`	Définit les coordonnées x,y d'une icône de bureau fixée. Si aucune valeur n'est spécifiée, l'icône est flottante.
`root/ConnectionType/telnet/connections/<UUID>/label`	Définit le nom de connexion qui s'affiche dans l'interface utilisateur. Sur Smart Zero, ce paramètre est normalement défini sur `Default Connection` et ne s'affiche pas dans l'interface utilisateur.
`root/ConnectionType/telnet/connections/<UUID>/locale`	Définit les paramètres régionaux de premier plan de la connexion.
`root/ConnectionType/telnet/connections/<UUID>/loginfields/server`	S'il est réglé sur 1, le champ **mot de passe** est affiché dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, la case est affichée puis désactivée. Si la valeur est réglée sur 0, la case est masquée. Si la valeur est définie sur 3, les paramètres du système sont utilisés.
`root/ConnectionType/telnet/connections/<UUID>/port`	Définit le numéro de port à utiliser pour contacter le serveur. La valeur par défaut est 23.
`root/ConnectionType/telnet/connections/<UUID>/startMode`	Si la valeur par défaut `focus` est définie et que la connexion a déjà démarré, la connexion est mise en avant. Sinon, une erreur est renvoyée indiquant que la connexion est déjà démarrée.
`root/ConnectionType/telnet/connections/<UUID>/waitForNetwork`	Si la valeur est définie sur 1, la connexion n'est pas lancée tant que le réseau n'est pas disponible. Ce paramètre permet de s'assurer que, sur un réseau lent, la connexion ne se lance pas avant que le réseau soit disponible, ce qui pourrait entraîner un échec.
`root/ConnectionType/telnet/coreSettings/USBrelevant`	Spécifie si ce type de connexion est conforme à l'USB. Si c'est le cas, il peut y avoir une connexion USB pour rediriger les périphériques USB.
`root/ConnectionType/telnet/coreSettings/appName`	Définit le nom de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/telnet/coreSettings/className`	Définit la classe de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/telnet/coreSettings/editor`	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de connexion s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/telnet/coreSettings/generalSettingsEditor`	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de paramètres généraux s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/telnet/coreSettings/icon`	Spécifie l'icône à partir du thème d'icône défini à utiliser pour cette connexion.
`root/ConnectionType/telnet/coreSettings/icon16Path`	Définit le chemin d'accès à l'icône 16 x 16 pixels représentant cette application.
`root/ConnectionType/telnet/coreSettings/icon32Path`	Définit le chemin d'accès à l'icône 32 x 32 pixels représentant cette application.
`root/ConnectionType/telnet/coreSettings/icon48Path`	Définit le chemin d'accès à l'icône 48 x 48 pixels représentant cette application.
`root/ConnectionType/telnet/coreSettings/iconActive`	Réservé à une utilisation ultérieure.
`root/ConnectionType/telnet/coreSettings/label`	Définit le nom à afficher pour ce type de connexion dans l'interface utilisateur.

Clé de registre	Description
`root/ConnectionType/telnet/coreSettings/priorityInConnectionLists`	Définit la priorité de ce type de connexion lorsqu'elle s'affiche dans le gestionnaire de connexion et dans l'assistant de configuration qui s'affiche pendant l'installation initiale. Une valeur supérieure déplacera ce type de connexion vers le haut de la liste. Si la valeur est définie sur 0, ce type de connexion est masqué pour l'assistant de configuration et figure en dernière place dans le gestionnaire de connexion. Les types de connexions avec la même priorité sont répertoriés dans l'ordre alphabétique.
`root/ConnectionType/telnet/coreSettings/serverRequired`	Définit si un nom ou une adresse de serveur est `unused`, `optional` ou `required` pour ce type de connexion.
`root/ConnectionType/telnet/coreSettings/stopProcess`	Définit le comportement attendu lorsque la commande `connexion-mgr stop` est appelée sur cette connexion. Par défaut, il s'agit de `close`, qui provoque l'envoi d'un signal « kill » standard au processus. Si la valeur est définie sur `kill`, le processus spécifié par `appName` est tué de force. Si la valeur est définie sur `custom`, un script d'exécution personnalisé spécifié par `wrapperScript` sera exécuté avec l'argument `stop` pour mettre fin au processus normalement.
`root/ConnectionType/telnet/coreSettings/tier`	Indique l'importance relative de ce type de connexion et l'ordre dans lequel elle est répertoriée dans le menu Créer.
`root/ConnectionType/telnet/coreSettings/wrapperScript`	Définit le nom du script ou du fichier binaire à exécuter au lancement de ce type de connexion. Il s'agit du script principal gérant tous les paramètres de connexion et les arguments de ligne de commande de la connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/telnet/gui/TelnetManager/name`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/telnet/gui/TelnetManager/status`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/telnet/gui/TelnetManager/title`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/address`	Contrôle l'état du widget **Adresse** dans le gestionnaire de connexion Telnet. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/autoReconnect`	Contrôle l'état du widget **Reconnexion automatique** dans le gestionnaire de connexion Telnet. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/autostart`	Contrôle l'état du widget **Priorité du démarrage automatique** dans le gestionnaire de connexion Telnet. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/backgroundColor`	Contrôle l'état du widget **Couleur de l'arrière-plan** dans le gestionnaire de connexion Telnet. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le

Clé de registre	Description
	widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/fallBackConnection`	Contrôle l'état du widget **Connexion de repli** dans le gestionnaire de connexion Telnet. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/foregroundColor`	Contrôle l'état du widget **Couleur du premier plan** dans le gestionnaire de connexion Telnet. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/hasDesktopIcon`	Contrôle l'état du widget **Afficher l'icône sur le Bureau** dans le gestionnaire de connexion Telnet. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/label`	Contrôle l'état du widget **Nom** dans le gestionnaire de connexion Telnet. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/port`	Contrôle l'état du widget **Port** dans le gestionnaire de connexion Telnet. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/telnet/gui/TelnetManager/widgets/waitForNetwork`	Contrôle l'état du widget **Attendre le réseau avant connexion** dans le gestionnaire de connexion Telnet. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.

view

Clé de registre	Description
`root/ConnectionType/view/authorizations/user/add`	Si la clé est définie sur 1, un utilisateur final est autorisé à ajouter une nouvelle connexion de ce type à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
`root/ConnectionType/view/authorizations/user/commandLineBox`	Si la clé est définie sur 1, un utilisateur final est autorisé à saisir des arguments de ligne de commande dans le gestionnaire de connexion VMware Horizon View.
`root/ConnectionType/view/authorizations/user/general`	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres généraux de ce type de connexion à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.

Clé de registre	Description
`root/ConnectionType/view/connections/<UUID>/ExtraArgs`	Spécifie des arguments supplémentaires pour le client VMware Horizon View. Exécutez `view_client --help` ou `vmware-view --help` dans un terminal X pour afficher tous les arguments disponibles.
`root/ConnectionType/view/connections/<UUID>/SingleSignOn`	
`root/ConnectionType/view/connections/<UUID>/afterStartedCommand`	Permet de régler la commande à exécuter après le démarrage de la connexion.
`root/ConnectionType/view/connections/<UUID>/afterStoppedCommand`	Permet de régler la commande à exécuter une fois que la connexion a été arrêtée.
`root/ConnectionType/view/connections/<UUID>/allowBlacklistedDrivers`	Si défini sur 1, permet aux connexions VMware Horizon View d'activer la fonctionnalité H.264 avec les pilotes graphiques open-source AMD. Si défini sur 0, les connexions VMware Horizon View désactivent l'accélération matérielle avec les pilotes figurant sur la liste noire (comme AMDGPU et Radeon).
`root/ConnectionType/view/connections/<UUID>/appInMenu`	Si la valeur est définie sur 1, toutes les applications de cette connexion s'affichent dans le menu de la barre des tâches.
`root/ConnectionType/view/connections/<UUID>/appOnDesktop`	Si la valeur est définie sur 1, toutes les applications de cette connexion s'affichent sur le bureau.
`root/ConnectionType/view/connections/<UUID>/applicationSize`	Définit la taille dans laquelle le client VMware Horizon View lance les applications.
`root/ConnectionType/view/connections/<UUID>/attachToConsole`	
`root/ConnectionType/view/connections/<UUID>/authorizations/user/edit`	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres de la connexion pour cette connexion.
`root/ConnectionType/view/connections/<UUID>/authorizations/user/execution`	Si la clé est définie sur 1, un utilisateur final est autorisé à exécuter cette connexion.
`root/ConnectionType/view/connections/<UUID>/autoHideMenuBar`	
`root/ConnectionType/view/connections/<UUID>/autoReconnect`	Si la valeur est définie sur 1, la connexion redémarre lorsqu'elle est fermée ou déconnectée.
`root/ConnectionType/view/connections/<UUID>/autoReconnectDelay`	Définit le temps d'attente en secondes avant la reconnexion de la session. La valeur par défaut de 0 entraîne la reconnexion immédiate de la connexion. Ce paramètre ne prend effet que lorsque `autoReconnect` est définie sur 1.
`root/ConnectionType/view/connections/<UUID>/automaticLogin`	Si la clé est définie sur 1, le client VMware Horizon View tente de se connecter automatiquement si tous les champs sont fournis. Si la clé est définie sur 0, les utilisateurs doivent sélectionner **Se connecter** manuellement dans le client VMware Horizon View, se connecter, puis sélectionner un bureau.
`root/ConnectionType/view/connections/<UUID>/autostart`	Si définie sur une valeur de 1 à 5, la connexion se lancera automatiquement après le démarrage du système, la valeur de 1 ayant la priorité la plus élevée.
`root/ConnectionType/view/connections/<UUID>/autostartDelay`	Réservé à une utilisation ultérieure.
`root/ConnectionType/view/connections/<UUID>/beforeStartingCommand`	Définit la commande à exécuter avant le démarrage de la connexion.

Clé de registre	Description
root/ConnectionType/view/connections/<UUID>/closeAfterDisconnect	Si la valeur est définie sur 1, la connexion est terminée après la fermeture du premier bureau. Si la valeur est définie sur 0, le client VMware Horizon View revient à l'écran de sélection du bureau. Ce paramètre est activé par défaut pour empêcher les utilisateurs de quitter involontairement la connexion dans l'écran de sélection du bureau après la fermeture de session.
root/ConnectionType/view/connections/<UUID>/closeAfterRoaming	Si elle est définie sur 1, la connexion VMware est déconnectée si elle est envoyée à un autre emplacement..
root/ConnectionType/view/connections/<UUID>/coord	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/view/connections/<UUID>/credentialsType	Spécifie le type d'informations d'authentification parmi anonymous (accès non-authentifié), sso (authentification unique), startup (les informations d'authentification sont demandées au démarrage), password (utilisateur/domaine/mot de passe préconfiguré) ou smartcard (carte à puce).
root/ConnectionType/view/connections/<UUID>/dependConnectionId	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/view/connections/<UUID>/desktop	Si celui-ci est spécifié, le bureau indiqué sera automatiquement lancé à l'ouverture de session. Par défaut, si un seul bureau est disponible, il sera automatiquement lancé même lorsqu'il n'est pas indiqué.
root/ConnectionType/view/connections/<UUID>/desktopSize	Définit la taille dans laquelle le client VMware Horizon View lance le bureau.
root/ConnectionType/view/connections/<UUID>/directory	
root/ConnectionType/view/connections/<UUID>/disableMaximizedApp	Si la valeur est définie sur 1, les paramètres de taille de fenêtre pour les applications agrandies sont désactivés.
root/ConnectionType/view/connections/<UUID>/domain	Définit le domaine à fournir au serveur View Connection. Si aucun domaine n'est spécifié, le domaine par défaut du serveur est utilisé.
root/ConnectionType/view/connections/<UUID>/enableCDR	Si défini sur 1, l'extension Client Drive Redirection est activée.
root/ConnectionType/view/connections/<UUID>/enableMMR	Si la valeur est définie sur 1, le module Redirection multimédia est activé via le protocole Blast/PCoIP, ce qui entraîne la redirection vers le client des codecs compatibles lus dans Windows Media Player. La lecture de vidéos en haute définition et en plein écran pour les codecs comme WMV9, VC1 et MPEG4 est considérablement améliorée. La vidéo est rendue localement à l'aide de la puissance du processeur.
root/ConnectionType/view/connections/<UUID>/enableMediaProvider	Si défini sur 1, le composant Pack de virtualisation VMware Horizon pour Skype pour les Professionnels est activé. Ce composant permet aux utilisateurs de Linux de rediriger des appels Skype pour les Professionnels avec le client VMware Horizon View.
root/ConnectionType/view/connections/<UUID>/enableSeamlessWindow	Si défini sur 1, le client VMware Horizon View démarre des applications en mode fenêtre transparente.
root/ConnectionType/view/connections/<UUID>/enableSingleMode	
root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/key	Définit le nom d'une variable d'environnement supplémentaire à utiliser avec la connexion.

Clé de registre	Description
`root/ConnectionType/view/connections/<UUID>/extraEnvValues/<UUID>/value`	Définit la valeur d'une variable d'environnement supplémentaire à utiliser avec la connexion.
`root/ConnectionType/view/connections/<UUID>/fallBackConnection`	Permet de régler la connexion de secours via son UUID.
`root/ConnectionType/view/connections/<UUID>/fullscreen`	Si la valeur est définie sur 1, le client VMware Horizon View se lance en mode plein écran lors du démarrage.
`root/ConnectionType/view/connections/<UUID>/hasDesktopIcon`	Si la valeur est définie sur 1, l'icône du Bureau pour cette connexion est activée. Cette clé n'a aucun effet sur Smart Zero.
`root/ConnectionType/view/connections/<UUID>/hideMenuBar`	Si la valeur est définie sur 1, la barre de menus supérieure du bureau est masquée. Cette barre permet de gérer les périphériques distants et de démarrer d'autres bureaux.
`root/ConnectionType/view/connections/<UUID>/iconPosition`	Définit les coordonnées x,y d'une icône de bureau fixée. Si aucune valeur n'est spécifiée, l'icône est flottante.
`root/ConnectionType/view/connections/<UUID>/isInMenu`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/view/connections/<UUID>/label`	Définit le nom de connexion qui s'affiche dans l'interface utilisateur. Sur Smart Zero, ce paramètre est normalement défini sur `Default Connection` et ne s'affiche pas dans l'interface utilisateur.
`root/ConnectionType/view/connections/<UUID>/lockServer`	Si la clé est définie sur 1, les utilisateurs finaux ne peuvent pas modifier l'adresse du serveur.
`root/ConnectionType/view/connections/<UUID>/loginfields/domain`	Si la valeur est définie sur 1, le champ **Domaine** est affiché dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, le champ est affiché puis désactivé. Si la valeur est définie sur 0, le champ est masqué.
`root/ConnectionType/view/connections/<UUID>/loginfields/password`	Si la valeur est définie sur 1, le champ **Mot de passe** est affiché dans la boîte de dialogue ouverture de session pour la connexion. Si la valeur est définie sur 2, le champ est affiché puis désactivé. Si la valeur est définie sur 0, le champ est masqué.
`root/ConnectionType/view/connections/<UUID>/loginfields/rememberme`	Lorsqu'elle est définie sur 1, la case **Se souvenir de moi** figure dans la boîte de dialogue d'ouverture de session pour la connexion. Lorsqu'elle est définie sur 2, la case est affichée mais désactivée. Lorsqu'elle est définie sur 0, la case est masquée.
`root/ConnectionType/view/connections/<UUID>/loginfields/server`	S'il est réglé sur 1, le champ **mot de passe** est affiché dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, la case est affichée puis désactivée. Si la valeur est réglée sur 0, la case est masquée. Si la valeur est définie sur 3, les paramètres du système sont utilisés.
`root/ConnectionType/view/connections/<UUID>/loginfields/showpassword`	Lorsqu'elle est définie sur 1, la case **Se souvenir de moi** figure dans la boîte de dialogue d'ouverture de session pour la connexion. Lorsqu'elle est définie sur 2, la case est affichée mais désactivée. Lorsqu'elle est définie sur 0, la case est masquée.
`root/ConnectionType/view/connections/<UUID>/loginfields/smartcard`	Lorsqu'elle est définie sur 1, la case **Connexion carte à puce** figure dans la boîte de dialogue d'ouverture de session pour la connexion. Lorsqu'elle est définie sur 2, la case est affichée mais désactivée. Lorsqu'elle est définie sur 0, la case est masquée. Cette case peut ne pas figurer si aucune carte à puce n'est détectée, même si cette option est activée.
`root/ConnectionType/view/connections/<UUID>/loginfields/username`	Si la valeur est définie sur 1, le champ **Nom d'utilisateur** apparaît dans la boîte de dialogue d'ouverture de session pour la

Clé de registre	Description
	connexion. Si la valeur est définie sur 2, le champ est affiché puis désactivé. Si la valeur est définie sur 0, le champ est masqué.
`root/ConnectionType/view/connections/<UUID>/networkCondition`	Permet de sélectionner les conditions du réseau pour bénéficier de la meilleure expérience possible.
`root/ConnectionType/view/connections/<UUID>/password`	Définit le mot de passe par défaut à fournir à l'hôte distant lors de l'ouverture de session. Cette valeur est cryptée. En général, ce paramètre est utilisé avec les applications de style kiosque dans lesquelles un mot de passe générique est utilisé pour l'ouverture de session.
`root/ConnectionType/view/connections/<UUID>/preferredProtocol`	Définit le protocole favori.
`root/ConnectionType/view/connections/<UUID>/printerMapping`	Lorsqu'elle est définie sur 1, toutes les imprimantes définies localement via CUPS sont redirigées vers l'hôte distant via ThinPrint. Lorsqu'elle est définie sur 0, le mappage d'imprimante est désactivé. Si la valeur est définie sur 2, les imprimantes USB sont redirigées selon la configuration définie dans le gestionnaire USB.
`root/ConnectionType/view/connections/<UUID>/saveCredentials`	
`root/ConnectionType/view/connections/<UUID>/sendCtrlAltDelToVM`	
`root/ConnectionType/view/connections/<UUID>/server`	Définit l'adresse de l'hôte distant auquel se connecter. Il s'agit généralement d'une URL de type `http://server.domain.com`.
`root/ConnectionType/view/connections/<UUID>/sessionEndAction`	
`root/ConnectionType/view/connections/<UUID>/singleDesktop`	
`root/ConnectionType/view/connections/<UUID>/smartcard`	Si la valeur est définie sur 1, les cartes Smart Card connectées localement sont transmises à l'hôte distant, ce qui leur permettra d'être utilisées par les applications sur l'hôte distant. Cela permet uniquement de connecter les cartes Smart Card à l'hôte distant et non au serveur View Connection.
`root/ConnectionType/view/connections/<UUID>/startMode`	Si la valeur par défaut `focus` est définie et que la connexion a déjà démarré, la connexion est mise en avant. Sinon, une erreur est renvoyée indiquant que la connexion est déjà démarrée.
`root/ConnectionType/view/connections/<UUID>/usbAutoConnectAtStartUp`	
`root/ConnectionType/view/connections/<UUID>/usbAutoConnectOnInsert`	
`root/ConnectionType/view/connections/<UUID>/useCurrentViewConfig`	Si défini sur 1, le script HP ne crée pas un nouveau fichier `/etc/vmware/config` et le client VMware Horizon View utilise le fichier actuel `/etc/vmware/config`.
`root/ConnectionType/view/connections/<UUID>/username`	Définit le nom d'utilisateur par défaut à fournir à l'hôte distant lors de l'ouverture de session. En général, ce paramètre est utilisé avec les applications de style kiosque dans lesquelles un nom d'utilisateur générique est utilisé pour l'ouverture de session.

Clé de registre	Description
root/ConnectionType/view/connections/<UUID>/viewSecurityLevel	Si la valeur `Refuse insecure connections` est définie, le client VMware Horizon View n'autorisera pas l'utilisateur à se connecter au serveur View Connection si le certificat du serveur SSL n'est pas valide. Si la valeur est définie sur `Warn`, le client VMware Horizon View affichera un avertissement si le certificat du serveur ne peut pas être vérifié. S'il est auto-signé ou a expiré, l'utilisateur ne sera pas non plus autorisé à se connecter. Si la valeur est définie sur `Allow all connections`, le certificat du serveur ne sera pas vérifié et la connexion à tous les serveurs sera autorisée.
root/ConnectionType/view/connections/<UUID>/waitForNetwork	Si la valeur est définie sur 1, la connexion n'est pas lancée tant que le réseau n'est pas disponible. Ce paramètre permet de s'assurer que, sur un réseau lent, la connexion ne se lance pas avant que le réseau soit disponible, ce qui pourrait entraîner un échec.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/attachToConsole	
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/audioLatency	Définit la durée moyenne en millisecondes du décalage entre le flux audio et l'affichage des images vidéo correspondantes après décodage.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/clipboardExtension	Si la clé est définie sur 1, la fonctionnalité de presse-papiers est activée entre différentes sessions RDP et entre les sessions RDP et le système local.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/colorDepth	Ce paramètre est obsolète. Il permet de réduire la profondeur de couleur de la connexion sous celle de la résolution native du bureau. Cela a fréquemment été utilisé pour réduire la bande passante du réseau. La réduction de la profondeur de couleur à un niveau non pris en charge par le pilote vidéo peut provoquer une corruption de l'écran ou un échec du lancement.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/compression	Si la valeur est définie sur 1, la compression des données RDP entre le client et le serveur est activée.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/disableMMRwithRFX	Si la valeur est définie sur 1, la redirection multimédia est désactivée si une session RemoteFX valide est établie.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/enableMMR	Si la valeur est définie sur 1, l'extension Redirection multimédia est activée, ce qui entraîne la redirection vers le client des codecs compatibles lus dans Windows Media Player.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/frameAcknowledgeCount	Définit le nombre d'images vidéo que le serveur peut envoyer sans attendre d'accusé de réception de la part du client. Des valeurs plus faibles donnent lieu à un bureau plus réactif, mais réduisent le nombre d'image par seconde. Si la valeur est définie sur 0, les interactions client-serveur portant sur les images se font sans accusé de réception.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname	Si la valeur `hostname` est définie, le nom d'hôte du système est envoyé à l'hôte distant. Ce paramétrage est généralement utilisé pour identifier le client léger, associé à une session RDP donnée. Le nom d'hôte envoyé peut être remplacé à l'aide de `sendHostname` dans les paramètres spécifiques à la connexion. Si la valeur est définie sur `mac`, l'adresse MAC du premier adaptateur réseau disponible est envoyée à la place du nom d'hôte.
root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/hostnameType	Si la valeur hostname est définie, le nom d'hôte du système est envoyé à l'hôte distant. Ce paramétrage est généralement utilisé pour identifier le client léger, associé à une session RDP donnée.

Clé de registre	Description
	Le nom d'hôte envoyé peut être remplacé à l'aide de `sendHostname` dans les paramètres spécifiques à la connexion. Si la valeur est définie sur mac, l'adresse MAC du premier adaptateur réseau disponible est envoyée à la place du nom d'hôte.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/loadBalanceInfo`	Cette valeur est le cookie d'équilibrage de charge envoyé à des fins de brokering au serveur lors de la connexion et correspond au champ `loadbalanceinfo` du fichier .rdp. Par défaut, la valeur est vide.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/mouseMotionEvents`	Si la valeur est définie sur 0, les évènements de déplacement de la souris ne sont pas envoyés au serveur. Ce paramétrage peut empêcher certaines interactions de l'utilisateur, comme les info-bulles, de fonctionner correctement.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/offScreenBitmaps`	Si la valeur est définie sur 0, les images bitmaps hors écran sont désactivées. Cela peut augmenter légèrement les performances, mais provoquera une mise à jour asynchrone de certains blocs de l'écran, ce qui entraine des actualisations d'écran non-uniformes.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagDesktopComposition`	Si la valeur est définie sur 1, cette clé permet la composition du bureau, par exemple des bordures translucides, lorsque cette fonction est prise en charge par le serveur. La désactivation de ce paramètre peut améliorer les performances sur les connexions à faible bande passante. En général, ce paramètre affecte uniquement RemoteFX. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagFontSmoothing`	Si la valeur est définie sur 1, cette clé permet le lissage de police lorsque cette fonction est prise en charge par le serveur et activée. La désactivation de ce paramètre peut améliorer les performances sur les connexions à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorSettings`	Si la valeur est définie sur 1, le clignotement de curseur est désactivé, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoCursorShadow`	Si la valeur est définie sur 1, les ombres de curseur sont désactivées, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoMenuAnimations`	Si la valeur est définie sur 1, les animations de menu sont désactivées, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoTheming`	Si la valeur est définie sur 1, les thèmes d'interface utilisateur sont désactivés, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoWallpaper`	Si la valeur est définie sur 1, le papier peint du bureau est désactivé, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/perfFlagNoWindowDrag`	Si la valeur est définie sur 1, le glissement de fenêtre intégral est désactivé, ce qui peut améliorer les performances sur les connexions RDP à faible bande passante. Le contour de la fenêtre

Clé de registre	Description
	est utilisé à la place. Si définie sur 2, la valeur est sélectionnée en fonction de la performance du client léger.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/portMapping`	Si la valeur est définie sur 1, les ports séries et parallèles suivants sont redirigés vers l'hôte distant : ttyS0, ttyS1, ttyS2, ttyS3, ttyUSB0, lp0.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/printerMapping`	Si la valeur est définie sur 1, toutes les imprimantes définies localement via CUPS sont redirigées vers l'hôte distant.
`root/ConnectionType/freerdp/connections/<UUID>/rdp6Buffering`	Si la valeur est définie sur 1, les performances graphiques non-RemoteFX, sont augmentées au coût de mises à jour d'écran moins fréquentes.
`root/ConnectionType/freerdp/connections/<UUID>/rdp8Codecs`	Si la valeur est définie sur 1, des codecs RDP 8 sont utilisés s'ils sont disponibles. Ce paramètre doit être désactivé uniquement dans le cas d'un défaut spécifique aux codecs RDP 8. La désactivation de ce paramètre peut également désactiver des codecs plus avancés.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/rdpEncryption`	Si la valeur est définie sur 1, un cryptage RDP standard est utilisé pour crypter toutes les données entre le client et le serveur.
`root/ConnectionType/freerdp/connections/<UUID>/rdpH264Codec`	Si la valeur est définie sur 1, des codecs RDP 8 H.264 sont utilisés s'ils sont disponibles. Ce paramètre présente des erreurs visuelles connues, en particulier dans des configurations à plusieurs écrans et il doit être considéré comme expérimental et non pris en charge. L'activation de ce paramètre informe simplement le serveur que le client léger prend en charge les H.264 pour l'affichage du bureau. Le serveur doit également prendre en charge les H.264, et le serveur prend la décision finale sur les codecs à utiliser. Ce paramètre affecte uniquement les codecs bureau. Il n'affecte pas les codecs de redirection multimédia.
`root/ConnectionType/freerdp/connections/<UUID>/rdpProgressiveCodec`	Si la valeur est définie sur 1, des codecs progressifs RDP 8 sont utilisés s'ils sont disponibles. Ce paramètre doit être désactivé uniquement dans le cas d'un défaut spécifique aux codecs progressif RDP 8. La désactivation de ce paramètre peut également désactiver des codecs plus avancés.
`root/ConnectionType/freerdp/connections/<UUID>/redirectPreference`	Pour la redirection, le client RDP se voit proposer plusieurs destinations possibles. Il les essaie toutes, dans l'ordre suivant : FQDN, IP principale, liste d'IP, NetBIOS. Si FQDN n'est pas souhaité, une des autres alternatives peut être tentée en premier en définissant cette clé de registre. Si la méthode spécifiée ne fonctionne pas, le client RDP reprend l'ordre d'origine. Le paramétrage sur `auto` force l'ordre d'origine.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/remoteFx`	Si la valeur est définie sur 1, RemoteFX est utilisé s'il est disponible.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sendHostname`	Définit le nom d'hôte du client léger qui est envoyé à l'hôte distant. Si vide, le nom d'hôte du système est envoyé. La clé de registre `root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/general/sendHostname` doit être définie sur `hostname` pour que cette clé soit utilisée.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/sound`	Si la valeur est définie sur le paramètre `Bring to this computer`, le son est redirigé de l'hôte distant vers le client à l'aide d'un canal virtuel standard. Si la valeur est définie sur `Leave at remote computer`, le son est laissé sur l'hôte distant. Ce paramétrage peut être utile dans le cas où un périphérique audio redirigé par USB est utilisé. Si la valeur est définie sur une autre valeur, le son est désactivé. En général, HP

Clé de registre	Description
	vous recommande de définir cette valeur sur `Bring to this computer` et de ne pas rediriger les périphériques de lecture USB vers l'hôte distant. Ce paramétrage permet d'améliorer la qualité audio et de veiller à ce que le son du client redirigé par d'autres canaux virtuels (par exemple, la `Multimedia Redirection`) corresponde aux paramètres audio locaux.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutError`	Définit le nombre de millisecondes à attendre après une perte de connexion avant que toute tentative de reconnexion avec le serveur soit abandonnée. Si la valeur est définie sur 0, le nombre de tentatives de reconnexion est illimité.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutRecovery`	Définit le nombre de millisecondes à attendre après une perte de connexion pour que le réseau soit restauré sans effectuer de tentative de reconnexion forcée.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutWarning`	Le nombre de millisecondes à attendre après une perte de connexion avant d'avertir l'utilisateur que la connexion a été perdue.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutWarningDialog`	Si la valeur est définie sur 1, lorsqu'une baisse de connexion de bout en bout est détectée, une boîte de dialogue s'affiche et l'écran passe en mode nuances de gris. Dans le cas contraire, des messages sont écrits dans le journal des connexions et la session se fige.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/timeoutsEnabled`	Si la valeur est définie sur 1, des vérifications sont effectuées au niveau de la connexion de bout en bout.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/tlsVersion`	Définit la version TLS (Transport Layer Security) à utiliser au cours des étapes initiales de négociation avec le serveur RDP. Définissez cette option sur la version TLS utilisée par votre serveur RDP ou essayez de la régler sur auto. **REMARQUE :** Il existe certains défauts côté serveur sur des serveurs RDP auxquels les correctifs n'ont pas été appliqués, susceptibles de provoquer l'échec de la valeur auto, c'est pourquoi il ne s'agit pas de la valeur par défaut.
`root/ConnectionType/view/connections/<UUID>/xfreerdpOptions/xkbLayoutId`	Définit un identifiant de disposition XKB pour contourner le clavier du système. Pour accéder à la liste des identifiants disponibles, saisissez la commande suivante dans un terminal X : `xfreerdp --kbd-list`.
`root/ConnectionType/view/coreSettings/USBrelevant`	Indique si ce type de connexion est conforme à l'USB. Si c'est le cas, il peut y avoir une connexion de USB pour rediriger les périphériques USB.
`root/ConnectionType/view/coreSettings/appName`	Définit le nom de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/view/coreSettings/className`	Définit la classe de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/view/coreSettings/editor`	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de connexion s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/view/coreSettings/icon`	Spécifie l'icône à partir du thème d'icône défini à utiliser pour cette connexion.
`root/ConnectionType/view/coreSettings/icon16Path`	Définit le chemin d'accès à l'icône 16 x 16 pixels représentant cette application.

Clé de registre	Description
`root/ConnectionType/view/coreSettings/icon32Path`	Définit le chemin d'accès à l'icône 32 x 32 pixels représentant cette application.
`root/ConnectionType/view/coreSettings/icon48Path`	Définit le chemin d'accès à l'icône 48 x 48 pixels représentant cette application.
`root/ConnectionType/view/coreSettings/iconActive`	Réservé à une utilisation ultérieure.
`root/ConnectionType/view/coreSettings/label`	Définit le nom à afficher pour ce type de connexion dans l'interface utilisateur.
`root/ConnectionType/view/coreSettings/priorityInConnectionLists`	Définit la priorité de ce type de connexion lorsqu'elle s'affiche dans le gestionnaire de connexion et dans l'assistant de configuration qui s'affiche pendant l'installation initiale. Une valeur supérieure déplacera ce type de connexion vers le haut de la liste. Si la clé est définie sur 0, ce type de connexion est masqué pour l'assistant de configuration et figure en dernière place dans le gestionnaire de connexion. Les types de connexions avec la même priorité sont répertoriés dans l'ordre alphabétique.
`root/ConnectionType/view/coreSettings/serverRequired`	Définit si un nom ou une adresse de serveur est `unused`, `optional` ou `required` pour ce type de connexion.
`root/ConnectionType/view/coreSettings/stopProcess`	Définit le comportement attendu lorsque la commande `connexion-mgr stop` est appelée sur cette connexion. Par défaut, il s'agit de `close`, qui provoque l'envoi d'un signal « kill » standard au processus. Si la valeur est définie sur `kill`, le processus spécifié par `appName` est tué de force. Si la valeur est définie sur `custom`, un script d'exécution personnalisé spécifié par `wrapperScript` sera exécuté avec l'argument `stop` pour mettre fin au processus normalement.
`root/ConnectionType/view/coreSettings/tier`	Indique l'importance relative de ce type de connexion et l'ordre dans lequel elle est répertoriée dans le menu Créer.
`root/ConnectionType/view/coreSettings/watchPid`	Si la valeur est définie sur 1, la connexion est contrôlée sous le nom spécifié par `appName`. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/view/coreSettings/wrapperScript`	Définit le nom du script ou du fichier binaire à exécuter au lancement de ce type de connexion. Il s'agit du script principal gérant tous les paramètres de connexion et les arguments de ligne de commande de la connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/view/coreSettings/wrapperScriptGeneration`	Indique au gestionnaire de connexion quel type de paramètres transmettre au script de la passerelle.
`root/ConnectionType/view/general/enableComPortRedirection`	
`root/ConnectionType/view/general/rdpOptions`	Les options spécifiées ici seront transmises directement au client RDP si RDP est utilisé en tant que protocole d'affichage par la connexion VMware Horizon View. Pour accéder à la liste complète des options, saisissez la commande suivante dans un terminal X : `rdesktop --aide`.
`root/ConnectionType/view/gui/viewManager/name`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/view/gui/viewManager/status`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.

Clé de registre	Description
root/ConnectionType/view/gui/viewManager/title	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/view/gui/viewManager/widgets/autostart	Contrôle l'état du widget **Priorité du démarrage automatique** dans le gestionnaire de connexion VMware Horizon View. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.
root/ConnectionType/view/gui/viewManager/widgets/fallBackConnection	Contrôle l'état du widget **Connexion de repli** dans le gestionnaire de connexion VMware Horizon View. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.
root/ConnectionType/view/gui/viewManager/widgets/label	Contrôle l'état du widget **Nom** dans le gestionnaire de connexion VMware Horizon View. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.

xdmcp

Clé de registre	Description
root/ConnectionType/xdmcp/authorizations/user/add	Si la clé est définie sur 1, un utilisateur final est autorisé à ajouter une nouvelle connexion de ce type à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/xdmcp/authorizations/user/general	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres généraux de ce type de connexion à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/xdmcp/connections/<UUID>/address	Définit le nom d'hôte ou l'adresse IP auquel se connecter.
root/ConnectionType/xdmcp/connections/<UUID>/afterStartedCommand	Permet de régler la commande à exécuter après le démarrage de la connexion.
root/ConnectionType/xdmcp/connections/<UUID>/afterStoppedCommand	Permet de régler la commande à exécuter une fois que la connexion a été arrêtée.
root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/edit	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres de la connexion pour cette connexion.
root/ConnectionType/xdmcp/connections/<UUID>/authorizations/user/execution	Si la clé est définie sur 1, un utilisateur final est autorisé à exécuter cette connexion.
root/ConnectionType/xdmcp/connections/<UUID>/autoReconnect	Si la valeur est définie sur 1, la connexion redémarre lorsqu'elle est fermée ou déconnectée.
root/ConnectionType/xdmcp/connections/<UUID>/autostart	Si définie sur une valeur de 1 à 5, la connexion se lancera automatiquement après le démarrage du système, la valeur de 1 ayant la priorité la plus élevée.
root/ConnectionType/xdmcp/connections/<UUID>/beforeStartingCommand	Définit la commande à exécuter avant le démarrage de la connexion.

Clé de registre	Description
root/ConnectionType/xdmcp/connections/<UUID>/color	Définit la profondeur de couleur de l'affichage de la connexion.
root/ConnectionType/xdmcp/connections/<UUID>/connectionEndAction	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/xdmcp/connections/<UUID>/coord	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/xdmcp/connections/<UUID>/dependConnectionId	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/key	Définit le nom d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/xdmcp/connections/<UUID>/extraEnvValues/<UUID>/value	Définit la valeur d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/xdmcp/connections/<UUID>/fallBackConnection	Permet de régler la connexion de secours via son UUID.
root/ConnectionType/xdmcp/connections/<UUID>/fontServer	Définit l'adresse du serveur de polices à utiliser. La clé de registre `useFontServer` doit également être définie sur 1.
root/ConnectionType/xdmcp/connections/<UUID>/hasDesktopIcon	Si la valeur est définie sur 1, l'icône du Bureau pour cette connexion est activée. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/xdmcp/connections/<UUID>/iconPosition	Définit les coordonnées x,y d'une icône de bureau fixée. Si aucune valeur n'est spécifiée, l'icône est flottante.
root/ConnectionType/xdmcp/connections/<UUID>/isInMenu	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/xdmcp/connections/<UUID>/label	Définit le nom de connexion qui s'affiche dans l'interface utilisateur. Sur Smart Zero, ce paramètre est normalement défini sur `Default Connection` et ne s'affiche pas dans l'interface utilisateur.
root/ConnectionType/xdmcp/connections/<UUID>/loginfields/server	S'il est réglé sur 1, le champ **mot de passe** est affiché dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, la case est affichée puis désactivée. Si la valeur est réglée sur 0, la case est masquée. Si la valeur est définie sur 3, les paramètres du système sont utilisés.
root/ConnectionType/xdmcp/connections/<UUID>/refreshRate	Définit la fréquence de rafraîchissement de l'affichage de la connexion.
root/ConnectionType/xdmcp/connections/<UUID>/startMode	Si la valeur par défaut `focus` est définie et que la connexion a déjà démarré, la connexion est mise en avant. Sinon, une erreur est renvoyée indiquant que la connexion est déjà démarrée.
root/ConnectionType/xdmcp/connections/<UUID>/type	Définit le type de connexion XDMCP. Si vous définissez la valeur sur `chooser`, tous les hôtes disponibles sont répertoriés et l'utilisateur peut sélectionner celui à utiliser pour la connexion. Si vous définissez la valeur sur `query`, une requête XDMCP est envoyée directement à l'hôte spécifié. Si vous définissez la valeur sur `broadcast`, tous les hôtes disponibles sont répertoriés et le premier est connecté automatiquement.
root/ConnectionType/xdmcp/connections/<UUID>/useFontServer	Si la valeur est définie sur 1, le serveur de polices est activé. Si la valeur est définie sur 0, la police locale est utilisée.
root/ConnectionType/xdmcp/connections/<UUID>/waitForNetwork	Si la valeur est définie sur 1, la connexion n'est pas lancée tant que le réseau n'est pas disponible. Ce paramètre permet de s'assurer que, sur un réseau lent, la connexion ne se lance pas

Clé de registre	Description
	avant que le réseau soit disponible, ce qui pourrait entraîner un échec.
root/ConnectionType/xdmcp/connections/<UUID>/windowSize	Définit la taille de police de la connexion.
root/ConnectionType/xdmcp/coreSettings/USBrelevant	Spécifie si ce type de connexion est conforme à l'USB. Si c'est le cas, il peut y avoir une connexion de USB pour rediriger les périphériques USB.
root/ConnectionType/xdmcp/coreSettings/appName	Définit le nom de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/xdmcp/coreSettings/audio	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/xdmcp/coreSettings/className	Définit la classe de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/xdmcp/coreSettings/desktopButton	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/xdmcp/coreSettings/editor	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de connexion s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/xdmcp/coreSettings/generalSettingsEditor	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/xdmcp/coreSettings/icon	Spécifie l'icône à partir du thème d'icône défini à utiliser pour cette connexion.
root/ConnectionType/xdmcp/coreSettings/icon16Path	Définit le chemin d'accès à l'icône 16 x 16 pixels représentant cette application.
root/ConnectionType/xdmcp/coreSettings/icon32Path	Définit le chemin d'accès à l'icône 32 x 32 pixels représentant cette application.
root/ConnectionType/xdmcp/coreSettings/icon48Path	Définit le chemin d'accès à l'icône 48 x 48 pixels représentant cette application.
root/ConnectionType/xdmcp/coreSettings/iconActive	Réservé à une utilisation ultérieure.
root/ConnectionType/xdmcp/coreSettings/label	Définit le nom à afficher pour ce type de connexion dans l'interface utilisateur.
root/ConnectionType/xdmcp/coreSettings/priorityInConnectionLists	Définit la priorité de ce type de connexion lorsqu'elle s'affiche dans le gestionnaire de connexion et dans l'assistant de configuration qui s'affiche pendant l'installation initiale. Une valeur supérieure déplacera ce type de connexion vers le haut de la liste. Si la clé est définie sur 0, ce type de connexion est masqué pour l'assistant de configuration et figure en dernière place dans le gestionnaire de connexion. Les types de connexions avec la même priorité sont répertoriés dans l'ordre alphabétique.
root/ConnectionType/xdmcp/coreSettings/serverRequired	Définit si un nom ou une adresse de serveur est `unused`, `optional` ou `required` pour ce type de connexion.
root/ConnectionType/xdmcp/coreSettings/stopProcess	Définit le comportement attendu lorsque la commande `connexion-mgr stop` est appelée sur cette connexion. Par défaut, il s'agit de `close`, qui provoque l'envoi d'un signal « kill » standard au processus. Si la valeur est définie sur `kill`, le processus spécifié par `appName` est tué de force. Si la valeur est définie sur `custom`, un script d'exécution personnalisé spécifié

Clé de registre	Description
	par `wrapperScript` sera exécuté avec l'argument `stop` pour mettre fin au processus normalement.
`root/ConnectionType/xdmcp/coreSettings/tier`	Indique l'importance relative de ce type de connexion et l'ordre dans lequel elle est répertoriée dans le menu Créer.
`root/ConnectionType/xdmcp/coreSettings/watchPid`	Si la valeur est définie sur 1, la connexion est contrôlée sous le nom spécifié par `appName`. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/xdmcp/coreSettings/wrapperScript`	Définit le nom du script ou du fichier binaire à exécuter au lancement de ce type de connexion. Il s'agit du script principal gérant tous les paramètres de connexion et les arguments de ligne de commande de la connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/xdmcp/gui/XdmcpManager/name`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/xdmcp/gui/XdmcpManager/status`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/xdmcp/gui/XdmcpManager/title`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/address`	Contrôle l'état du widget **Adresse** dans le gestionnaire de connexion XDMCP. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autoReconnect`	Contrôle l'état du widget **Reconnexion automatique** dans le gestionnaire de connexion XDMCP. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/autostart`	Contrôle l'état du widget **Priorité du démarrage automatique** dans le gestionnaire de connexion XDMCP. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/color`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/fontServer`	Contrôle l'état du widget **Serveur de polices** dans le gestionnaire de connexion XDMCP. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/hasDesktopIcon`	Contrôle l'état du widget **Afficher l'icône sur le Bureau** dans le gestionnaire de connexion XDMCP. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/isInMenu`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.

Clé de registre	Description
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/label	Contrôle l'état du widget **Nom** dans le gestionnaire de connexion XDMCP. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/refreshRate	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/type	Contrôle l'état du widget **Type** dans le gestionnaire de connexion XDMCP. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/useFontServer	Contrôle l'état du widget **User font server** (Utiliser le serveur de polices) dans le gestionnaire de connexion XDMCP. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/waitForNetwork	Contrôle l'état du widget **Attendre le réseau avant connexion** dans le gestionnaire de connexion XDMCP. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur inactive, le widget est masqué. Si la clé est définie sur read-only, le widget est visible en lecture seule.
root/ConnectionType/xdmcp/gui/XdmcpManager/widgets/windowSize	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.

xen

Clé de registre	Description
root/ConnectionType/xen/authorizations/user/add	Si la clé est définie sur 1, un utilisateur final est autorisé à ajouter une nouvelle connexion de ce type à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/xen/authorizations/user/general	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres généraux de ce type de connexion à l'aide du gestionnaire de connexion. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/xen/connections/<UUID>/SingleSignOn	Si la clé est définie sur 1, la connexion partage les informations d'identification avec l'économiseur d'écran.
root/ConnectionType/xen/connections/<UUID>/address	Définit l'adresse de l'hôte distant auquel se connecter. Il s'agit généralement d'une URL de type http://server.domain.com.
root/ConnectionType/xen/connections/<UUID>/afterStartedCommand	Permet de régler la commande à exécuter après le démarrage de la connexion.
root/ConnectionType/xen/connections/<UUID>/afterStoppedCommand	Permet de régler la commande à exécuter une fois que la connexion a été arrêtée.
root/ConnectionType/xen/connections/<UUID>/allowSaveConnInfo	

Clé de registre	Description
root/ConnectionType/xen/connections/<UUID>/appInMenu	Si la valeur est définie sur 1, toutes les applications de cette connexion s'affichent dans le menu de la barre des tâches.
root/ConnectionType/xen/connections/<UUID>/appInWindowOrOnDesktop	Si défini sur 1 et que appOnDesktop est activé, toutes les applications pour la connexion sont affichées dans une fenêtre de broker. Si la valeur est définie sur 0, les applications pour cette connexion s'affichent directement sur le bureau.
root/ConnectionType/xen/connections/<UUID>/appOnDashboard	Si la valeur est définie sur 1, toutes les applications de cette connexion s'affichent dans la barre des tâches.
root/ConnectionType/xen/connections/<UUID>/appOnDesktop	Si la valeur est définie sur 1, toutes les applications de cette connexion s'affichent sur le bureau.
root/ConnectionType/xen/connections/<UUID>/authorizations/user/edit	Si la clé est définie sur 1, un utilisateur final est autorisé à modifier les paramètres de la connexion pour cette connexion.
root/ConnectionType/xen/connections/<UUID>/authorizations/user/execution	Si la clé est définie sur 1, un utilisateur final est autorisé à exécuter cette connexion.
root/ConnectionType/xen/connections/<UUID>/autoLaunchSingleApp	Si la valeur est définie sur 1, et si le serveur Citrix ne renvoie qu'une seule application publiée ou qu'un seul bureau publié, cette ressource est lancée automatiquement.
root/ConnectionType/xen/connections/<UUID>/autoReconnect	Si la valeur est définie sur 1, la connexion redémarre lorsqu'elle est fermée ou déconnectée.
root/ConnectionType/xen/connections/<UUID>/autoReconnectAppsOnLogin	Si la valeur est définie sur 1, le système essaie de reconnecter toute session Citrix active ou déconnectée dans l'écran d'ouverture de session initial.
root/ConnectionType/xen/connections/<UUID>/autoReconnectDelay	Définit le temps d'attente en secondes avant la reconnexion de la session. La valeur par défaut de 0 entraîne la reconnexion immédiate de la connexion. Ce paramètre ne prend effet que lorsque autoReconnect est définie sur 1.
root/ConnectionType/xen/connections/<UUID>/autoRefreshInterval	Contrôle la durée en secondes avant que des ressources ne soient effacées et actualisées à nouveau sur le serveur. Réglez-la sur -1 pour la désactiver. Il n'est normalement pas nécessaire de réactualiser fréquemment les ressources du serveur.
root/ConnectionType/xen/connections/<UUID>/autoStartDesktop	Si la valeur est définie sur 1 et si autoStartResource est vide, le premier bureau disponible lorsque la connexion est lancée est démarré automatiquement.
root/ConnectionType/xen/connections/<UUID>/autoStartResource	Définit le nom du bureau ou de l'application à démarrer automatiquement lorsque la connexion est lancée.
root/ConnectionType/xen/connections/<UUID>/autoStartWithGuessing	Si elle est définie sur 1, la connexion tente de lancer autoStartDesktop ou autoStartResource en premier. Si la connexion ne peut lancer aucune des deux avec succès, elle essaie de lancer une autre ressource en devinant.
root/ConnectionType/xen/connections/<UUID>/autostart	Si définie sur une valeur de 1 à 5, la connexion se lancera automatiquement après le démarrage du système, la valeur de 1 ayant la priorité la plus élevée.
root/ConnectionType/xen/connections/<UUID>/autostartDelay	Réservé à une utilisation ultérieure.
root/ConnectionType/xen/connections/<UUID>/beforeStartingCommand	Définit la commande à exécuter avant le démarrage de la connexion.
root/ConnectionType/xen/connections/<UUID>/connectionMode	Définit le mode de connexion Citrix pour la connexion :

Clé de registre	Description
root/ConnectionType/xen/connections/<UUID>/connectionStopAction	Définit l'action à effectuer lorsque la connexion est terminée à partir de Connection Manager. Les options disponibles sont disconnect et logoff.
root/ConnectionType/xen/connections/<UUID>/continueWithNewPassword	Si elle est définie sur 1, après avoir réinitialisé le mot de passe, la connexion continue de se lancer à l'aide du nouveau mot de passe. Si elle est définie sur 0, après la réinitialisation du mot de passe, la connexion actuelle se ferme.
root/ConnectionType/xen/connections/<UUID>/coord	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/xen/connections/<UUID</credentialsType	Spécifie le type d'informations d'authentification parmi anonymous (accès non-authentifié), sso (authentification unique), startup (les informations d'authentification sont demandées au démarrage), password (utilisateur/domaine/mot de passe préconfiguré) ou smartcard (carte à puce).
root/ConnectionType/xen/connections/<UUID>/dependConnectionId	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/ConnectionType/xen/connections/<UUID>/domain	Définit le domaine à fournir au serveur XenDesktop. Si aucun domaine n'est spécifié, le domaine par défaut du serveur est utilisé.
root/ConnectionType/xen/connections/<UUID>/enableRSAToken	**ATTENTION :** Cette fonctionnalité n'est pas prise en charge. Si la valeur est définie sur 1, l'utilisateur sera invité avant de se connecter à indiquer une valeur de jeton de sécurité à utiliser lors de l'authentification avec NetScaler Gateway.
root/ConnectionType/xen/connections/<UUID>/extraEnvValues/<UUID>/key	Définit le nom d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/xen/connections/<UUID>/extraEnvValues/<UUID>/value	Définit la valeur d'une variable d'environnement supplémentaire à utiliser avec la connexion.
root/ConnectionType/xen/connections/<UUID>/fallBackConnection	Permet de régler la connexion de secours via son UUID.
root/ConnectionType/xen/connections/<UUID>/folder	
root/ConnectionType/xen/connections/<UUID>/forceHttps	Si la valeur est définie sur 1, seules les connexions HTTPS sont autorisées.
root/ConnectionType/xen/connections/<UUID>/fullscreen	Si la valeur est définie sur 1, le client Citrix se lance en mode plein écran lors du démarrage.
root/ConnectionType/xen/connections/<UUID>/hasDesktopIcon	Si la valeur est définie sur 1, l'icône du Bureau pour cette connexion est activée. Cette clé n'a aucun effet sur Smart Zero.
root/ConnectionType/xen/connections/<UUID>/iconPosition	Définit les coordonnées x,y d'une icône de bureau fixée. Si aucune valeur n'est spécifiée, l'icône est flottante.
root/ConnectionType/xen/connections/<UUID>/ignoreCertCheck	Si la valeur est définie sur 1, la vérification des certificats est ignorée pour la connexion.
root/ConnectionType/xen/connections/<UUID>/label	Définit le nom de connexion qui s'affiche dans l'interface utilisateur. Sur Smart Zero, ce paramètre est normalement défini sur Default Connection et ne s'affiche pas dans l'interface utilisateur.
root/ConnectionType/xen/connections/<UUID>/logOnMethod	

Clé de registre	Description
`root/ConnectionType/xen/connections/<UUID>/loginfields/domain`	Si la valeur est définie sur 1, le champ **Domaine** est affiché dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, le champ est affiché puis désactivé. Si la valeur est définie sur 0, le champ est masqué.
`root/ConnectionType/xen/connections/<UUID>/loginfields/password`	Si la valeur est définie sur 1, le champ **Mot de passe** est affiché dans la boîte de dialogue ouverture de session pour la connexion. Si la valeur est définie sur 2, le champ est affiché puis désactivé. Si la valeur est définie sur 0, le champ est masqué.
`root/ConnectionType/xen/connections/<UUID>/loginfields/rememberme`	Lorsqu'elle est définie sur 1, la case **Se souvenir de moi** figure dans la boîte de dialogue d'ouverture de session pour la connexion. Lorsqu'elle est définie sur 2, la case est affichée mais désactivée. Lorsqu'elle est définie sur 0, la case est masquée.
`root/ConnectionType/xen/connections/<UUID>/loginfields/server`	S'il est réglé sur 1, le champ **mot de passe** est affiché dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, la case est affichée puis désactivée. Si la valeur est réglée sur 0, la case est masquée. Si la valeur est définie sur 3, les paramètres du système sont utilisés.
`root/ConnectionType/xen/connections/<UUID>/loginfields/showpassword`	Si la valeur est réglée à 1, le bouton **Show password** (Afficher le mot de passe) apparaît dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est réglée sur 2, le bouton est affiché mais désactivé. Si la valeur est réglée sur 0, le bouton est masqué.
`root/ConnectionType/xen/connections/<UUID>/loginfields/smartcard`	Lorsqu'elle est définie sur 1, la case **Connexion carte à puce** figure dans la boîte de dialogue d'ouverture de session pour la connexion. Lorsqu'elle est définie sur 2, la case est affichée mais désactivée. Lorsqu'elle est définie sur 0, la case est masquée. Cette case peut ne pas figurer si aucune carte à puce n'est détectée, même si cette option est activée.
`root/ConnectionType/xen/connections/<UUID>/loginfields/username`	Si la valeur est définie sur 1, le champ **Nom d'utilisateur** apparaît dans la boîte de dialogue d'ouverture de session pour la connexion. Si la valeur est définie sur 2, le champ est affiché puis désactivé. Si la valeur est définie sur 0, le champ est masqué.
`root/ConnectionType/xen/connections/<UUID>/password`	Définit le mot de passe par défaut à fournir à l'hôte distant lors de l'ouverture de session. Cette valeur est cryptée. En général, ce paramètre est utilisé avec les applications de style kiosque dans lesquelles un mot de passe générique est utilisé pour l'ouverture de session.
`root/ConnectionType/xen/connections/<UUID>/resListRequest`	Si la clé est définie sur 1, une seule connexion affiche la liste des ressources sans les lancer ni télécharger les icônes.
`root/ConnectionType/xen/connections/<UUID>/saveNewUrl`	Il s'agit d'une valeur interne. Si la clé est définie sur `ToBeAsked`, le script interroge l'utilisateur. Si la clé est définie sur `Auto`, le script n'interroge pas l'utilisateur et l'enregistrement de l'URL dépend du cas. Si la clé est définie sur `Yes` (Oui), l'utilisateur a demandé l'enregistrement de la nouvelle URL. Si la clé est définie sur `No` (Non), l'utilisateur a demandé à ne pas enregistrer la nouvelle URL.
`root/ConnectionType/xen/connections/<UUID>/savePassword`	
`root/ConnectionType/xen/connections/<UUID>/smartCardModuleKey`	Spécifie le module de sécurité à utiliser pour une connexion de la carte Smart Card.

Clé de registre	Description
root/ConnectionType/xen/connections/<UUID>/startMode	Si la valeur par défaut focus est définie et que la connexion a déjà démarré, la connexion est mise en avant. Sinon, une erreur est renvoyée indiquant que la connexion est déjà démarrée.
root/ConnectionType/xen/connections/<UUID>/subscribedOnly	Si la clé est définie sur 1, les ressources auxquelles les utilisateurs se sont abonnés pour la connexion sont affichées.
root/ConnectionType/xen/connections/<UUID>/unplugSmartCardAction	Définit l'action à effectuer lorsqu'une carte Smart Card est débranchée au cours d'une connexion. disconnect provoquera une déconnexion de la session en cours. close fermera toutes les ressources ouvertes. noaction ne provoquera aucune action.
root/ConnectionType/xen/connections/<UUID>/useCurrentCitrixConfig	
root/ConnectionType/xen/connections/<UUID>/username	Définit le nom d'utilisateur par défaut à fournir à l'hôte distant lors de l'ouverture de session. En général, ce paramètre est utilisé avec les applications de style kiosque dans lesquelles un nom d'utilisateur générique est utilisé pour l'ouverture de session.
root/ConnectionType/xen/connections/<UUID>/waitForNetwork	Si la valeur est définie sur 1, la connexion n'est pas lancée tant que le réseau n'est pas disponible. Ce paramètre permet de s'assurer que, sur un réseau lent, la connexion ne se lance pas avant que le réseau soit disponible, ce qui pourrait entraîner un échec.
root/ConnectionType/xen/coreSettings/USBrelevant	Spécifie si ce type de connexion est conforme à l'USB. Si c'est le cas, il peut y avoir une connexion USB pour rediriger les périphériques USB.
root/ConnectionType/xen/coreSettings/appName	Définit le nom de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/xen/coreSettings/autoLogoutDelayAfterLaunch	Ce paramètre s'applique aux serveurs Citrix avec plusieurs ressources publiées. Si la valeur définie est inférieure à 0, aucune fermeture de session automatique n'est effectuée. Dans le cas contraire, ce paramètre indique le délai en secondes entre la fermeture de la dernière ressource publiée Xen et la fermeture de session automatique de l'utilisateur et l'affichage de l'écran d'ouverture de session initial. Les délais de traitement de Citrix peuvent augmenter le temps de fermeture de session automatique.
root/ConnectionType/xen/coreSettings/autoLogoutDelayBeforeLaunch	Ce paramètre s'applique aux serveurs Citrix avec plusieurs ressources publiées. Si la valeur définie est inférieure à 0, aucune fermeture de session automatique n'est effectuée. Dans le cas contraire, ce paramètre indique le délai en secondes avant que l'utilisateur soit déconnecté automatiquement et retourne à l'écran de connexion initial si aucune application n'est lancée. Les délais de traitement de Citrix peuvent augmenter le temps de fermeture de session automatique.
root/ConnectionType/xen/coreSettings/className	Définit la classe de l'application interne à utiliser pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ConnectionType/xen/coreSettings/connectionUtil	Définit l'utilitaire de connexion Citrix pour la connexion.
root/ConnectionType/xen/coreSettings/credsCache	Indique si le gestionnaire de connexion met en cache les informations d'identification pour une utilisation ultérieure.

Clé de registre	Description
`root/ConnectionType/xen/coreSettings/editor`	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de connexion s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/xen/coreSettings/generalSettingsEditor`	Définit le nom de l'application interne à utiliser lorsque le gestionnaire de paramètres généraux s'exécute pour ce type de connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/xen/coreSettings/icon`	Spécifie l'icône à partir du thème d'icône défini à utiliser pour cette connexion.
`root/ConnectionType/xen/coreSettings/icon16Path`	Définit le chemin d'accès à l'icône 16 x 16 pixels représentant cette application.
`root/ConnectionType/xen/coreSettings/icon32Path`	Définit le chemin d'accès à l'icône 32 x 32 pixels représentant cette application.
`root/ConnectionType/xen/coreSettings/icon48Path`	Définit le chemin d'accès à l'icône 48 x 48 pixels représentant cette application.
`root/ConnectionType/xen/coreSettings/iconActive`	Réservé à une utilisation ultérieure.
`root/ConnectionType/xen/coreSettings/label`	Définit le nom à afficher pour ce type de connexion dans l'interface utilisateur.
`root/ConnectionType/xen/coreSettings/priorityInConnectionLists`	Définit la priorité de ce type de connexion lorsqu'elle s'affiche dans le gestionnaire de connexion et dans l'assistant de configuration qui s'affiche pendant l'installation initiale. Une valeur supérieure déplacera ce type de connexion vers le haut de la liste. Si la clé est définie sur 0, ce type de connexion est masqué pour l'assistant de configuration et figure en dernière place dans le gestionnaire de connexion. Les types de connexions avec la même priorité sont répertoriés dans l'ordre alphabétique.
`root/ConnectionType/xen/coreSettings/retryTimeout`	Ce paramètre s'applique lorsqu'une machine virtuelle redémarre et n'est pas encore disponible pour le lancement en tant que ressource Citrix. Si la valeur est définie sur un nombre négatif, aucune reconnexion n'est tentée. Dans le cas contraire, du temps est laissé (en secondes) pour que HP ThinPro essaie de se reconnecter à la machine virtuelle.
`root/ConnectionType/xen/coreSettings/serverRequired`	Définit si un nom ou une adresse de serveur est `unused`, `optional` ou `required` pour ce type de connexion.
`root/ConnectionType/xen/coreSettings/stopProcess`	Définit le comportement attendu lorsque la commande `connexion-mgr stop` est appelée sur cette connexion. Par défaut, il s'agit de `close`, qui provoque l'envoi d'un signal « kill » standard au processus. Si la valeur est définie sur `kill`, le processus spécifié par `appName` est tué de force. Si la valeur est définie sur `custom`, un script d'exécution personnalisé spécifié par `wrapperScript` sera exécuté avec l'argument `stop` pour mettre fin au processus normalement.
`root/ConnectionType/xen/coreSettings/tier`	Indique l'importance relative de ce type de connexion et l'ordre dans lequel elle est répertoriée dans le menu Créer.
`root/ConnectionType/xen/coreSettings/watchPid`	Si la valeur est définie sur 1, la connexion est contrôlée sous le nom spécifié par `appName`. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/xen/coreSettings/wrapperScript`	Définit le nom du script ou du fichier binaire à exécuter au lancement de ce type de connexion. Il s'agit du script principal gérant tous les paramètres de connexion et les arguments de

Clé de registre	Description
	ligne de commande de la connexion. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/ConnectionType/xen/coreSettings/wrapperScriptGeneration`	Indique au gestionnaire de connexion quel type de paramètres transmettre au script de la passerelle.
`root/ConnectionType/xen/general/CGPAddress`	Spécifie l'adresse CGP en utilisant la syntaxe `nom d'hôte:port`. Facultativement, vous pouvez taper un astérisque (*) au lieu de spécifier le nom d'hôte. Dans ce cas, la valeur de la clé de registre `d'adresse` de la connexion est utilisée comme hôte. Par exemple : `* : 2598` La valeur du port est facultative. Si vous ne spécifiez pas de valeur de port, la valeur par défaut 2598 est utilisée. Lorsqu'une connexion au port 2598, le client léger tente d'établir une connexion sur le port 1494.
`root/ConnectionType/xen/general/TWIMode`	Contrôle le mode transparent pour les applications publiées. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix `TWIMode`.
`root/ConnectionType/xen/general/TWIModeResizeType`	Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix `TWIMoveResizeType`.
`root/ConnectionType/xen/general/allowReadOnA ... allowReadOnZ`	Si la valeur est définie sur 1, un utilisateur peut lire l'unité mappée.
`root/ConnectionType/xen/general/allowWriteOnA ... allowWriteOnZ`	Si la valeur est définie sur 1, un utilisateur peut écrire sur l'unité mappée.
`root/ConnectionType/xen/general/async`	Si la valeur est définie sur 1, l'interrogation asynchrone est activée. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix `CommPollSize`.
`root/ConnectionType/xen/general/autoReconnect`	Si la valeur est définie sur 1, la reconnexion automatique à la session est activée. Il ne s'agit pas du même paramètre que le paramètre « Reconnexion automatique » de la connexion. Cette reconnexion se produit en interne au sein du client Citrix sans redémarrage de la connexion. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix `TransportReconnectEnabled`.
`root/ConnectionType/xen/general/bitmapCacheSize`	Définit la taille minimale pour la mise en cache des bitmaps. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix `PersistentCacheMinBitmap`.
`root/ConnectionType/xen/general/bottomMonitor`	Permet de régler la zone de l'écran du moniteur inférieur pour afficher le bureau virtuel. En cas de réglage à 0, l'écran n'est pas utilisé pour afficher le bureau virtuel.
`root/ConnectionType/xen/general/colorDepth`	Force à utiliser une profondeur de couleur spécifique pour toutes les connexions. Cette opération est généralement effectuée dans des environnements spécialisés où la sélection automatique de profondeur échoue ou sur des réseaux très lents afin de réduire la congestion.
`root/ConnectionType/xen/general/colorMapping`	Si la valeur est définie sur `Shared - Approximate Colors`, les couleurs approximatives de la palette par défaut sont utilisées. Si la valeur est définie sur `Private - Exact Colors`, les couleurs exactes sont utilisées. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix `ApproximateColors`.

Clé de registre	Description
`root/ConnectionType/xen/general/contentRedirection`	Si la valeur est définie sur 1, des liens de contenu web sont envoyés par le serveur au client afin que le client puisse tenter de les ouvrir localement.
`root/ConnectionType/xen/general/debugLogLevel`	Si la valeur est définie sur 0, aucun journal de débogage n'est crée. Si la valeur est définie sur 3, un journal de niveau d'erreur est créé. Si la valeur est définie sur 4, un journal de niveau d'avertissement est créé. Si la valeur est définie sur 7, tous les journaux de niveau de débogage sont créés.
`root/ConnectionType/xen/general/defaultBrowserProtocol`	Contrôle le protocole utilisé pour localiser l'hôte pour la connexion. Si elle n'est pas spécifiée, la valeur par défaut de la section `[WFClient]` du fichier wfclient.ini est utilisée. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix `BrowserProtocol`.
`root/ConnectionType/xen/general/drivePathMappedOnA ... drivePathMappedOnZ`	Définit le répertoire de système de fichiers local à mapper sur l'hôte distant. En général, il est défini sur `/media` pour permettre à toutes les unités USB connectées d'être mappés sur l'hôte distant via une seule lettre d'unité.
`root/ConnectionType/xen/general/enableAlertSound`	Si la valeur est définie sur 1, les alertes sonores de Windows sont activées. Ce paramètre est indirectement mappé sur le paramètre de fichier .ini Citrix `DisableSound`.
`root/ConnectionType/xen/general/enableClipboard`	Si la valeur est définie sur 1, la redirection du presse-papiers est activée.
`root/ConnectionType/xen/general/enableConnectionBar`	Si la valeur est définie sur 1, Citrix Desktop Viewer est activée dans l'interface utilisateur de la session. Par défaut, ce paramètre est défini sur 0 (désactivé) côté client car cette valeur est définie sur le client par le fichier ICA pour une session de bureau.
`root/ConnectionType/xen/general/enableCursorColors`	Si la valeur est définie sur 1, les curseurs de couleur sont activés. Définir ce paramètre sur 0 est susceptible de corriger certaines corruptions graphiques du curseur.
`root/ConnectionType/xen/general/enableDataCompression`	Si la valeur est définie sur 1, la compression des données est activée. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix `Compress`.
`root/ConnectionType/xen/general/enableDriveMapAndRedirect`	Si la valeur est définie sur 1, le mappage et la redirection des périphériques de stockage USB sont activés.
`root/ConnectionType/xen/general/enableDriveMapping`	Si la valeur est définie sur 1, les répertoires du système de fichiers local peuvent être transmis vers l'hôte distant via une unité virtuelle. En général, `/media` est mappé sur `Z` pour permettre aux unités USB d'être transmises à l'hôte distant. Si la redirection USB est activée, ce paramètre doit être désactivé pour éviter les conflits de stockage. Pour être mappés correctement sur l'hôte distant de cette manière, l'unité USB doit utiliser l'un des systèmes de fichiers suivants : FAT32, NTFS, ext2, ext3.
`root/ConnectionType/xen/general/enableDynamicDriveMapping`	Si la valeur est définie sur 1, les périphériques de stockage USB seront mappés dynamiquement sur le serveur Citrix. Si la valeur est définie sur 0, le mappage dynamique des périphériques de stockage USB est désactivé.
`root/ConnectionType/xen/general/enableH264Compression`	Si la valeur est définie sur 1, la compression H.264 est activée. Les réseaux WAN bénéficient de meilleures performances sur leurs applications graphiques riches et professionnelles avec le codec H.264, qu'avec le codec JPEG.

Clé de registre	Description
root/ConnectionType/xen/general/enableHDXFlashRedirection	**REMARQUE :** Cette fonction est uniquement prise en charge pour la version 32 bits de HP ThinPro. Contrôle le comportement de la Redirection de HDX Flash. Si le paramètre est défini sur `Always`, la Redirection de HDX Flash est utilisée si possible et l'utilisateur ne reçoit aucune invite. Si le paramètre est défini sur `Ask`, l'utilisateur reçoit une invite. Si la valeur est définie sur `Never`, la fonction est désactivée.
root/ConnectionType/xen/general/enableHDXFlashServerContentFetch	**REMARQUE :** Cette fonction est uniquement prise en charge pour la version 32 bits de HP ThinPro. Contrôle le comportement du Rapport de contenu du serveur HDX Flash. Si désactivé, le client devra récupérer le contenu.
root/ConnectionType/xen/general/enableHDXMediaStream	Si la clé est définie sur 1, HDX MediaStream est activé. Si la clé est définie sur 0, les fichiers multimédias continuent d'être lus en streaming standard, mais la qualité peut être affectée.
root/ConnectionType/xen/general/enableHWH264	Si défini sur 1, et si `enableH264Compression` est aussi définie sur 1, la compression de matériel pour les H.264 est activée. En cas de réglage sur 0, la compression des H.264 sera gérée par le logiciel.
root/ConnectionType/xen/general/enableMapOnA ... enableMapOnZ	Si la valeur est définie sur 1, un répertoire système fichiers local peut être mappé sur cette unité sur l'hôte distant. La clé de registre `drivePathMappedOn` correspondante doit être définie sur un répertoire local valide pour que le mappage des unités fonctionne correctement.
root/ConnectionType/xen/general/enableMultiMedia	Si la valeur est définie sur 1, le multimédia est activé. HDX Lync risque de faire l'objet d'un conflit si ce paramètre est activé. Ce paramètre correspond directement au multimédia dans la section des canaux virtuels des paramètres du fichier .ini de Citrix. Activez ce paramètre lorsque HDX MediaStream est activé.
root/ConnectionType/xen/general/enableOffScreenSurface	Si la valeur est définie sur 1, le serveur peut utiliser le format `X PixMap` pour le dessin hors écran. Ce paramétrage permet de réduire la bande passante en mode couleurs 15 et 24 bits au détriment de la mémoire et du temps processeur du serveur X. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix `EnableOSS`.
root/ConnectionType/xen/general/enableRC4128SHA	
root/ConnectionType/xen/general/enableRC4MD5	
root/ConnectionType/xen/general/enableSessionReliability	Si la valeur est définie sur 1, la Fiabilité de Session Citrix est activée. La Session fiabilité change la manière dont les sessions reprennent après une perte de connexion réseau. Reportez-vous à la documentation Citrix pour plus d'informations sur la fiabilité de la Session.
root/ConnectionType/xen/general/enableSmallFrames	Si la valeur est définie sur 1, de petites mises à jour rectangulaires H.264 sont activées pour H.264. `enableTextTracking` doit également être activé pour que cela se produise.
root/ConnectionType/xen/general/enableSmartCard	Si la valeur est définie sur 1, la connexion carte Smart Card est activée.
root/ConnectionType/xen/general/enableTLSRSA	
root/ConnectionType/xen/general/enableTextTracking	Si la valeur est définie sur 1, des recouvrements de texte sans perte optimisés sont activés pour les H.264.

Clé de registre	Description
root/ConnectionType/xen/general/enableUSBRedirection	Si défini sur 1, les périphériques de stockage USB seront redirigés.
root/ConnectionType/xen/general/encryptionLevel	Définit le niveau de cryptage. Les protocoles de cryptage de tous les niveaux sont définis dans la section [EncryptionLevelSession] du fichier module.ini. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix [EncryptionLevelSession].
root/ConnectionType/xen/general/fontSmoothingType	Définit le type de lissage de police.
root/ConnectionType/xen/general/hotKey<1thru15>Char	Définit le raccourci clavier à transmettre à la session à distance lorsque la touche ou la combinaison de touches définies dans le hotKeyShift correspondant est pressée.
root/ConnectionType/xen/general/hotKey<1thru15>Shift	Définit la touche ou la combinaison de touches utilisées pour activer le raccourci clavier dans le hotKeyChar correspondant.
root/ConnectionType/xen/general/httpAddresses/<UUID>/address	
root/ConnectionType/xen/general/keyPassthroughEscapeChar	Définit la touche du clavier pour la désactivation du mode « clavier transparent ». Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix KeyPassthroughEscapeChar.
root/ConnectionType/xen/general/keyPassthroughEscapeShift	Définit la combinaison de touches du clavier pour la désactivation du mode « clavier transparent ». Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix KeyPassthroughEscapeShift.
root/ConnectionType/xen/general/keyboardMappingFile	Spécifie un fichier de configuration du clavier pour une session Citrix. Par défaut, le script de démarrage sélectionne un fichier de configuration du clavier en fonction de la disposition du clavier.
root/ConnectionType/xen/general/lastComPortNum	Définit le nombre de ports série mappés. Si la valeur est définie sur 0, le mappage de port série est désactivé.
root/ConnectionType/xen/general/leftMonitor	Permet de régler la zone de l'écran du moniteur gauche pour afficher le bureau virtuel. En cas de réglage à 0, l'écran n'est pas utilisé pour afficher le bureau virtuel.
root/ConnectionType/xen/general/localTextEcho	Contrôle la réduction de la latence du clavier. Ce paramètre est indirectement mappé sur le paramètre de fichier .ini Citrix ZLKeyboardMode.
root/ConnectionType/xen/general/monitorNetwork	Si défini sur Off, la connectivité réseau n'est pas contrôlée. Si définit sur Local network link status only, seul le statut du lien réseau local est contrôlé. Si définit sur Server online status, le statut du lien réseau local et la connectivité réseaux sont tous deux contrôlés.
root/ConnectionType/xen/general/mouseClickFeedback	Contrôle la réduction de la latence de la souris. Ce paramètre est indirectement mappé sur le paramètre de fichier .ini Citrix ZLMouseMode.
root/ConnectionType/xen/general/mouseMiddleButtonPaste	Si la valeur est définie sur 1, l'émulation de l'opération de collage à l'aide du bouton central de la souris est activée pour les sessions de Windows. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix MouseSendsControlV.
root/ConnectionType/xen/general/noInfoBox	Si la valeur est définie sur 1, le gestionnaire de client (wfcmgr) ne s'affiche pas lorsqu'une session du client est interrompue. Ce

Clé de registre	Description
	paramètre est directement mappé sur le paramètre de fichier .ini Citrix `PopupOnExit`.
`root/ConnectionType/xen/general/printerAutoCreation`	Si la clé est définie sur 0, le mappage imprimantes est désactivé. Si la clé est définie sur 1, les imprimantes définies localement sont mappées sur la connexion. Si la clé est définie sur 2, les imprimantes USB sont redirigées selon la configuration définie dans le gestionnaire USB.
`root/ConnectionType/xen/general/proxyAddress`	Définit l'adresse du proxy à utiliser si un paramètre de proxy manuel est sélectionné par le biais de `proxyType`.
`root/ConnectionType/xen/general/proxyPassword`	Définit le mot de passe proxy à utiliser si un paramètre de proxy manuel est sélectionné par le biais de `proxyType`. Ce mot de passe est crypté à l'aide d'un cryptage rc4.
`root/ConnectionType/xen/general/proxyPort`	Définit le port proxy à utiliser si un paramètre de proxy manuel est sélectionné par le biais de `proxyType`.
`root/ConnectionType/xen/general/proxyType`	Définit le type de proxy à utiliser pour les connexions XenDesktop. La valeur `Use Browser settings` est uniquement prise en charge si un navigateur local est installé.
`root/ConnectionType/xen/general/proxyUser`	Définit le nom d'utilisateur proxy à utiliser si un paramètre de proxy manuel est sélectionné par le biais de `proxyType`.
`root/ConnectionType/xen/general/rightMonitor`	Permet de régler la zone de l'écran du moniteur droit pour afficher le bureau virtuel. En cas de réglage à 0, l'écran n'est pas utilisé pour afficher le bureau virtuel.
`root/ConnectionType/xen/general/saveLogs`	Si la valeur est définie sur 1, des informations détaillées du journal sont enregistrées une fois la session terminée. Ces informations de connexion seront enregistrées sur le répertoire suivant : `/tmp/debug/citrix/<date>/`
`root/ConnectionType/xen/general/selfservice/disableConfigMgr`	Si la valeur est définie sur 1, les demandes de partage de session sont envoyées aux autres sessions Citrix sur le même affichage X. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix `EnableSessionSharingClient`.
`root/ConnectionType/xen/general/selfservice/disableConnectionCenter`	
`root/ConnectionType/xen/general/selfservice/enableKioskMode`	
`root/ConnectionType/xen/general/selfservice/sharedUserMode`	
`root/ConnectionType/xen/general/selfservice/showTaskBarInKioskMode`	
`root/ConnectionType/xen/general/serverCheckTimeout`	
`root/ConnectionType/xen/general/sessionReliabilityTTL`	Spécifie le délai d'expiration de la fiabilité de session en secondes. Cette option configure la durée de vie (TTL) de la fiabilité de session.
`root/ConnectionType/xen/general/showOnAllMonitors`	Si défini sur 1, le bureau virtuel est affiché sur tous les écrans.
`root/ConnectionType/xen/general/smartCardModuleMap/CoolKeyPK11`	Spécifie le chemin d'accès pour le module de sécurité de carte Smart Card `CoolKey PKCS #11`.

Clé de registre	Description
root/ConnectionType/xen/general/smartCardModuleMap/GemaltoDotNet	Spécifie le chemin d'accès pour le module de sécurité de carte Smart Card Gemalto.NET.
root/ConnectionType/xen/general/sound	Définit la qualité audio. Ce paramètre est indirectement mappé sur le paramètre de fichier .ini Citrix AudioBandwidthLimit.
root/ConnectionType/xen/general/speedScreen	
root/ConnectionType/xen/general/tcpAccel	
root/ConnectionType/xen/general/tcpAddresses/<UUID>/address	
root/ConnectionType/xen/general/topMonitor	Permet de régler la zone de l'écran du moniteur supérieur pour afficher le bureau virtuel. En cas de réglage à 0, l'écran n'est pas utilisé pour afficher le bureau virtuel.
root/ConnectionType/xen/general/transparentKeyPassthrough	Contrôle la façon dont certaines combinaisons de touches Windows sont gérées. Si la valeur est définie sur Translated, les combinaisons de touches s'appliquent au bureau local. Si la valeur est définie sur Direct in full screen desktops only, les combinaisons de touches s'appliquent à la session à distance uniquement en mode plein écran. Si la valeur est définie sur Direct, les combinaisons de touches s'appliquent toujours à la session à distance tant que la fenêtre est active. Ce paramètre est indirectement mappé sur le paramètre de fichier .ini Citrix TransparentKeyPassthrough.
root/ConnectionType/xen/general/transportProtocol	Définit le protocole de transport. Si la valeur est définie sur On (valeur par défaut), la connexion utilise le protocole UDP et ne retombe pas en TCP en cas d'échec. Si la valeur est définie sur Off, la connexion utilise TCP. Si la valeur est définie sur Favori, la connexion tente d'utiliser UDP en premier et retombe en TCP en cas d'échec.
root/ConnectionType/xen/general/twRedundantImageItems	Contrôle le nombre de zones d'écran suivies par ThinWire afin d'éviter tout dessin redondant d'images bitmap. Une valeur adéquate pour les sessions 1024 x 768 est 300.
root/ConnectionType/xen/general/useAlternateAddress	Si la valeur est définie sur 1, une adresse alternative est utilisée pour les connexions de pare-feu. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix UseAlternateAddress.
root/ConnectionType/xen/general/useBitmapCache	Si la valeur est définie sur 1, le cache disque persistant est activé. Le cache disque persistant stocke des objets graphiques couramment utilisés comme les images bitmaps sur le disque dur du client léger. Utiliser le cache disque persistant augmente les performances sur les connexions à faible bande passante, mais réduit la quantité d'espace disque disponible pour le client léger. Pour les clients légers sur des réseaux locaux à haut débit, l'utilisation du cache de disque persistant n'est pas nécessaire. Ce paramètre est directement mappé sur le paramètre de fichier .ini Citrix PersistentCacheEnabled.
root/ConnectionType/xen/general/useEUKS	Contrôle l'utilisation d'EUKS (Extended Unicode Keyboard Support) sur les serveurs Windows. Si la valeur est définie sur 0, EUKS n'est pas utilisé. Si la valeur est définie sur 1, EUKS est utilisé en cas de secours. Si la valeur est définie sur 2, EUKS est utilisé autant que possible.
root/ConnectionType/xen/general/useLocalIM	Si ce paramètre est activé, la méthode d'entrée X locale est utilisée pour interpréter les entrées du clavier. Prise en charge uniquement pour les langues européennes. Ce paramètre est

Clé de registre	Description
	directement mappé sur le paramètre de fichier .ini Citrix `useLocalIME`.
`root/ConnectionType/xen/general/userAgent`	La chaîne de cette clé est présentée par le client Citrix et permet aux administrateurs de savoir d'où provient la demande de connexion.
`root/ConnectionType/xen/general/waitForNetwork`	Si la valeur est définie sur 1, la connexion n'est pas lancée tant que le réseau n'est pas disponible. Ce paramètre permet de s'assurer que, sur un réseau lent, la connexion ne se lance pas avant que le réseau soit disponible, ce qui pourrait entraîner un échec.
`root/ConnectionType/xen/general/webcamFramesPerSec`	Contrôle la variable `HDXWebCamFramesPerSec` dans le fichier All_Regions.ini.
`root/ConnectionType/xen/general/webcamHeight`	Contrôle la variable `HDXWebCamHeight` dans le fichier `All_Regions.ini`.
`root/ConnectionType/xen/general/webcamQuality`	Contrôle la variable `HDXWebCamQuality` dans le fichier `All_Regions.ini`. Les entrées valides sont comprises entre 1 et 63.
`root/ConnectionType/xen/general/webcamSupport`	Si la valeur est définie sur 0, la webcam et le son de la webcam sont désactivés. Si la valeur est définie sur 1, la webcam et le son de la webcam sont activés, avec compression. Si la valeur est définie sur 2, la redirection USB de la webcam et du son de la webcam est activée.
`root/ConnectionType/xen/general/webcamWidth`	Contrôle la variable `HDXWebCamWidth` dans le fichier `All_Regions.ini`.
`root/ConnectionType/xen/general/windowHeight`	Permet de régler la hauteur de la fenêtre en pixels si `windowSize` est défini sur `Fixed Size`.
`root/ConnectionType/xen/general/windowPercent`	Permet de régler la taille de la fenêtre en pourcentage si `windowSize` est défini sur le `Percentage of Screen Size`.
`root/ConnectionType/xen/general/windowSize`	Si la valeur est définie sur `Default`, les paramètres côté serveur sont utilisés. Si la valeur est définie sur `Full screen`, la fenêtre est agrandie sans bordure sur tous les écrans disponibles. Si la valeur est définie sur `Fixed Size`, les clés de registre `windowWidth` et `windowHeight` peuvent être utilisées pour spécifier la taille de la fenêtre en pixels. Si la valeur est définie sur `Percentage of Screen Size`, la clé `windowPercent` peut être utilisée pour spécifier la taille de la fenêtre en pourcentage. Pour que le paramètre `Percentage of Screen Size` prenne effet, `enableForceDirectConnect` doit être défini sur 1 et `TWIMode` doit être défini sur 0. Ce paramètre ne fonctionne qu'avec XenApp et uniquement si le serveur autorise les connexions directes. Ce paramètre ne fonctionne pas avec XenDesktop.
`root/ConnectionType/xen/general/windowWidth`	Permet de régler la largeur de la fenêtre en pixels si `windowSize` est défini sur la `Fixed Size`.
`root/ConnectionType/xen/gui/XenDesktopPanel/disabled`	Si la valeur est définie sur 1, le panneau XenDesktop et sa barre des tâches sont désactivés. Généralement, elle est définie sur 1 lorsque `autoStartResource` ou `autoStartDesktop` est activé.

Clé de registre	Description
`root/ConnectionType/xen/gui/XenManager/name`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/xen/gui/XenManager/status`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/xen/gui/XenManager/title`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/ConnectionType/xen/gui/XenManager/widgets/address`	Contrôle l'état du widget **URL de service** dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/appInMenu`	Contrôle l'état du widget **Afficher les applications dans la barre des tâches** dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/appOnDesktop`	Contrôle l'état du widget **Afficher les applications sur le bureau** dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/autoReconnect`	Contrôle l'état du widget **Reconnexion automatique** dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/autoStartDesktop`	Contrôle l'état du widget **Démarrage automatique du bureau** dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/autoStartResource`	Contrôle l'état du widget **Démarrage automatique de la ressource** dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/autostart`	Contrôle l'état du widget **Priorité du démarrage automatique** dans le gestionnaire de connexion Citrix. Si la valeur est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la valeur est définie sur `inactive`, le widget est masqué. Si la valeur est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/domain`	Contrôle l'état du widget **Domaine** dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.

Clé de registre	Description
`root/ConnectionType/xen/gui/XenManager/widgets/fallBackConnection`	Contrôle l'état du widget **Connexion de repli** dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/folder`	
`root/ConnectionType/xen/gui/XenManager/widgets/hasDesktopIcon`	Contrôle l'état du widget **Afficher l'icône sur le Bureau** dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/label`	Contrôle l'état du widget **Nom** dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/password`	Contrôle l'état du widget **Mot de passe** dans le gestionnaire de connexion Citrix. Si la valeur est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la valeur est définie sur `inactive`, le widget est masqué. Si la valeur est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/username`	Contrôle l'état du widget **Nom d'utilisateur** dans le gestionnaire de connexion Citrix. Si la valeur est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la valeur est définie sur `inactive`, le widget est masqué. Si la valeur est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/XenManager/widgets/waitForNetwork`	Contrôle l'état du widget **Wait for network before connection** (Attendre le réseau avant connexion) dans le gestionnaire de connexion Citrix. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/ConnectionType/xen/gui/fbpanel/autohide`	Si la valeur est définie sur `true`, la barre des tâches se masque automatiquement.
`root/ConnectionType/xen/gui/fbpanel/edge`	Définit la position par défaut de la barre des tâches lorsque plusieurs applications ou bureaux publiés sont disponibles.
`root/ConnectionType/xen/gui/fbpanel/hidden`	Si la valeur est définie sur 1, la barre des tâches est complètement masquée, mais uniquement si `autoStartResource` ou `autoStartDesktop` est activé.

DHCP

Ce dossier existe pour prendre en charge des clés de registre temporaires qui sont ajoutées lorsque le système acquiert un bail DHCP. Aucune modification n'est nécessaire.

Dashboard

REMARQUE : Le tableau de bord est la même chose que la barre des tâches.

Clé de registre	Description
`root/Dashboard/GUI/Clock`	Si la valeur est définie sur 1, l'horloge est affichée dans la barre des tâches.
`root/Dashboard/GUI/DomainUser`	Si la valeur est définie sur 1, l'icône domaine-utilisateur s'affiche dans la barre de tâches si le système est en mode domaine-connexion.
`root/Dashboard/GUI/PowerButton`	Si la valeur est définie sur 1, le bouton marche/arrêt est affiché dans la barre des tâches.
`root/Dashboard/GUI/Search`	Si la valeur est définie sur 1, le bouton Recherche est affiché dans la barre des tâches.
`root/Dashboard/GUI/SystemTray`	Si la valeur est définie sur 1, la barre d'état système est affichée dans la barre des tâches.
`root/Dashboard/GUI/TaskBar`	Si la valeur est définie sur 1, la zone d'application est affichée dans la barre des tâches.
`root/Dashboard/General/AutoHide`	Si la valeur est définie sur 1, la barre des tâches se masque automatiquement.
`root/Dashboard/General/EnterLeaveTimeout`	Définit le délai en millisecondes avant que la barre des tâches se masque ou s'affiche lorsque `AutoHide` est activé.
`root/Dashboard/General/IconSize`	Définit la taille des icônes sur la barre des tâches. Si la valeur est définie sur -1, la taille de l'icône est basée sur la largeur de la barre des tâches.
`root/Dashboard/General/Length`	Définit la longueur de la barre des tâches.
`root/Dashboard/General/LengthToScreenSide`	Si la valeur est définie sur 1, la longueur de la barre des tâches est fixe et égale à la longueur du côté de l'écran sur lequel elle est ancrée.
`root/Dashboard/General/PanelDockSide`	Définit le côté de l'écran sur lequel la barre des tâches est ancrée.
`root/Dashboard/General/SlidingTimeout`	Définit le temps en millisecondes que la barre des tâches prend pour se masquer ou s'afficher lorsque `AutoHide` est activé.
`root/Dashboard/General/Width`	Définit la largeur de la barre des tâches. Si la valeur est définie sur -1, la largeur est mise à l'échelle en fonction de la hauteur de l'écran principal.

Imprivata

Clé de registre	Description
`root/Imprivata/ImprivataServer`	Spécifie l'URL du serveur Imprivata.
`root/Imprivata/USBr/Devices`	Répertorie certains périphériques USB dotés d'une règle de redirection prédéfinie spécifique aux connexions distantes lancées à l'aide de l'environnement Imprivata. Pour chaque périphérique USB, la règle de redirection est donnée par le

Clé de registre	Description
	réglage : forcedState. Nécessite OneSign ProveID Embedded 6,2 capable d'utiliser le jeu de scripts du fournisseur.
`root/Imprivata/USBr/Devices/1162:2200/forcedState`	Si la valeur est définie sur 0, elle ne redirigera pas.
`root/Imprivata/USBr/Devices/1162:2200/info`	
`root/Imprivata/USBr/Devices/147e:2016/forcedState`	Si la valeur est définie sur 0, elle ne redirigera pas.
`root/Imprivata/USBr/Devices/147e:2016/info`	
`root/Imprivata/enableImprivata`	Si la valeur est définie sur 1, le paramètre Imprivata ProveID Embedded est activé. Par défaut, cette clé est définie sur 0.

InputMethod

Clé de registre	Description
`root/InputMethod/enablelbus`	

Network

Clé de registre	Description
`root/Network/ActiveDirectory/Domain`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/Network/ActiveDirectory/DynamicDNS`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/Network/ActiveDirectory/Enabled`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/Network/ActiveDirectory/Method`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/Network/ActiveDirectory/Password`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/Network/ActiveDirectory/Username`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/Network/DNSServers`	D'autres serveurs DNS pour la résolution des noms de domaine peuvent être spécifiés ici. Les serveurs spécifiés seront utilisés en plus des serveurs récupérés via DHCP. Jusqu'à trois adresses IPv4 ou IPv6 peuvent être spécifiées, séparées par des virgules.
`root/Network/DefaultHostnamePattern`	Définit le modèle de nom d'hôte par défaut à utiliser lors de la génération d'un nouveau nom d'hôte. Cette option est utilisée si la clé de registre de `Hostname` et `/etc/hostname` sont tous les deux vides. Le modèle de nom d'hôte utilise `%` comme délimiteur. Dans l'exemple `HPTC%MAC: 1-6%`, `HPTC` serait le préfixe et les six caractères suivants seraient les premiers caractères de l'adresse MAC du client léger. Par conséquent, si l'adresse MAC du client léger est `11:22:33:44:55:66`, le nom d'hôte généré serait `HPTC112233`. Si le modèle est `TC%MAC%`, le nom d'hôte

Clé de registre	Description
	généré serait TC112233445566. Si le modèle est HP%MAC:7%, le nom d'hôte généré serait HP1122334.
root/Network/EncryptWpaConfig	Si la clé est définie sur 1, le champ est chiffré.
root/Network/FtpProxy	Définit l'adresse du proxy FTP. HP vous recommande d'utiliser le format suivant pour cette valeur, car le préfixe http est mieux pris en charge : http://ProxyServer:Port
root/Network/Hostname	Définit le nom d'hôte du client léger.
root/Network/HttpProxy	Définit l'adresse du proxy HTTP. HP vous recommande d'utiliser le format suivant : http://ProxyServer:Port
root/Network/HttpsProxy	Définit l'adresse du proxy HTTPS. HP vous recommande d'utiliser le format suivant pour cette valeur, car le préfixe http est mieux pris en charge : http://ProxyServer:Port
root/Network/IPSec/IPSecRules/<UUID>/DstAddr	Définit l'adresse de destination de la règle IPSec.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethod	Définit la méthode d'authentification de la règle IPSec. PSK est destiné à l'utilisation d'une clé prépartagée et Certificate est destiné à l'utilisation de fichiers de certificat.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodCACert	Si la méthode d'authentification utilisée est Certificate, le chemin d'accès du fichier de certificat CA est enregistré dans cette clé de registre.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodClientCert	Si la méthode d'authentification utilisée est Certificate, le chemin d'accès du fichier de certificat de client est enregistré dans cette clé de registre.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPresharedKey	Si la méthode d'authentification utilisée est PSK, la valeur de clé pré-partagée est enregistrée dans cette clé de registre.
root/Network/IPSec/IPSecRules/<UUID>/MMAuthMethodPrivateKey	Si la méthode d'authentification utilisée est Certificate, le chemin d'accès du fichier de clé privée correspondant au certificat de client est enregistré dans cette clé de registre.
root/Network/IPSec/IPSecRules/<UUID>/MMDHGroup	Définit le groupe Diffie-Hellman de la phase 1.
root/Network/IPSec/IPSecRules/<UUID>/MMEncryptionAlg	Définit l'algorithme de cryptage de la phase 1.
root/Network/IPSec/IPSecRules/<UUID>/MMIntegrityAlg	Définit l'algorithme d'intégrité de la phase 1.
root/Network/IPSec/IPSecRules/<UUID>/MMLifetimeMinutes	Définit la durée de vie de la phase 1.
root/Network/IPSec/IPSecRules/<UUID>/QMAHEnable	Active le protocole AH de la phase 2.
root/Network/IPSec/IPSecRules/<UUID>/QMAHIntegrityAlg	Définit l'algorithme d'intégrité AH de la phase 2.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEnable	Active le protocole ESP de la phase 2.
root/Network/IPSec/IPSecRules/<UUID>/QMESPEncryptionAlg	Définit l'algorithme de cryptage ESP de la phase 2.
root/Network/IPSec/IPSecRules/<UUID>/QMESPIntegrityAlg	Définit l'algorithme d'intégrité ESP de la phase 2.

Clé de registre	Description
root/Network/IPSec/IPSecRules/<UUID>/QMLifetimeSeconds	Définit la durée de vie de la phase 2.
root/Network/IPSec/IPSecRules/<UUID>/RuleDescription	Définit la description de la règle IPSec.
root/Network/IPSec/IPSecRules/<UUID>/RuleEnable	Si la valeur est définie sur 1, la règle est activée.
root/Network/IPSec/IPSecRules/<UUID>/RuleName	Définit le nom de la règle IPSec.
root/Network/IPSec/IPSecRules/<UUID>/SrcAddr	Définit l'adresse de la source de la règle IPSec.
root/Network/IPSec/IPSecRules/<UUID>/TunnelDstAddr	Définit l'adresse de destination du tunnel pour la règle IPSec.
root/Network/IPSec/IPSecRules/<UUID>/TunnelEnable	Active le mode tunnel pour la règle IPSec.
root/Network/IPSec/IPSecRules/<UUID>/TunnelSrcAddr	Définit l'adresse source du tunnel pour la règle IPSec.
root/Network/KeepPreviousDNS	Si la valeur est définie sur 1, les serveurs DNS configurés au préalable et les domaines de recherche non générés par le gestionnaire réseau sont conservés dans resolv.conf. Si la valeur est définie sur 0, resolv.conf est complètement écrasé.
root/Network/SearchDomains	D'autres domaines de recherche pour la résolution FQDN peuvent être spécifiés ici. Les domaines spécifiés seront ajoutés à toute définition de serveur incomplète afin de tenter de générer un FQDN pouvant être résolu via DNS. Par exemple, un domaine de recherche de mydomain.com permettra à la définition du serveur myserver de résoudre correctement myserver.mydomain.com, même si le serveur DNS ne contient pas myserver dans ses tables de résolution de nom. Jusqu'à cinq domaines de recherche supplémentaires peuvent être spécifiés.
root/Network/VPN/AutoStart	Si la valeur est définie sur 1, VPN se lance automatiquement lorsque le système démarre.
root/Network/VPN/PPTP/Domain	Définit le domaine PPTP.
root/Network/VPN/PPTP/Gateway	Définit la passerelle PPTP.
root/Network/VPN/PPTP/Password	Définit le mot de passe de l'utilisateur PPTP.
root/Network/VPN/PPTP/Username	Définit le nom de l'utilisateur PPTP.
root/Network/VPN/Type	Définit le type de VPN.
root/Network/VPN/VPNC/DPDEndianess	Définit les endiannes du numéro de séquence DPD (voir rfc3706). 0 : big endian ; 1 : little endian. Essayez de les commuter si la session est abandonnée par intermittence sans raison apparente.
root/Network/VPN/VPNC/DPDInterval	Définit l'intervalle DPD (voir rfc3706) en secondes.
root/Network/VPN/VPNC/DebugLevel	Définit le niveau de débogage sur 0, 1, 2, 3, ou 99. Ceci génère de nombreux journaux. Ne l'activez que lorsque vous devez dépanner un problème de VPN.
root/Network/VPN/VPNC/Domain	Définit le domaine VPNC.
root/Network/VPN/VPNC/Gateway	Définit la passerelle VPNC.

Clé de registre	Description
root/Network/VPN/VPNC/Group	Définit le groupe VPNC.
root/Network/VPN/VPNC/GroupPassword	Définit le mot de passe du groupe VPNC.
root/Network/VPN/VPNC/IKEDHGroup	Définit le groupe Diffie-Hellman VPNC IKE.
root/Network/VPN/VPNC/LocalUDPPort	Définit le port UDP local à utiliser pour VPNC. Si le jeu est défini sur 0, un port aléatoire sera utilisé. Ce paramètre est valide uniquement lorsque le mode transversal NAT (NATTMode) est cisco udp.
root/Network/VPN/VPNC/NATTMode	Définit le mode transversal NAT VPNC.
root/Network/VPN/VPNC/Password	Définit le mot de passe de l'utilisateur VPNC.
root/Network/VPN/VPNC/PerfectForwardSecrecy	Définit le groupe Diffie-Hellman de VPNC à utiliser pour Perfect Forward Secrecy (PFS).
root/Network/VPN/VPNC/Security	Définit le niveau de sécurité du VPNC.
root/Network/VPN/VPNC/Username	Définit le nom de l'utilisateur VPNC.
root/Network/VisibleInSystray	Si la valeur est définie sur 1, l'icône de réseau est visible dans la barre d'état système.
root/Network/Wired/DefaultGateway	Définit la passerelle par défaut utilisée par le périphérique pour communiquer avec Internet. En général, il s'agit de l'adresse IP du routeur. Ce paramètre ne prend effet que si Method est définie sur Static.
root/Network/Wired/EnableDefGatewayAsDNS	Si la valeur est définie sur 1, la passerelle par défaut est également le serveur de noms.
root/Network/Wired/EthernetSpeed	Définit la vitesse de liaison de l'interface réseau Ethernet principale. Automatic permet d'utiliser la vitesse de connexion la plus rapide disponible, qui est généralement de 1 Gbit/s ou de 100 Mbit/s à plein débit selon le commutateur. La vitesse de connexion peut également être forcée sur une seule vitesse (100 ou 10 Mbit/s) et sur le mode duplex (intégral ou semi-duplex) pour prendre en charge les commutateurs et les concentrateurs qui ne réalisent pas la négociation automatique appropriée.
root/Network/Wired/IPAddress	Définit l'adresse IPv4 du client léger. Ce paramètre prend uniquement effet lorsque Method est défini sur Static.
root/Network/Wired/IPv6Enable	Si la valeur est définie sur 1, IPv6 est activé.
root/Network/Wired/Interface	Définit la carte réseau ou l'interface Ethernet par défaut.
root/Network/Wired/MTU	Définit le MTU. Peu importe que l'adresse IP soit statique ou obtenue par DHCP.
root/Network/Wired/Method	Si la clé est définie sur Automatic, le client léger utilise DHCP pour tenter de récupérer les paramètres du réseau. Si la clé est définie sur Static, les valeurs des clés de registre IPAddress, SubnetMask et DefaultGateway sont utilisées. HP ne recommande pas l'utilisation du paramètre Static dans un profil de client générique, car cela implique que tous les clients reçoivent la même adresse IP.
root/Network/Wired/Profiles/<UUID>/AutoConnect	Si la valeur est définie sur 1, la connexion automatique au réseau est activée.
root/Network/Wired/Profiles/<UUID>/EthernetSpeed	Définit la vitesse de liaison de l'interface réseau Ethernet principale. Automatic permet d'utiliser la vitesse de connexion

Clé de registre	Description
	la plus rapide disponible, qui est généralement de 1 Gbit/s ou de 100 Mbit/s à plein débit selon le commutateur. La vitesse de connexion peut être forcée sur la combinaison d'une seule vitesse (`100` ou `10` Mbit/s) et sur le mode duplex (`Full` ou `Half`) pour prendre en charge les commutateurs et les concentrateurs qui ne réalisent pas la négociation automatique.
`root/Network/Wired/Profiles/<UUID>/IPv4/Address`	Définit l'adresse IPv4 du client. Ce paramètre ne prend effet que si `Method` est définie sur `Static`.
`root/Network/Wired/Profiles/<UUID>/IPv4/DefaultGateway`	Définit la passerelle par défaut utilisée par le périphérique pour communiquer avec Internet. En général, il s'agit de l'adresse IP du routeur. Ce paramètre ne prend effet que si `Method` est définie sur `Static`.
`root/Network/Wired/Profiles/<UUID>/IPv4/Enabled`	Si la valeur est définie sur 1, IPv4 est activé pour ce profil.
`root/Network/Wired/Profiles/<UUID>/IPv4/Method`	Si la valeur est définie sur `Automatic`, le client utilise DHCP pour tenter de récupérer les paramètres du réseau. Si la valeur est définie sur `Static`, les valeurs des clés de registre `Address`, `SubnetMask` et `DefaultGateway` sont utilisées. HP ne recommande pas l'utilisation du paramètre `Static` dans un profil client générique, car cela implique que tous les clients reçoivent la même adresse IP.
`root/Network/Wired/Profiles/<UUID>/IPv4/SubnetMask`	Définit le masque de sous-réseau du périphérique, comme 255.255.255.0 (pour un sous-réseau standard de classe C). Ce paramètre ne prend effet que si `Method` est définie sur `Static`.
`root/Network/Wired/Profiles/<UUID>/IPv6/Address`	Définit l'adresse IPv6 du client. Ce paramètre ne prend effet que si `Method` est définie sur `Static`.
`root/Network/Wired/Profiles/<UUID>/IPv6/DefaultGateway`	Définit la passerelle par défaut utilisée par le périphérique pour communiquer avec Internet. En général, il s'agit de l'adresse IP du routeur. Ce paramètre ne prend effet que si `Method` est définie sur `Static`.
`root/Network/Wired/Profiles/<UUID>/IPv6/Enabled`	Si la valeur est définie sur 1, IPv6 est activé pour ce profil.
`root/Network/Wired/Profiles/<UUID>/IPv6/Method`	Si la valeur est définie sur `Automatic`, le client utilise DHCP pour tenter de récupérer les paramètres du réseau. Si la valeur est définie sur `Static`, les valeurs des clés de registre `Address`, `SubnetMask` et `DefaultGateway` sont utilisées. HP ne recommande pas l'utilisation du paramètre `Static` dans un profil client générique, car cela implique que tous les clients reçoivent la même adresse IP.
`root/Network/Wired/Profiles/<UUID>/IPv6/SubnetMask`	Définit le masque de sous-réseau du périphérique, qui est généralement la longueur du préfixe IPv6. Ce paramètre ne prend effet que si `Method` est définie sur `Static`.
`root/Network/Wired/Profiles/<UUID>/MTU`	Définit le MTU. Peu importe que l'adresse IP soit statique ou obtenue par DHCP.
`root/Network/Wired/Profiles/<UUID>/Priority`	Réservé pour un réseau câblé.
`root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/AnonyIdentity`	Définit l'identité anonyme pour l'authentification PEAP.
`root/Network/Wired/Profiles/<UUID>/EAPPEAP/CACert`	Définit le chemin d'accès au fichier de certificat CA pour l'authentification PEAP.

Clé de registre	Description
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/InnerAuth	Définit le protocole d'authentification interne PEAP.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/PEAPVer	Définit la version du PEAP.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/Password	Définit le mot de passe pour l'authentification PEAP.
root/Network/Wired/Profiles/<UUID>/Security/EAPPEAP/Username	Définit le nom d'utilisateur pour l'authentification PEAP.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/CACert	Définit le chemin d'accès au fichier de certificat CA pour l'authentification TLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/Identity	Définit l'identité pour l'authentification TLS.
root/Network/Wired/Profiles/<UUID>/EAPTLS/PrivateKey	Définit le chemin d'accès à un fichier de clé privée pour l'authentification TLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTLS/PrivateKeyPassword	Définit le mot de passe à un fichier de clé privée pour l'authentification TLS.
root/Network/Wired/Profiles/<UUID>/EAPTLS/UserCert	Définit le chemin d'accès à un fichier de certificat utilisateur pour l'authentification TLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/AnonyIdentity	Définit l'identité anonyme pour l'authentification TTLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/CACert	Définit le chemin d'accès au fichier de certificat CA pour l'authentification TTLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/InnerAuth	Définit le protocole d'authentification interne TTLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/Password	Définit le mot de passe pour l'authentification TTLS.
root/Network/Wired/Profiles/<UUID>/Security/EAPTTLS/Username	Définit le nom d'utilisateur pour l'authentification TTLS.
root/Network/Wired/Profiles/<UUID>/Security/Type	Définit le type d'authentification câblée.
root/Network/Wired/Profiles/<UUID>/WiredInterface	Définit l'interface câblée pour le profil.
root/Network/Wired/Security/CACert	Définit le chemin d'accès au fichier de certificat CA.
root/Network/Wired/Security/EnableMachineAuth	Si la valeur est définie sur 1, l'authentification de la machine pour PEAP est activée.
root/Network/Wired/Security/Identity	Définit si l'identité est anonyme ou non.
root/Network/Wired/Security/InnerAuth	Définit le protocole d'authentification interne PEAP.
root/Network/Wired/Security/InnerAuthTTLS	Définit le protocole d'authentification interne TTLS.
root/Network/Wired/Security/MachineAuthName	Stocke le nom du compte de la machine lorsque l'authentification de la machine est activée.
root/Network/Wired/Security/MachineAuthPassword	Stocke le mot de passe du compte de la machine lorsque l'authentification de la machine est activée.
root/Network/Wired/Security/PEAPVersion	Définit la version du PEAP.

Clé de registre	Description
root/Network/Wired/Security/Password	Définit le mot de passe.
root/Network/Wired/Security/PrivateKey	Définit le chemin d'accès à un fichier de clé privée. Cette option est utilisée uniquement pour l'authentification TLS.
root/Network/Wired/Security/Type	Définit le type d'authentification 802.1 x.
root/Network/Wired/Security/UserCert	Définit le chemin d'accès à un fichier de certificat utilisateur. Cette option est utilisée uniquement pour l'authentification TLS.
root/Network/Wired/Security/Username	Définit le nom de l'utilisateur.
root/Network/Wired/SubnetMask	Définit le masque de sous-réseau du périphérique, comme 255.255.255.0 (pour un sous-réseau standard de classe C). Ce paramètre prend uniquement effet lorsque Method est défini sur Static.
root/Network/Wired/UseWiredProfiles	Si la valeur est définie sur 1, la connexion câblée est configurée en mode profil, pour se connecter à plusieurs réseaux câblés. Si la valeur est définie sur 0, elle ne peut se connecter qu'à un seul réseau câblé.
root/Network/WiredWirelessSwitch	Si la valeur est définie sur 0, un réseau câblé et un réseau sans fil peuvent être connectés simultanément. Si la valeur est définie sur 1, le réseau câblé prend la priorité sur le réseau sans fil ; ce qui signifie qu'un réseau sans fil configuré est utilisé si le réseau câblé ne peut pas se connecter.
root/Network/Wireless/DefaultGateway	Définit la passerelle par défaut utilisée par le périphérique pour communiquer avec Internet. En général, il s'agit de l'adresse IP du routeur. Ce paramètre prend uniquement effet lorsque Method est défini sur Static.
root/Network/Wireless/EnableDefGatewayAsDNS	Si la valeur est définie sur 1, la passerelle par défaut est également le serveur de noms.
root/Network/Wireless/EnableWireless	Si la valeur est définie sur 1, la fonctionnalité sans fil est activée. Si la valeur est définie sur 0, la fonctionnalité sans fil est désactivée.
root/Network/Wireless/IPAddress	Définit l'adresse IPv4 du client léger. Ce paramètre prend uniquement effet lorsque Method est défini sur Static.
root/Network/Wireless/IPv6Enable	Si la valeur est définie sur 1, IPv6 est activé.
root/Network/Wireless/Interface	Définit l'adaptateur réseau sans fil ou l'interface sans fil par défaut.
root/Network/Wireless/Method	Si la clé est définie sur Automatic, le client léger utilise DHCP pour tenter de récupérer les paramètres du réseau. Si la clé est définie sur Static, les valeurs des clés de registre IPAddress, SubnetMask et DefaultGateway sont utilisées. HP ne recommande pas l'utilisation du paramètre Static dans un profil de client générique, car cela implique que tous les clients reçoivent la même adresse IP.
root/Network/Wireless/PowerEnable	Si la valeur est définie sur 1, la gestion de l'alimentation de la carte réseau sans fil est activée.
root/Network/Wireless/Profiles/<UUID>/AutoConnect	Si la valeur est définie sur 1, la connexion automatique au SSID est activée.
root/Network/Wireless/Profiles/<UUID>/IPv4/Address	Définit l'adresse IPv4 du client. Ce paramètre ne prend effet que si Method est définie sur Static.

Clé de registre	Description
root/Network/Wireless/Profiles/<UUID>/IPv4/DefaultGateway	Définit la passerelle par défaut utilisée par le périphérique pour communiquer avec Internet. En général, il s'agit de l'adresse IP du routeur. Ce paramètre ne prend effet que si Method est définie sur Static.
root/Network/Wireless/Profiles/<UUID>/IPv4/Enabled	Si la valeur est définie sur 1, IPv4 est activé pour ce profil.
root/Network/Wireless/Profiles/<UUID>/IPv4/Method	Si la valeur est définie sur Automatic, le client utilise DHCP pour tenter de récupérer les paramètres du réseau. Si la valeur est définie sur Static, les valeurs des clés de registre Address, SubnetMask et DefaultGateway sont utilisées. HP ne recommande pas l'utilisation du paramètre Static dans un profil client générique, car cela implique que tous les clients utilisant ce profil reçoivent la même adresse IP.
root/Network/Wireless/Profiles/<UUID>/IPv4/SubnetMask	Définit le masque de sous-réseau du périphérique, comme 255.255.255.0 (pour un sous-réseau standard de classe C). Ce paramètre ne prend effet que si Method est définie sur Static.
root/Network/Wireless/Profiles/<UUID>/IPv6/Address	Définit l'adresse IPv6 du client. Ce paramètre ne prend effet que si Method est définie sur Static.
root/Network/Wireless/Profiles/<UUID>/IPv6/DefaultGateway	Définit la passerelle par défaut utilisée par le périphérique pour communiquer avec Internet. En général, il s'agit de l'adresse IP du routeur. Ce paramètre ne prend effet que si Method est définie sur Static.
root/Network/Wireless/Profiles/<UUID>/IPv6/Enabled	Si la valeur est définie sur 1, IPv6 est activé pour ce profil.
root/Network/Wireless/Profiles/<UUID>/IPv6/Method	Si la valeur est définie sur Automatic, le client utilise DHCP pour tenter de récupérer les paramètres du réseau. Si la valeur est définie sur Static, les valeurs des clés de registre Address, SubnetMask et DefaultGateway sont utilisées. HP ne recommande pas l'utilisation du paramètre Static dans un profil client générique, car cela implique que tous les clients reçoivent la même adresse IP.
root/Network/Wireless/Profiles/<UUID>/IPv6/SubnetMask	Définit le masque de sous-réseau du périphérique, qui est généralement la longueur du préfixe IPv6. Ce paramètre ne prend effet que si Method est définie sur Static.
root/Network/Wireless/Profiles/<UUID>/PowerEnable	Si la valeur est définie sur 1, la gestion de l'alimentation de la carte réseau sans fil est activée.
root/Network/Wireless/Profiles/<UUID>/Priority	Définit la priorité du réseau. Pour un réseau sans fil, un nombre plus élevé signifie une priorité plus élevée. Une priorité élevée est préférable pour une connexion réseau sans fil.
root/Network/Wireless/Profiles/<UUID>/SSID	Définit le point d'accès sans fil à utiliser via son SSID.
root/Network/Wireless/Profiles/<UUID>/SSIDHidden	Spécifie si le SSID du point d'accès sans fil est masqué.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/AnonyIdentity	Définit l'identité anonyme pour l'authentification EAP-FAST.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/FastProvision	Définit l'option d'approvisionnement pour l'authentification EAP FAST.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/PACFile	Définit le chemin d'accès au fichier PAC pour l'authentification EAP-FAST.

Clé de registre	Description
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/Password	Définit le mot de passe pour l'authentification EAP-FAST.
root/Network/Wireless/Profiles/<UUID>/Security/EAPFAST/Username	Définit le nom d'utilisateur pour l'authentification EAP-FAST.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/AnonyIdentity	Définit l'identité anonyme pour l'authentification EAP PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/CACert	Définit le chemin d'accès au fichier de certificat CA pour l'authentification EAP PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/InnerAuth	Définit le protocole d'authentification interne PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/PEAPVer	Définit la version du PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/Password	Définit le mot de passe pour l'authentification EAP PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPPEAP/Username	Définit le nom d'utilisateur pour l'authentification EAP PEAP.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/CACert	Définit le chemin d'accès au fichier de certificat CA pour l'authentification TLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/Identity	Définit l'identité pour l'authentification TLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/PrivateKey	Définit le chemin d'accès à un fichier de clé privée pour l'authentification TLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/PrivateKeyPassword	Définit le mot de passe à un fichier de clé privée pour l'authentification TLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTLS/UserCert	Définit le chemin d'accès à un fichier de certificat utilisateur pour l'authentification TLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/AnonyIdentity	Définit l'identité anonyme pour l'authentification TTLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/CACert	Définit le chemin d'accès au fichier de certificat CA pour l'authentification TTLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/InnerAuth	Définit le protocole d'authentification interne TTLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/Password	Définit le mot de passe pour l'authentification TTLS.
root/Network/Wireless/Profiles/<UUID>/Security/EAPTTLS/Username	Définit le nom d'utilisateur pour l'authentification TTLS.
root/Network/Wireless/Profiles/<UUID>/Security/PSK/HexdecimalMode	
root/Network/Wireless/Profiles/<UUID>/Security/PSK/PreSharedKey	Définit le mot de passe pour l'authentification PSK.
root/Network/Wireless/Profiles/<UUID>/Security/Type	Définit le type d'authentification sans fil.
root/Network/Wireless/Profiles/<UUID>/Security/WEP/AuthType	Définit le type d'authentification WEP.

Clé de registre	Description
root/Network/Wireless/Profiles/<UUID>/Security/WEP/Key	Définit le mot de passe WEP.
root/Network/Wireless/Profiles/<UUID>/Security/WEP/KeyIndex	Définit l'index de mot de passe WEP.
root/Network/Wireless/Profiles/<UUID>/Security/WirelessBand	Spécifie la sélection de la plage de fréquence. Sélectionnez `Auto` pour rechercher tous les canaux sans fil ; sélectionnez `2,4 GHz` pour rechercher uniquement les canaux 2,4 GHz ; sélectionnez `5 GHz` pour rechercher uniquement les canaux 5 GHz.
root/Network/Wireless/Profiles/<UUID>/Security/WirelessInterface	Définit l'interface sans fil pour le profil.
root/Network/Wireless/Roaming/enableRoamingOptions	Si elle est définie sur 1, les options d'itinérance sont configurables.
root/Network/Wireless/Roaming/longScanInterval	Spécifie la fréquence, en secondes, pour rechercher un point d'accès avec un signal plus fort lorsque l'intensité du signal est supérieure au seuil d'itinérance. La valeur par défaut est 60.
root/Network/Wireless/Roaming/roamingNap	Spécifie la fréquence, en secondes, pour mettre en veille la connexion lorsque l'état wpa_applicant change. Cela permet de réduire les faux événements Wi-Fi pouvant briser les connexions en direct lorsque l'itinérance se produit.
root/Network/Wireless/Roaming/roamingThreshold	Définit la puissance maximale du signal, en dBm, autorisée avant de tenter une itinérance vers un point d'accès plus robuste. À noter que cette valeur est négative.
root/Network/Wireless/Roaming/scanInterval	Définit à quelle fréquence, en secondes, la recherche d'un point d'accès plus robuste doit être effectuée lorsque la puissance du signal est inférieure au seuil d'itinérance.
root/Network/Wireless/SSID	Définit le point d'accès sans fil à utiliser via son SSID.
root/Network/Wireless/SSIDHidden	Spécifie si le SSID du point d'accès sans fil est masqué.
root/Network/Wireless/SSIDWhiteList	Spécifie une liste blanche des points d'accès sans fil. Si la valeur de cette clé de Registre n'est pas vide, seuls les SSID spécifiés dans la valeur seront affichés dans les résultats de recherche du point d'accès sans fil. Utilisez un point-virgule (;) pour séparer les SSID.
root/Network/Wireless/Security/CACert	Définit le chemin d'accès au fichier de certificat CA.
root/Network/Wireless/Security/EAPFASTPAC	Définit le chemin d'accès au fichier PAC pour l'authentification EAP-FAST.
root/Network/Wireless/Security/EAPFASTProvision	Définit l'option d'approvisionnement pour l'authentification EAP FAST.
root/Network/Wireless/Security/Identity	Définit si l'identité est anonyme ou non.
root/Network/Wireless/Security/InnerAuth	Définit le protocole d'authentification interne PEAP.
root/Network/Wireless/Security/InnerAuthTTLS	Définit le protocole d'authentification interne TTLS.
root/Network/Wireless/Security/PEAPVersion	Définit la version du PEAP.
root/Network/Wireless/Security/Password	Définit le mot de passe.
root/Network/Wireless/Security/PrivateKey	Définit le chemin d'accès à un fichier de clé privée. Cette option est utilisée uniquement pour l'authentification TLS.

Clé de registre	Description
`root/Network/Wireless/Security/Type`	Définit le type d'authentification sans fil.
`root/Network/Wireless/Security/UserCert`	Définit le chemin d'accès à un fichier de certificat utilisateur. Cette option est utilisée uniquement pour l'authentification TLS.
`root/Network/Wireless/Security/Username`	Définit le nom de l'utilisateur.
`root/Network/Wireless/Security/WEPAuth`	Définit le type d'authentification WEP.
`root/Network/Wireless/Security/WEPIndex`	Définit l'index de mot de passe WEP.
`root/Network/Wireless/SubnetMask`	Définit le masque de sous-réseau du périphérique, comme 255.255.255.0 (pour un sous-réseau standard de classe C). Ce paramètre prend uniquement effet lorsque `Method` est défini sur `Static`.
`root/Network/Wireless/UseWirelessProfiles`	Si la valeur est définie sur 1, la connexion sans fil est configurée en mode profil, pour se connecter à plusieurs réseaux sans fil. Cette option est utile pour l'informatique mobile. Si la valeur est définie sur 0, un seul réseau sans fil configuré peut être connecté.
`root/Network/Wireless/WirelessBand`	Spécifie la sélection de la plage de fréquence. Sélectionnez `Auto` (Automatique) pour rechercher tous les canaux sans fil ; sélectionnez `2,4 GHz` pour rechercher uniquement les canaux 2,4 GHz ; sélectionnez `5 GHz` pour rechercher uniquement les canaux 5 GHz.
`root/Network/Wireless/WpaDriver`	Spécifie le pilote utilisé par wpa_supplicant (`wext`, par défaut). `nl80211` est le seul autre pilote actuellement pris en charge.
`root/Network/Wireless/bcmwlCountryOverride`	Remplace la valeur du pays du BIOS dans l'éventualité où le BIOS ne dispose pas de la valeur requise. Le pilote bcmwl accepte l'option wl_country, qui est récupérée des valeurs du BIOS en fonction des besoins (seule l'Indonésie est prise en charge actuellement). Un redémarrage du système est nécessaire pour que les modifications apportées soient prises en compte.
`root/Network/Wireless/disableUserCreateWirelessProfile`	Si la valeur est définie sur 1, les comptes utilisateur ne peuvent pas créer de profils sans fil à partir de la barre des tâches sans fil.
`root/Network/Wireless/disableUserWirelessProfileTrayMenu`	Si la valeur est définie sur 1, le menu sans fil dans la barre des tâches sans fil est désactivé pour le compte de l'utilisateur.
`root/Network/Wireless/disableWirelessProfileTrayMenu`	Si la valeur est définie sur 1, le menu sans fil de l'icône de la barre des tâches sans fil est désactivé.
`root/Network/Wireless/tryAutoWirelessIfUserFailed`	Si la valeur est définie sur 1, si un utilisateur essaie de se connecter à un AP sans fil et échoue, le module sans fil essaie de se connecter sans fil en utilisant tous les profils disponibles. Si la valeur est définie sur 0, si un utilisateur essaie de se connecter à un AP sans fil et échoue, l'état sans fil est défini sur déconnecté. Il s'agit d'une fonction de repli.
`root/Network/disableLeftClickMenu`	Si la valeur est définie sur 1, le menu contextuel (clic gauche) de l'icône de la barre d'état système réseau est désactivé.
`root/Network/disableRightClickMenu`	Si la valeur est définie sur 1, le menu contextuel (clic droit) de l'icône de la barre d'état système réseau est désactivé.
`root/Network/enableVPNMenu`	Si la valeur est définie sur 1, le menu VPN du clic gauche accessible depuis l'icône Réseau de la barre des tâches est activé.

Clé de registre	Description
root/Network/userLock	Si la clé est définie sur 1 et si les paramètres réseau ont été modifiés par l'utilisateur, les paramètres réseau sont conservés lors de l'importation d'un profil de client.
root/Network/userLockEngaged	Cette clé est définie sur 1 automatiquement une fois que les paramètres de réseau ont été modifiés par l'utilisateur. Il n'est normalement pas nécessaire de modifier ce paramètre.

Power

Clé de registre	Description
root/Power/applet/VisibleInSystray	Si la valeur est définie sur 1, l'icône de batterie est affichée dans la barre d'état système.
root/Power/buttons/logout/authorized	Si la valeur est définie sur 1, la fonction de déconnexion est disponible.
root/Power/buttons/power/authorized	Si la valeur est définie sur 1, la fonction d'alimentation est disponible.
root/Power/buttons/poweroff/authorized	Si la valeur est définie sur 1, la fonction d'extinction est disponible.
root/Power/buttons/reboot/authorized	Si la valeur est définie sur 1, la fonction de redémarrage est disponible.
root/Power/buttons/sleep/authorized	Si la valeur est définie sur 1, la fonction de veille est disponible.
root/Power/currentPowerPlan	Cette clé de registre sélectionne le plan d'alimentation utilisé. Ce paramètre est automatiquement défini par défaut.
root/Power/default/AC/brightness	Définit le niveau de luminosité par défaut en pourcentage lorsque le client léger mobile est branché.
root/Power/default/AC/cpuMode	Définit le mode UC pour un plan d'alimentation alors que l'ordinateur est connecté à l'alimentation sur secteur. Par défaut, il est mis en performance.
root/Power/default/AC/lidAction	Définit l'action qui se produit lorsque le capot de l'ordinateur est fermé alors qu'il est connecté à l'alimentation sur secteur. Par défaut, il est défini sur Veille.
root/Power/default/AC/powerButtonAction	Définit l'action qui se produit lorsque vous appuyez sur le bouton d'alimentation alors que l'ordinateur est connecté à l'alimentation sur secteur. Par défaut, il est mis à l'arrêt.
root/Power/default/AC/sleep	Définit la valeur (en minutes) que l'ordinateur doit attendre avant d'entrer en état Veille alors qu'il est connecté à l'alimentation sur secteur. Par défaut, cette valeur est définie sur 30. Si cette valeur est définie sur 0, l'ordinateur ne passe jamais en état Veille.
root/Power/default/AC/standby	Définit la valeur (en minutes) que l'ordinateur doit attendre avant que l'écran ne s'éteigne alors qu'il est connecté à l'alimentation sur secteur. Par défaut, cette valeur est définie sur 15. Si cette valeur est définie sur 0, l'ordinateur ne passe jamais en mode veille prolongée.
root/Power/default/AC/timeoutDim	Cette clé est actuellement inutilisée.
root/Power/default/battery/brightness	Définit le niveau de luminosité par défaut en pourcentage lorsque le client léger mobile n'est pas branché.

Clé de registre	Description
`root/Power/default/battery/cpuMode`	Définit le mode UC pour un plan d'alimentation alors que l'ordinateur n'est pas connecté à l'alimentation sur secteur. Par défaut, il est défini sur à la demande.
`root/Power/default/battery/critical/criticalBatteryAction`	Définit l'action à effectuer lorsque le niveau de charge de la batterie est critique, défini par `criticalBatteryLevel`.
`root/Power/default/battery/critical/criticalBatteryLevel`	Définit le seuil en pourcentage auquel le niveau de puissance de la batterie est considéré comme critique.
`root/Power/default/battery/lidAction`	Définit l'action qui se produit lorsque le capot de l'ordinateur est fermé alors qu'il n'est pas connecté à l'alimentation sur secteur. Par défaut, il est défini sur Veille.
`root/Power/default/battery/low/brightness`	Définit le niveau de luminosité par défaut en pourcentage lorsque la puissance de la batterie est faible.
`root/Power/default/battery/low/cpuMode`	Définit le mode CPU (performance ou à la demande).
`root/Power/default/battery/low/lowBatteryLevel`	Définit le pourcentage de puissance de la batterie considéré comme critique.
`root/Power/default/battery/low/sleep`	Définit la valeur (en minutes) que l'ordinateur doit attendre avant d'entrer en état Veille alors que l'ordinateur n'est pas connecté à l'alimentation sur secteur. Par défaut, cette valeur est définie sur 30. Si cette valeur est définie sur 0, l'ordinateur ne passe jamais en état Veille.
`root/Power/default/battery/low/standby`	Définit la valeur (en minutes) que l'ordinateur doit attendre avant que l'écran ne s'éteigne alors qu'il n'est pas connecté à l'alimentation sur secteur. Par défaut, cette valeur est définie sur 15. Si cette valeur est définie sur 0, l'ordinateur ne passe jamais en mode veille prolongée.
`root/Power/default/battery/low/timeoutDim`	Cette clé est actuellement inutilisée.
`root/Power/default/battery/powerButtonAction`	Spécifie que faire lorsque le bouton d'alimentation est enfoncé.
`root/Power/default/battery/sleep`	Définit combien de minutes restent à attendre avant de passer en mode veille. 0 = jamais.
`root/Power/default/battery/standby`	Définit combien de minutes restent à attendre avant que l'écran s'éteigne. 0 = jamais.
`root/Power/default/battery/timeoutDim`	Cette clé est actuellement inutilisée.

ScepMgr

Clé de registre	Description
`root/ScepMgr/General/AutoRenew/Enabled`	Si la valeur est définie sur 1, les certificats seront renouvelés automatiquement avant qu'ils n'expirent.
`root/ScepMgr/General/AutoRenew/TimeFrame`	Définit le nombre de jours avant la date d'expiration d'un certificat pendant lesquels le gestionnaire de SCEP essaie de renouveler le certificat automatiquement.
`root/ScepMgr/IdentifyingInfo/CommonName`	Définit le nom commun à utiliser pour plus d'informations identification SCEP, telles que votre nom ou le nom de domaine Fully-Qualified (FQDN) du périphérique. Le FQDN est utilisé par défaut si cette valeur est laissée vide.

Clé de registre	Description
root/ScepMgr/IdentifyingInfo/CountryName	Définit le pays ou région à utiliser pour les informations d'identification SCEP.
root/ScepMgr/IdentifyingInfo/EmailAddress	Définit l'adresse e-mail à utiliser pour les informations d'identification SCEP.
root/ScepMgr/IdentifyingInfo/LocalityName	Définit le nom de localité à utiliser pour plus d'informations d'identification SCEP, tel qu'un nom de ville.
root/ScepMgr/IdentifyingInfo/OrganizationName	Définit le nom de l'organisation à utiliser pour plus d'informations d'identification SCEP, tel qu'un nom de société ou le nom d'une organisation gouvernementale.
root/ScepMgr/IdentifyingInfo/OrganizationUnitName	Définit le nom de l'unité organisationnelle à utiliser pour plus d'informations d'identification SCEP, tel que le nom du service informatique ou le nom de la section.
root/ScepMgr/IdentifyingInfo/StateName	Permet de définir l'État ou la province à utiliser pour les informations d'identification SCEP.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/CertFileChanged	La clé de Registre est utilisée uniquement pour informer d'autres applications qu'un fichier de certificat a changé. Vous ne devriez pas avoir besoin de modifier cette clé.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/DontVerifyPeer	Cette clé de registre est utilisée pour HTTPS uniquement. Si la valeur est définie sur 1, le client SCEP ne vérifie pas le certificat du serveur. Cette clé est définie sur 0 par défaut.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/KeySize	Permet de régler la taille de clé à utiliser pour la paire générée.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ServerName	Définit le nom de serveur SCEP.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/ServerUrl	Définit l'URL du serveur SCEP, qui est nécessaire pour que le client SCEP inscrive un certificat.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/Status/Code	Contient le code d'état de l'inscription SCEP. Cette valeur est en lecture seule.
root/ScepMgr/ScepEnroll/ScepServers/<UUID>/Status/Detail	Contient des informations détaillées sur l'inscription SCEP. Cette valeur est en lecture seule.

Search

Clé de registre	Description
root/Search/Category/Miscellaneons/CheckForUpdate	
root/Search/Category/Miscellaneons/Logout	
root/Search/Category/Miscellaneons/Reboot	
root/Search/Category/Miscellaneons/ShutDown	
root/Search/Category/Miscellaneons/Sleep	
root/Search/Category/Miscellaneons/SwitchToAdmin	
root/Search/Category/Regeditor/byDir	

Clé de registre	Description
root/Search/Category/Regeditor/byKey	
root/Search/Category/Regeditor/byValue	
root/Search/Category/Regeditor/byWhole	

Serial

Clé de registre	Description
root/Serial/<UUID>/baud	Définit la vitesse du périphérique série.
root/Serial/<UUID>/dataBits	Définit le nombre de bits qui se trouvent dans chaque caractère.
root/Serial/<UUID>/device	Spécifie le périphérique série connecté au système.
root/Serial/<UUID>/flow	Définit le contrôle de flux du périphérique série, qui est utilisé pour communiquer les démarrages et les arrêts de la communication série.
root/Serial/<UUID>/name	Spécifie le port du périphérique Windows utilisé pour la communication avec le périphérique série.
root/Serial/<UUID>/parity	Définit le bit de parité du périphérique série. Le bit de parité est utilisé pour la détection des erreurs. Si la valeur est définie sur none, il n'y a pas de détection de la parité.

SystemInfo

Clé de registre	Description
root/SystemInfo/Pages/General	Si la clé est définie sur 0, l'onglet **Général** de la fenêtre Informations système est masqué pour les utilisateurs finaux.
root/SystemInfo/Pages/License	Si la clé est définie sur 0, l'onglet **Software License** (Licence du logiciel) de la fenêtre System Information (Informations système) est masqué pour les utilisateurs finaux.
root/SystemInfo/Pages/NetTools	Si définie sur 0, l'onglet **Net Tools** (Outils Internet) de la fenêtre System Information (Informations système) est masqué pour les utilisateurs finaux.
root/SystemInfo/Pages/Network	Si la clé est définie sur 0, l'onglet **Réseau** de la fenêtre System Information (Informations système) est masqué pour les utilisateurs finaux.
root/SystemInfo/Pages/SoftwareInformationTab/ServicePacks	Si la clé est définie sur 0, l'onglet **Service Packs** de la section **Software Information** (Informations du logiciel) de la fenêtre System Information (Informations système) est masqué pour les utilisateurs finaux.
root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInformation	Si la clé est définie sur 0, l'onglet **Informations du logiciel** de la fenêtre System Information (Informations système) est masqué pour les utilisateurs finaux.
root/SystemInfo/Pages/SoftwareInformationTab/SoftwareInstalled	Si la clé est définie sur 0, l'onglet **Logiciels installés** de la section **Informations du logiciel** de la fenêtre System Information (Informations système) est masqué pour les utilisateurs finaux.

Clé de registre	Description
`root/SystemInfo/Pages/SystemLogs`	Si la clé est définie sur 0, l'onglet **Journaux système** de la fenêtre System Information (Informations système) est masqué pour les utilisateurs finaux.
`root/SystemInfo/authorized`	Si la clé est définie sur 0, le bouton System Information (Informations système) de la barre des tâches est désactivé pour les utilisateurs finaux.

TaskMgr

Clé de registre	Description
`root/TaskMgr/General/AlwaysOnTop`	Si la valeur est définie sur 1, la fenêtre Gestionnaire des tâches est toujours en haut.

USB

Clé de registre	Description
`root/USB/Classes/(Defined at Interface level)/ClassID`	Définit le numéro d'identification de la classe USB.
`root/USB/Classes/(Defined at Interface level)/DisplayName`	Définit le nom de la classe USB.
`root/USB/Classes/(Defined at Interface level)/State`	Définit si la classe est mappée sur l'hôte distant.
`root/USB/Classes/(Defined at Interface level)/Visible`	Définit si la classe est affichée ou non dans l'interface utilisateur ou si elle est désactivée.
`root/USB/Devices/<UUID>/DisplayName`	Définit le nom à afficher dans le gestionnaire USB. Si ce nom n'est pas fourni, le gestionnaire USB tente de générer un nom approprié à l'aide d'informations sur le périphérique.
`root/USB/Devices/<UUID>/ProductID`	Définit l'identifiant produit du périphérique.
`root/USB/Devices/<UUID>/State`	Définit si ce périphérique est mappé sur l'hôte distant comme suit : 0 = Ne pas rediriger ; 1 = Utiliser les valeurs par défaut ; 2 = Ne pas rediriger.
`root/USB/Devices/<UUID>/VendorID`	Définit l'identifiant du fournisseur du périphérique.
`root/USB/root/autoSwitchProtocol`	Si la clé est définie sur 1, le protocole USB distant ne commute pas automatiquement selon le protocole choisi.
`root/USB/root/mass-storage/allowed`	Si la clé est définie sur 1, les dispositifs de stockage de masse sont montés automatiquement lorsque le protocole est `local`.
`root/USB/root/mass-storage/read-only`	Si la clé est définie sur 1, les dispositifs de stockage de masse sont montés en lecture seule lorsqu'ils sont montés automatiquement.

Clé de registre	Description
`root/USB/root/protocol`	Définit à quel protocole appartient l'USB distant. Les valeurs valides dépendent des protocoles installés sur le système mais peuvent inclure `local`, `xen`, `rdp` et `view`.
`root/USB/root/showClasses`	Si la clé est définie sur 1, la section **Classes** est affichée dans le gestionnaire USB.

auto-update

Clé de registre	Description
`root/auto-update/DNSAliasDir`	Définit le répertoire racine par défaut pour le mode alias DNS sur le serveur hébergeant HP Smart Client Services.
`root/auto-update/LockScreenTimeout`	Spécifie la temporisation (en minutes) après laquelle l'écran se déverrouille lors d'une mise à jour automatique. Si la valeur est définie sur 0, l'écran est déverrouillé pendant toute la mise à jour automatique, jusqu'à ce qu'elle soit terminée.
`root/auto-update/ManualUpdate`	Si la valeur est définie sur 1, les méthodes de mise à jour par balisage DHCP, par alias DNS et par diffusion pour la mise à jour automatique sont désactivées. Lors de l'exécution d'une mise à jour manuelle, les clés de registre `password`, `path`, `protocol`, `user` et `ServerURL` doivent être configurées pour vous assurer que le serveur de mise à jour est connu.
`root/auto-update/ScheduledScan/Enabled`	Si la valeur est définie sur 1, le client léger exécute des analyses périodiques du serveur de mise à jour automatique pour vérifier la présence de mises à jour. Si la valeur est définie sur 0, le client léger vérifie uniquement la présence de mises à jour au démarrage du système.
`root/auto-update/ScheduledScan/Interval`	Définit le délai d'attente entre chaque analyse de mise à jour planifiée. Ce délai doit être indiqué au format `hh:mm`. Des intervalles de plus de 24 heures peuvent être spécifiés. Par exemple, pour que les analyses se produisent toutes les 48 heures, réglez ce paramètre sur `48:00`.
`root/auto-update/ScheduledScan/Period`	Les clients légers activeront de manière aléatoire leur analyse programmée tout au long de la période définie. Définir une longue période permet d'éviter que tous les clients légers ne se mettent à jour au même moment, ce qui pourrait entraîner une surcharge du réseau. Cette période doit être spécifiée au format `hh:mm`. Par exemple, pour répartir les mises à jour de clients légers sur une période de 2,5 heures, régler ce paramètre sur `02:30`.
`root/auto-update/ScheduledScan/StartTime`	Définit l'heure de démarrage de la première période d'analyse de mise à jour planifiée au format `hh:mm`, à l'aide du format 24 heures. Par exemple, 16 heures 35 minutes correspond à `16:35`.
`root/auto-update/ServerURL`	Définit le nom de domaine ou l'adresse IP du serveur de mise à jour utilisé lorsque `ManualUpdate` est activé.
`root/auto-update/VisibleInSystray`	Si la valeur est définie sur 1, l'icône de barre d'état système de la mise à jour automatique est activée.
`root/auto-update/checkCertSig`	Si la valeur est définie sur 1, la signature du certificat est vérifiée.

Clé de registre	Description
`root/auto-update/checkCustomSig`	Si la valeur est définie sur 1, la signature de packages personnalisés est vérifiée.
`root/auto-update/checkImgSig`	Réservé à une utilisation ultérieure.
`root/auto-update/checkPackageSig`	Si la valeur est définie sur 1, la signature de packages est vérifiée.
`root/auto-update/checkProfileSig`	Si la valeur est définie sur 1, la signature de profils est vérifiée.
`root/auto-update/enableLockScreen`	Si elle est définie sur 1, l'écran se verrouille lorsqu'une mise à jour automatique est en cours.
`root/auto-update/enableOnBootup`	Si la valeur est définie sur 1, la mise à jour automatique est activée au démarrage du système.
`root/auto-update/enableSystrayLeftClickMenu`	Si la valeur est définie sur 1, le menu contextuel (clic gauche) de l'icône de la barre d'état système de la mise à jour automatique est activé.
`root/auto-update/enableSystrayRightClickMenu`	Si la valeur est définie sur 1, le menu contextuel (clic droit) de l'icône de la barre d'état système de la mise à jour automatique est activé.
`root/auto-update/gui/auto-update/ManualUpdate`	Contrôle l'état du widget **Activer la configuration manuelle** dans l'outil Automatic Update. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/auto-update/gui/auto-update/ServerURL`	Contrôle l'état du widget **Serveur** dans l'outil Automatic Update. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/auto-update/gui/auto-update/enableLockScreen`	Contrôle l'état du widget **Activer le verrouillage d'écran lors de la mise à jour automatique** dans l'outil de mise à jour automatique. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut interagir avec. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `lecture seule`, le widget est visible en lecture seule.
`root/auto-update/gui/auto-update/enableOnBootup`	Contrôle l'état du widget **Activer la mise à jour automatique au démarrage du système** dans l'outil Automatic Update. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/auto-update/gui/auto-update/password`	Contrôle l'état du widget **Mot de passe** dans l'outil de mise à jour automatique. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut interagir avec. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `lecture seule`, le widget est visible en lecture seule.
`root/auto-update/gui/auto-update/protocol`	Contrôle l'état du widget **Protocole** dans l'outil Automatic Update. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.

Clé de registre	Description
`root/auto-update/gui/auto-update/tag`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/auto-update/gui/auto-update/user`	Contrôle l'état du widget **Nom d'utilisateur** dans l'outil Automatic Update. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/auto-update/password`	Définit le mot de passe utilisé lorsque `ManualUpdate` est activé. Cette option est utilisée uniquement lorsque `protocol` est défini sur `ftp`. Cette valeur est cryptée.
`root/auto-update/path`	Définit le chemin d'accès relatif depuis l'URL du serveur par défaut lorsque `ManualUpdate` est activé. En général, cette valeur est vide ou définie sur `auto-update`.
`root/auto-update/preserveConfig`	Si la valeur est définie sur 1, les paramètres de configuration du client léger actuels sont conservés lorsqu'une mise à jour de l'image logicielle se produit via une mise à jour automatique.
`root/auto-update/protocol`	Définit le protocole utilisé lorsque `ManualUpdate` est activé.
`root/auto-update/tag`	Cette clé de registre est obsolète. Elle définissait le numéro de balise utilisé pour DHCP (137). Ce numéro est désormais détecté via le nom de balise `auto-update`.
`root/auto-update/user`	Définit le nom de l'utilisateur utilisé lorsque `ManualUpdate` est activé. Cette option est utilisée uniquement lorsque « protocol » (Protocole) est défini sur « ftp ».

background

Clé de registre	Description
`root/background/bginfo/alignment`	Définit l'alignement du texte Background Sysinfo.
`root/background/bginfo/enabled`	Si la clé est définie sur `1`, les informations sur le système sont affichées à l'arrière-plan du bureau (Background Sysinfo).
`root/background/bginfo/horizontalLocation`	Définit l'emplacement de Background Sysinfo sur l'axe des X, sous forme de pourcentage.
`root/background/bginfo/interval`	Définit l'intervalle de rafraîchissement en secondes de Background Sysinfo.
`root/background/bginfo/preset`	Définit le fichier prédéfini Background Sysinfo sur `use`. Si la clé est définie sur `none`, vous pouvez personnaliser les paramètres dans Background Manager (Gestionnaire d'arrière-plan).
`root/background/bginfo/shadowColor`	Définit la couleur de l'ombre Background Sysinfo.
`root/background/bginfo/shadowOffset`	Définit le décalage de l'ombre Background Sysinfo. Si la clé est définie sur `0`, l'ombre est désactivée.
`root/background/bginfo/text`	Définit le texte Background Sysinfo. Pour plus d'informations à ce sujet, consultez le livre blanc HP ThinPro *Login Screen Customization* (disponible en anglais uniquement).
`root/background/bginfo/textColor`	Définit la couleur du texte Background Sysinfo.

Clé de registre	Description
root/background/bginfo/textSize	Définit la taille du texte Background Sysinfo.
root/background/bginfo/verticalLocation	Définit l'emplacement de Background Sysinfo sur l'axe des Y, sous forme de pourcentage.
root/background/desktop/color	Spécifie la couleur unie, la couleur d'arrière-plan si elle est visible derrière l'image, ou la couleur du haut dans un dégradé.
root/background/desktop/color2	Si le paramètre theme (thème) est défini sur gradient (dégradé), cette clé enregistre la couleur du bas dans le dégradé.
root/background/desktop/imagePath	Si le paramètre theme est défini sur soit none (aucun) soit image, cette clé contient le chemin d'accès de l'image d'arrière-plan du bureau utilisée par le thème défini par l'utilisateur.
root/background/desktop/lastBrowseDir	Si le paramètre theme est défini sur none , cette clé contient le dernier répertoire utilisé.
root/background/desktop/style	Si le paramètre theme est défini sur none, cette clé contient la façon dont l'image d'arrière-plan est placée sur le bureau (comme centre, tile, stretch, fit et fill.
root/background/desktop/theme	Spécifie le paramètre du thème du système. Cette valeur est définie via Background Manager (Gestionnaire d'arrière-plan) du Panneau de configuration. Les valeurs valides dépendent des thèmes qui existent sur le système. Cela peut être défini sur aucun ou image afin que l'utilisateur puisse définir une image d'arrière-plan, sur automatique pour que le système paramètre automatiquement le thème du protocole approprié pour Smart Zero ou sur par défaut pour utiliser le thème par défaut pour ThinPro ou l'un des différents thèmes prédéfinis.
root/background/desktop/updateInterval	Définit l'intervalle de rafraîchissement de l'arrière-plan en secondes.

amorçage

Clé de registre	Description
root/boot/enablePlymouth	
root/boot/extraCmdline	

config-wizard

Clé de registre	Description
root/config-wizard/configWizardOptions	Indique, dans une liste séparée par des espaces, les options de l'assistant de configuration qui s'affichent. Par défaut, toutes les options (langue, clavier, réseau, DateHeure, fin) sont répertoriées.
root/config-wizard/disableAllChecksAtStartup	Si la valeur est définie sur 1, tous les contrôles au démarrage sont désactivés. Si définie sur 0, vous pouvez activer/désactiver chaque type de contrôle individuellement avec les clés de registre enableConnectionCheck, enableNetworkCheck et enableUpdateCheck.

Clé de registre	Description
`root/config-wizard/enableConfigWizard`	Si la valeur est définie sur 1, l'assistant de configuration au démarrage du système est activé.
`root/config-wizard/enableConnectionCheck`	Si la valeur est définie sur 1, la vérification de la connexion au démarrage du système est activée.
`root/config-wizard/enableNetworkCheck`	Si la valeur est définie sur 1, la vérification du réseau au démarrage du système est activée.
`root/config-wizard/showNetworkSettingsButton`	Si la valeur est définie sur 1, le bouton des paramètres réseau est affiché dans la fenêtre de contrôle du réseau.

desktop

Clé de registre	Description
`root/desktop/preferences/arrangeBy`	Indique s'il faut réorganiser les icônes par nom ou par type.
`root/desktop/preferences/fontFamily`	Spécifie la police utilisée pour les icônes du bureau.
`root/desktop/preferences/gridSize`	Indique, en pixels, la taille de la grille d'icônes de bureau. Si la valeur est définie sur une valeur inférieure à 64, la taille est calculée comme un pourcentage de la taille du moniteur.
`root/desktop/preferences/iconGlowColor`	Spécifie la couleur qui brille derrière l'icône du bureau lorsque le pointeur la survole. Les chaînes de caractères valides sont dans le style `QColor::setNamedColor()`. Si non définie, le système choisit une couleur qui contraste avec le fond.
`root/desktop/preferences/iconPercent`	Indique le pourcentage de la taille de grille à utiliser pour l'icône. Si la valeur est supérieure à 0, elle est calculée comme un pourcentage de la taille de grille.
`root/desktop/preferences/iconShadowColor`	Indique la couleur de l'ombre derrière l'icône du bureau et du texte. Les chaînes valides sont dans le style `QColor::setNamedColor()`. Si non définie, le système choisit une couleur qui contraste avec le fond.
`root/desktop/preferences/menu/arrange/authorized`	Spécifie si les utilisateurs peuvent utiliser la fonction Réorganiser sur le bureau.
`root/desktop/preferences/menu/create/authorized`	Spécifie si les utilisateurs peuvent créer des connexions à partir du menu du bouton droit de la souris sur le bureau.
`root/desktop/preferences/menu/drag/authorized`	Spécifie si les utilisateurs peuvent faire glisser les icônes sur le bureau.
`root/desktop/preferences/menu/lockScreen/authorized`	Spécifie si les utilisateurs peuvent verrouiller l'écran à partir du menu du bouton droit de la souris sur le bureau.
`root/desktop/preferences/menu/logout/authorized`	Spécifie si les utilisateurs peuvent se déconnecter à partir du menu du bouton droit de la souris sur le bureau.
`root/desktop/preferences/menu/modeSwitch/authorized`	Spécifie si les utilisateurs peuvent basculer en mode administrateur à partir du menu du bouton droit de la souris sur le bureau.
`root/desktop/preferences/menu/power/authorized`	Spécifie si les utilisateurs peuvent accéder au sous-menu alimentation à partir du menu du bouton droit de la souris sur le bureau.

Clé de registre	Description
root/desktop/preferences/menu/poweroff/authorized	Spécifie si les utilisateurs peuvent éteindre le système à partir du menu du bouton droit de la souris sur le bureau.
root/desktop/preferences/menu/reboot/authorized	Spécifie si les utilisateurs peuvent redémarrer le système à partir du menu du bouton droit de la souris sur le bureau.
root/desktop/preferences/menu/sleep/authorized	Spécifie si les utilisateurs peuvent mettre le système en état Veille à partir du menu du bouton droit de la souris sur le bureau.
root/desktop/preferences/menuTextSize	Indique la hauteur du texte du menu bureau en pixels. Si non-positive, la hauteur est calculée en tant que pourcentage de la taille du moniteur.
root/desktop/preferences/screenMargin	Spécifie la marge entre les bords de l'écran et les icônes.
root/desktop/preferences/textBold	Spécifie si le texte est mis en gras.
root/desktop/preferences/textColor	Spécifie la couleur du texte pour les icônes du bureau. Les chaînes valides sont dans le style `QColor::setNamedColor()`. Si non définie, le système choisit une couleur qui contraste avec le fond.
root/desktop/preferences/textShadowColor	Indique la couleur de l'ombre derrière les icônes du bureau et le texte. Les chaînes de caractères valides sont dans le style `QColor::setNamedColor()`. Si non définie, le système choisit une couleur qui contraste avec la couleur du texte.
root/desktop/preferences/textSize	Indique la hauteur du texte de l'icône bureau en pixels. Si non-positive, la hauteur est calculée en tant que pourcentage de la taille du moniteur.
root/desktop/shortcuts/<action>/command	Définit la commande exécutée par le raccourci.
root/desktop/shortcuts/<action>/enabled	Si la valeur est définie sur 1, le raccourci est activé.
root/desktop/shortcuts/<action>/shortcut	Définit le nom du raccourci.
root/desktop/shortcuts/<action>/shortcutsMode	Définit le mode raccourci.

domaine

Clé de registre	Description
root/domain/OU	Spécifie l'unité organisationnelle associée à l'appartenance au domaine du client léger.
root/domain/allowSmartcard	Cette clé est actuellement inutilisée.
root/domain/cacheDomainLogin	Si cette option est activée, un hachage des informations d'authentification de connexion au domaine est enregistré sur le disque afin que les connexions suivantes puissent intervenir même si le serveur Active Directory est inaccessible.
root/domain/ddns	Lorsqu'elle est activée, le client léger tente d'actualiser le serveur DNS avec son nom d'hôte et son adresse IP à chaque renouvellement de DHCP.
root/domain/domain	Spécifie le domaine auquel ce client léger est lié ou par rapport auquel il est authentifié.

Clé de registre	Description
root/domain/domainAdminGroup	Si l'option enableDomainAdmin est activée, les membres de ce groupe AD peuvent passer le client léger en mode Administrateur.
root/domain/domainControllers	Spécifie une liste séparée par des virgules de contrôleurs de domaine à utiliser avec ce domaine. Lorsqu'elle est laissée vide (recommandé), la recherche automatique de contrôleurs de domaine est effectuée en utilisant le DNS.
root/domain/domainJoined	Indique si le client léger a été formellement ajouté au domaine.
root/domain/domainUsersGroup	Si l'option enableDomainUsers est activée, les connexions au domaine sont limitées aux membres directs de ce groupe. Les groupes imbriqués sont incompatibles avec cette fonctionnalité.
root/domain/enableDomainAdmin	Si elle est définie sur 1, les membres du groupe figurant dans domainAdminGroup peuvent passer le client léger en mode Administrateur. Si elle est définie sur 0, le compte racine local doit être utilisé pour réaliser les tâches administratives locales.
root/domain/enableDomainUsers	Si elle est définie sur 1, les connexions au domaine sont limitées aux membres du groupe qui figurent dans domainUserGroup. Si elle est définie sur 0, toutes les informations d'authentification de domaine valides sont autorisées à se connecter au client léger.
root/domain/enablePasswordChange	Si elle est définie sur 1, l'utilisateur peut changer son mot de passe de domaine directement depuis le client léger.
root/domain/enableSSO	Si cette option est activée, les informations d'authentification cryptées actuelles sont mises en mémoire cache et peuvent être au démarrage de connexions distantes.
root/domain/loginAtStart	Si elle est définie sur 1 et que le client léger a été ajouté à un domaine, un écran de connexion s'affiche au démarrage du client léger. Sinon, le bureau ThinPro partagé existant est affiché au démarrage.
root/domain/retainUserRegistry	Si elle est définie sur 1, toutes les modifications personnalisées effectuées par l'utilisateur sont conservées entre les sessions de connexion.
root/domain/workgroup	Spécifie le groupe de travail ou le « domaine abrégé » associé à l'appartenance au domaine du client léger. Lors de la création du domaine Active Directory, ceci est également appelé domaine NetBIOS. Cette valeur est généralement détectée automatiquement lors de l'authentification du domaine en recherchant la valeur depuis un contrôleur de domaine.

entries

Clé de registre	Description
root/entries/<UUID>/command	
root/entries/<UUID>/folder	
root/entries/<UUID>/icon	
root/entries/<UUID>/label	
root/entries/<UUID>/metaInfo	

Clé de registre	Description
root/entries/<UUID>/onDesktop	
root/entries/<UUID>/onMenu	

pare-feu

Clé de registre	Description
root/firewall/direct/pptp-rule	
root/firewall/icmp-blocks	
root/firewall/interfaces	
root/firewall/masquerade	
root/firewall/ports	
root/firewall/services/<service>/checked	
root/firewall/services/<service>/description	
root/firewall/services/<service>/ destinations/ipv4	
root/firewall/services/<service>/ destinations/ipv6	
root/firewall/services/<service>/modules	
root/firewall/services/<service>/port- protocols	
root/firewall/services/<service>/short	
root/firewall/sources	
root/firewall/startAtBoot	

hwh264

Clé de registre	Description
root/hwh264/force2x4k	HP ne recommande pas de modifier la valeur de cette clé. Dans certaines configurations de bureau H264 Citrix, les larges flux de bureau avec deux moniteurs causent un effet de scintillement. H264 est habituellement désactivé pour les larges flux à cause de ce problème.

keyboard

Clé de registre	Description
`root/keyboard/DrawLocaleLetter`	Si la valeur est définie sur 1, l'icône de la barre d'état système du clavier crée la chaîne de paramètres régionaux de langue au lieu d'utiliser des images statiques.
`root/keyboard/SystrayMenu/keyboardLayout`	Si la clé est définie sur 1, le menu contextuel (clic droit) de l'icône de la barre d'état système du clavier propose une option permettant d'ouvrir l'outil de disposition du clavier depuis le Panneau de configuration.
`root/keyboard/SystrayMenu/languages`	Si la clé est définie sur 1, le menu contextuel (clic droit) de l'icône de la barre d'état système du clavier propose une option permettant d'ouvrir l'outil Language (Langue) depuis le Panneau de configuration.
`root/keyboard/SystrayMenu/virtualKeyboard`	Si la valeur est définie sur 1, le menu contextuel (clic droit) de l'icône de la barre d'état système du clavier propose une option permettant d'ouvrir le clavier virtuel.
`root/keyboard/VisibleInSystray`	Si la valeur est définie sur 1, l'icône de la barre d'état système du clavier s'affiche et indique la disposition du clavier actuelle.
`root/keyboard/XkbLayout`	Il s'agit d'une clé interne servant à mapper le modèle/la disposition avec une disposition de clavier XKB. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/keyboard/XkbModel`	Il s'agit d'une clé interne servant à mapper le modèle/la disposition avec un modèle de clavier XKB. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/keyboard/XkbOptions`	Il s'agit d'une clé interne servant à mapper le modèle/la disposition avec des options de clavier XKB. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/keyboard/XkbVariant`	Il s'agit d'une clé interne servant à mapper le modèle/la disposition avec une variante de clavier XKB. Vous ne devriez pas avoir besoin de modifier cette clé.
`root/keyboard/enable2`	Si la valeur est définie sur 1, il est possible de basculer vers la disposition de clavier secondaire grâce à un raccourci clavier défini par `switch`.
`root/keyboard/layout`	Permet de régler la disposition de clavier principale.
`root/keyboard/layout2`	Permet de régler la disposition de clavier secondaire.
`root/keyboard/model`	Définit le modèle de clavier principal.
`root/keyboard/model2`	Définit le modèle de clavier secondaire.
`root/keyboard/numlock`	Si la clé est réglée sur 1, la fonction Verrouillage numérique est activée au démarrage du système. Cette clé de registre est ignorée intentionnellement sur les clients légers mobiles.
`root/keyboard/switch`	Définit le raccourci clavier pour basculer entre la première et la seconde disposition de clavier (`enable2` doit également être défini sur 1). Les valeurs valides sont les suivantes : `grp:ctrl_shift_toggle`, `grp:ctrl_alt_toggle`, `grp:alt_shift_toggle`.
`root/keyboard/variant`	Définit la variante de clavier principale.
`root/keyboard/variant2`	Définit la variante de clavier secondaire.

licence

Clé de registre	Description
`root/license/courtesyNotificationEnable`	Si la valeur est définie sur 1, les notifications de la barre des tâches sont activées lorsque l'expiration de licence approche.
`root/license/courtesyNotificationInterval`	Si positif, le nombre d'heures entre les notifications de courtoisie.
`root/license/courtesyNotificationStart`	Si le résultat est positif, les notifications de courtoisie commencent plusieurs jours avant l'expiration.
`root/license/courtesyNotificationText`	S'il n'est pas vide, ce texte est utilisé dans les notifications de courtoisie. % 1 est remplacé par le nombre de jours restants avant l'expiration ; % 2 est remplacé par la date d'expiration.
`root/license/watermark`	Cette valeur est en lecture seule.

logging

Clé de registre	Description
`root/logging/general/debugLevel`	Définit le niveau de débogage. Cette valeur sera soutenue par les autres modules pour générer les journaux correspondants.
`root/logging/general/showDebugLevelBox`	Si la clé est définie sur 1, l'option **Debug Level** (Niveau de débogage) de l'onglet **Journaux système** de la fenêtre **Informations système** sera disponible pour les utilisateurs standard. En cas de réglage à 0, l'option est disponible pour les administrateurs uniquement.

login

Clé de registre	Description
`root/login/buttons/configure/authorized`	Si la valeur est définie sur 1, le bouton de configuration est disponible dans l'écran de connexion.
`root/login/buttons/info/authorized`	Si la valeur est définie sur 1, le bouton d'informations système est disponible dans l'écran de connexion.
`root/login/buttons/keyboard/authorized`	Si la valeur est définie sur 1, les paramètres de disposition du clavier peuvent être configurés dans l'écran de connexion.
`root/login/buttons/locale/authorized`	Si la valeur est définie sur 1, les paramètres de langue peuvent être configurés dans l'écran de connexion.
`root/login/buttons/mouse/authorized`	Si la valeur est définie sur 1, les paramètres de la souris peuvent être configurés dans l'écran de connexion.
`root/login/buttons/onscreenKeyboard/authorized`	Si la valeur est définie sur 1, le clavier à l'écran est disponible dans l'écran de connexion.
`root/login/buttons/power/authorized`	Si la valeur est définie sur 1, le bouton d'alimentation est disponible dans l'écran de connexion.
`root/login/buttons/poweroff/authorized`	Si la valeur est définie sur 1, la fonction d'arrêt est disponible dans l'écran de connexion.

Clé de registre	Description
root/login/buttons/reboot/authorized	Si la valeur est définie sur 1, la fonction de redémarrage est disponible dans l'écran de connexion.
root/login/buttons/show/authorized	Si la valeur est définie sur 1, le tiroir de boutons contenant des options supplémentaires est disponible dans l'écran de connexion.
root/login/buttons/sleep/authorized	Si la valeur est définie sur 1, la fonction de veille est disponible dans l'écran de connexion.
root/login/buttons/touchscreen/authorized	Si la valeur est définie sur 1, les paramètres de l'écran tactile peuvent être configurés dans l'écran de connexion. La clé de registre root/touchscreen/enabled doit également être activée.
root/login/rememberedDomain	
root/login/rememberedUser	

mouse

Clé de registre	Description
root/mouse/MouseHandedness	Si la valeur est définie sur 0, la souris est configurée pour les droitiers. Si la valeur est définie sur 1, la souris est configurée pour les gauchers.
root/mouse/MouseSpeed	Définit l'accélération du pointeur de la souris. La plage utile s'étend normalement de 0 à 25. Une valeur de 0 désactive complètement l'accélération, le pointeur se déplaçant alors à une vitesse lente, mais sensible.
root/mouse/MouseThreshold	Définit le nombre de pixels avant l'activation de l'accélération de la souris. Une valeur de 0 règle l'accélération de telle sorte qu'elle augmente peu à peu, ce qui permet des mouvements à la fois rapides et précis.
root/mouse/disableTrackpadWhileTyping	Si la valeur est réglée sur 1, le pavé tactile est temporairement désactivé lors de la saisie. Si la valeur est réglée sur 0, le pavé tactile n'est pas temporairement désactivé lors de la saisie.
root/mouse/enableNaturalScrolling	Si la valeur est définie sur 1 (par défaut), le défilement normal est activé sur le pavé tactile. Si la valeur est définie sur 0, le défilement normal est désactivé sur le pavé tactile.
root/mouse/enableTrackpad	Si la valeur est définie sur 1, le pavé tactile est activé. Si la valeur est définie sur 0, le pavé tactile est désactivé.
root/mouse/enableTrackpadTapping	Si la valeur est définie sur 0 (valeur par défaut), le comportement taper-pour-cliquer du pavé tactile est désactivé. Si définie sur 1, le comportement taper-pour-cliquer est activé.
root/mouse/enableTwoFingerScrolling	Si la valeur est définie sur 1 (par défaut), le défilement à deux doigts est activé sur le pavé tactile. Si la valeur est définie sur 0, le défilement à deux doigts est désactivé sur le pavé tactile.
root/mouse/gui	

restore-points

Clé de registre	Description
`root/restore-points/factory`	Spécifie les instantanés à utiliser pour une réinitialisation des paramètres d'usine.

screensaver

Clé de registre	Description
`root/screensaver/SlideShowAllMonitors`	Si la valeur est définie sur 1, la diapo de l'écran de veille sera affichée sur tous les écrans. Si défini sur 0, la diapo indiquée s'affichera sur l'écran principal uniquement.
`root/screensaver/SlideShowInterval`	Définit l'intervalle en secondes pour le changement des images dans l'écran de veille.
`root/screensaver/SlideShowPath`	Spécifie le répertoire contenant les images du diaporama de l'écran de veille.
`root/screensaver/buttons/configure/authorized`	Si la valeur est définie sur 1, le bouton de configuration est disponible lorsque l'écran est verrouillé.
`root/screensaver/buttons/info/authorized`	Si la valeur est définie sur 1, le bouton d'informations système est disponible lorsque l'écran est verrouillé.
`root/screensaver/buttons/keyboard/authorized`	Si la valeur est définie sur 1, les paramètres de disposition du clavier peuvent être configurés lorsque l'écran est verrouillé.
`root/screensaver/buttons/locale/authorized`	Si la valeur est définie sur 1, les paramètres de langue peuvent être configurés lorsque l'écran est verrouillé.
`root/screensaver/buttons/mouse/authorized`	Si la valeur est définie sur 1, les paramètres de la souris peuvent être configurés lorsque l'écran est verrouillé.
`root/screensaver/buttons/onscreenKeyboard/authorized`	Si la valeur est définie sur 1, le clavier à l'écran est disponible lorsque l'écran est verrouillé.
`root/screensaver/buttons/power/authorized`	Si la valeur est définie sur 1, le bouton d'alimentation est disponible lorsque l'écran est verrouillé.
`root/screensaver/buttons/poweroff/authorized`	Si la valeur est définie sur 1, la fonction d'arrêt est disponible lorsque l'écran est verrouillé.
`root/screensaver/buttons/reboot/authorized`	Si la valeur est définie sur 1, la fonction de redémarrage est disponible lorsque l'écran est verrouillé.
`root/screensaver/buttons/show/authorized`	Si la valeur est définie sur 1, le tiroir de boutons contenant des options supplémentaires est disponible lorsque l'écran est verrouillé.
`root/screensaver/buttons/sleep/authorized`	Si la valeur est définie sur 1, la fonction de veille est disponible lorsque l'écran est verrouillé.
`root/screensaver/buttons/touchscreen/authorized`	Si la valeur est définie sur 1, les paramètres de l'écran tactile peuvent être configurés lorsque l'écran est verrouillé. La clé de registre `root/touchscreen/enabled` doit également être activée.
`root/screensaver/enableCustomLogo`	Si la valeur est définie sur 1, l'image personnalisée définie dans `logoPath` est utilisée pour l'écran de veille.

Clé de registre	Description
`root/screensaver/enableDPMS`	Si la valeur est définie sur 0, la gestion de l'alimentation du moniteur est désactivée. Avec ce paramétrage, le moniteur reste allumé tant qu'il n'est pas éteint manuellement.
`root/screensaver/enableScreensaver`	Si la valeur est définie sur 1, l'écran de veille est activé.
`root/screensaver/enableSleep`	Si la valeur est définie sur 1, le mode veille est activé.
`root/screensaver/lockScreen`	Si la valeur est définie sur 1 et que vous êtes connecté en mode Administrateur, un mot de passe est nécessaire pour retourner sur le bureau depuis l'écran de veille.
`root/screensaver/lockScreenDomain`	Si la valeur est définie sur 1 et que le système est en mode domaine, un mot de passe est nécessaire pour retourner sur le bureau depuis l'écran de veille.
`root/screensaver/lockScreenUser`	Si la valeur est définie sur 1 et que vous n'êtes pas connecté en mode Administrateur et que le système n'est pas en mode domaine, un mot de passe est nécessaire pour retourner sur le bureau depuis l'écran de veille.
`root/screensaver/logoPath`	Définit le chemin d'accès d'une image personnalisée à utiliser pour l'écran de veille.
`root/screensaver/mode`	Définit le mode de rendu de l'image de l'écran de veille (par exemple, `Center`, `Tile`, `Expand` et `Stretch`). Si la valeur est définie sur `Default`, l'image s'affiche sans aucun traitement. Si défini sur `slideshow (diaporama)`, l'écran de veille parcourra les images dans le répertoire spécifié par `SlideShowPath`.
`root/screensaver/off`	Définit le délai d'inactivité en minutes avant la mise hors tension du moniteur.
`root/screensaver/origImageCopyPath`	Il s'agit du chemin d'accès où l'image personnalisée est enregistrée lorsque le `mode` est défini sur `Default`.
`root/screensaver/solidColor`	Si `useSolidColor` est activé et `enableCustomLogo` est désactivé, cette couleur unie est utilisée pour l'économiseur d'écran.
`root/screensaver/standby`	Définit le délai d'inactivité en minutes avant la mise en veille (standby) du moniteur.
`root/screensaver/suspend`	Définit le délai d'inactivité en minutes avant la mise en veille (suspend) du moniteur.
`root/screensaver/timeoutScreensaver`	Définit le délai d'inactivité en minutes avant le démarrage de l'écran de veille.
`root/screensaver/timeoutSleep`	Définit le délai d'inactivité en minutes avant la mise en veille du client léger.
`root/screensaver/useSolidColor`	Si la valeur est définie sur 1 et `enableCustomLogo` est désactivé, la valeur de la clé `solidColor` est utilisée par l'économiseur d'écran.

security

Clé de registre	Description
`root/security/SecurityFeaturs/SpeculativeStoreBypassControl`	Contrôle si les mesures d'atténuation pour Speculative Store Bypass (CVE-2018-3639) sont activées. Par défaut, les mesures d'atténuation sont activées. Pour les activer, définissez la valeur de la clé sur « activé ». Pour que toute modification de cette clé prenne effet, redémarrez l'ordinateur.
`root/security/authenticationFailDelay`	Définit le délai approximatif, en millisecondes, après une tentative de connexion échouée. Le délai réel varie de plus ou moins 25 % de cette valeur. Par exemple, utilisez une valeur de 3 000 pour obtenir un délai d'environ 3 secondes.
`root/security/domainEntryMode`	Si la valeur est définie sur 1, le domaine doit être saisi dans un champ de texte distinct libellé **Domaine**. Si elle est définie sur 0, le domaine saisi doit faire partie du champ **User**.
`root/security/enableLockOverride`	Si la valeur est définie sur 1, les administrateurs peuvent neutraliser le verrouillage de l'écran d'un bureau local.
`root/security/enableSecretPeek`	Si la valeur est définie sur 1, les boîtes de dialogue de mot de passe et PIN sont dotées d'un bouton qui affiche le mot de passe/pin saisi en texte clair lorsqu'il est sélectionné.
`root/security/encryption/identity/encryptedSecretCipher`	Définit l'algorithme pour le cryptage symétrique d'un secret. Tous les algorithmes utilisent une quantité appropriée de salt aléatoires, qui est régénérée chaque fois que le secret est stocké. La clé de cryptage est différente sur chaque client léger et les fonctions de cryptage et décryptage ne sont disponibles que pour les programmes autorisés. La liste de chiffrage compatible inclut la plupart des chiffrages OpenSSL et ChaCha20–Poly1305.
`root/security/encryption/identity/encryptedSecretTTL`	Définit le nombre de secondes depuis la dernière connexion réussie pour qu'un secret crypté stocké soit considéré comme valide. Si la valeur est négative, les secrets cryptés ne sont pas assujettis à temporisation.
`root/security/encryption/identity/encryptedSecretTTLnonSSO`	Spécifie le nombre de secondes qu'un secret crypté non-SSO enregistré est considéré comme valide. Si la valeur est non-positive, les secrets cryptés ne sont pas assujettis à temporisation.
`root/security/encryption/identity/secretHashAlgorithm`	Définit l'algorithme pour créer le hachage d'un secret. Les fonctions de dérivation de clé (KDF) comme scrypt ou argon2 sont préférables aux hachages directs car le calcul d'un dictionnaire arc-en-ciel n'est pas rapide en utilisant une KDF. Tous les algorithmes utilisent une quantité appropriée de grains de sel aléatoires, qui est régénérée chaque fois que le secret est haché. La liste compatible inclut scrypt, Argon2, SHA-256 et SHA-512 (bien que les deux derniers ne soient pas des KDF).
`root/security/encryption/identity/secretHashTTL`	Définit le nombre de secondes depuis la dernière connexion réussie pour que des hachages de secret stockés soient considérés comme valides. Si la valeur est négative, les hachages de secrets ne sont pas assujettis à temporisation.
`root/security/mustLogin`	Si la valeur est définie sur 1, tous les utilisateurs sont forcés d'ouvrir une session pour accéder au bureau.

shutdown

Clé de registre	Description
`root/shutdown/enableAutomaticShutdownTimeout`	Si la valeur est définie sur 1, une barre de progression s'affiche dans la boîte de dialogue de confirmation d'arrêt/redémarrage/déconnexion. Si la question ne reçoit pas de réponse à temps, l'arrêt/redémarrage/déconnexion est automatique.
`root/shutdown/timeOfAutomaticShutdownTimeout`	Définit le temps d'attente pour la temporisation d'arrêt automatique.

sshd

Clé de registre	Description
`root/sshd/disableWeakCipher`	Si la valeur est définie sur 1, désactivez le chiffrage en mode CBC et les autres chiffrages faibles connus, comme 3DES, arcfour, etc.
`root/sshd/disableWeakHmac`	Si la valeur est définie sur 1, désactivez hmac 96 bits et tous les hmac basés sur sha1 et md5.
`root/sshd/disableWeakKex`	Si la valeur est définie sur 1, désactivez les algorithmes d'échange de clé qui contiennent DH avec SHA1.
`root/sshd/enabled`	Si la valeur est définie sur 1, le démon SSH est activé et le client léger est accessible via SSH.
`root/sshd/userAccess`	Si la clé est définie sur 1, les utilisateurs finaux peuvent se connecter au client léger via SSH.

time

Clé de registre	Description
`root/time/NTPServers`	Spécifie les serveurs NTP à utiliser via une liste séparée par des virgules. Les serveurs NTP privés ou les grands clusters NTP virtuels, tels que `pool.ntp.org`, sont les meilleures options pour minimiser la charge du serveur. Effacez cette valeur pour revenir à l'utilisation des serveurs DHCP (balise 42) au lieu d'une liste fixe.
`root/time/dateFormatLong`	Méthode facultative de neutralisation du format de date longue utilisée dans différents outils ThinPro. Pour le formatage, effectuez une recherche en ligne de `QDate::toString`. Si la valeur est laissée vide, une chaîne spécifique locale est généralement utilisée.
`root/time/dateFormatShort`	Méthode facultative de neutralisation du format de date courte utilisée dans différents outils ThinPro. Pour le formatage, effectuez une recherche en ligne de `QDate::toString`. Si la valeur est laissée vide, une chaîne spécifique locale est généralement utilisée.
`root/time/dateTimeFormatLong`	Méthode facultative de neutralisation du format de date et heure longues utilisées dans différents outils ThinPro. Pour le formatage, effectuez une recherche en ligne de

Clé de registre	Description
	`QDate::toString`. Si la valeur est laissée vide, une chaîne spécifique locale est généralement utilisée.
`root/time/dateTimeFormatShort`	Méthode facultative de neutralisation du format de date et heure courtes utilisées dans différents outils ThinPro. Pour le formatage, effectuez une recherche en ligne de `QDate::toString`. Si la valeur est laissée vide, une chaîne spécifique locale est généralement utilisée.
`root/time/hideCountries`	Liste séparée par des points-virgules des pays que vous souhaitez masquer dans l'IGU de sélection du fuseau horaire.
`root/time/hideMap`	Si la valeur est définie sur 1, la carte n'est pas dessinée. Cette approche peut être préférable dans les cas où les limites sont problématiques.
`root/time/hideWinZones`	Liste séparée par des points-virgules des fuseaux horaires au format Windows, comme « (UTC+2:00) Tripoli » que vous souhaitez masquer dans l'IGU de sélection du fuseau horaire.
`root/time/hideZones`	Liste séparée par des points-virgules des fuseaux horaires au format Linux, comme « Amérique/Denver » que vous souhaitez masquer dans l'IGU de sélection du fuseau horaire.
`root/time/timeFormatLong`	Méthode facultative de neutralisation du format d'heure longue utilisée dans différents outils ThinPro. Pour le formatage, effectuez une recherche en ligne de `QDate::toString`. Si la valeur est laissée vide, une chaîne spécifique locale est généralement utilisée.
`root/time/timeFormatShort`	Méthode facultative de neutralisation du format d'heure courte utilisée dans différents outils ThinPro. Pour le formatage, effectuez une recherche en ligne de `QDate::toString`. Si la valeur est laissée vide, une chaîne spécifique locale est généralement utilisée.
`root/time/timezone`	Définit le fuseau horaire. Les fuseaux horaires doivent être indiqués au format défini par **Fuseau horaire Linux** dans l'outil **Date et heure** du Panneau de configuration comme suit : `<région>/<sous-région>`
`root/time/use24HourFormat`	Si la valeur est définie sur -1, le système choisit le format automatiquement selon les paramètres régionaux. Si la valeur est définie sur 0, le format AM/PM est utilisé. Si la valeur est définie sur 1, le format 24 heures est utilisé.
`root/time/useADDNSTimeServers`	Si la valeur est définie sur 1, le client léger tente de définir le fuseau horaire découvert automatiquement sur le réseau local via les contrôleurs de domaine Active Directory. Pour ce faire, il utilise la requête DNS suivante pour les enregistrements SRV : `_ldap._tcp.dc._msdcs.domain`.
`root/time/useDHCPTimezone`	Si la valeur est définie sur 1, le client léger tente de définir le fuseau horaire via DHCP. Pour définir convenablement le fuseau horaire au moyen de cette clé de registre, assurez-vous que le serveur DHCP du client léger transmet la balise DHCP `tcode` (généralement la balise 101, mais les balises 100 et 2 fonctionnent également).
`root/time/useNTPServers`	Si la valeur est définie sur 1, l'utilisation de serveurs de temps NTP pour synchroniser l'horloge du client léger est activée. Si cette option est activée, assurez-vous qu'un serveur NTP est spécifié via DHCP ou via la clé `NTPServers`.

touchscreen

Clé de registre	Description
root/touchscreen/beep	Définit si le client léger émet un signal sonore lorsque l'écran tactile est utilisé.
root/touchscreen/calibrated	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/touchscreen/enabled	Si la valeur est définie sur 1, l'entrée tactile est activée.
root/touchscreen/maxx	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/touchscreen/maxy	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/touchscreen/minx	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/touchscreen/miny	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/touchscreen/port	Spécifie le port connecté à l'écran tactile.
root/touchscreen/swapx	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/touchscreen/swapy	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/touchscreen/type	Spécifie le type de contrôleur de l'écran tactile.

translation

Clé de registre	Description
root/translation/coreSettings/localeMapping/<LanguageCode>	Il s'agit de clés internes utilisées pour fournir la chaîne de texte en regard de la langue appropriée sur le sélecteur de langue. Vous ne devriez pas avoir besoin de modifier ces clés.
root/translation/coreSettings/localeSettings	Définit les paramètres régionaux pour le client léger. Ceux-ci sont également transmis à la connexion à distance. Les valeurs possibles sont en_US (anglais), de_DE (allemand), es_ES (espagnol), fr_FR (français), ru_RU (russe), ja_JP (japonais), ko_KR (coréen), zh_CN (chinois simplifié) et zh_TW (chinois traditionnel).
root/translation/gui/LocaleManager/name	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/translation/gui/LocaleManager/status	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/translation/gui/LocaleManager/title	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
root/translation/gui/LocaleManager/widgets/localeSettings	Contrôle l'état du widget des paramètres régionaux dans l'outil des langues. Si la clé est définie sur active, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé

Clé de registre	Description
	est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.

usb-update

Clé de registre	Description
`root/usb-update/authentication`	Si la valeur est définie sur 1, un mot de passe administrateur est nécessaire pour effectuer les mises à jour USB.
`root/usb-update/enable`	Si la valeur est définie sur 1, la détection automatique des mises à jour USB est activée.
`root/usb-update/height`	Permet de régler la hauteur de la fenêtre de Mise à jour USB en pixels.
`root/usb-update/searchMaxDepth`	Définit la profondeur des sous-répertoires à explorer pour les mises à jour. Une profondeur de recherche élevée peut entraîner des retards sur les unités flash USB disposant de milliers de répertoires.
`root/usb-update/width`	La largeur de la fenêtre de Mise à jour USB en pixels.

users

Clé de registre	Description
`root/users/root/enablePassword`	Lorsqu'elle est activée, les connexions au compte administrateur racine local sont activées. Si elle est désactivée, seuls les administrateurs Active Directory peuvent passer le client léger en mode Administrateur.
`root/users/root/password`	Définit le mot de passe administrateur. S'il est vide, le mode Administrateur est verrouillé.
`root/users/root/timeout`	Spécifie la temporisation d'attente (en minutes) après laquelle le mode Administrateur se termine. Si la valeur est égale ou inférieure à 0, le mode Administrateur ne se termine jamais.
`root/users/user/SSO`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/users/user/WOL`	Si la valeur est définie sur 1, le Wake-On-LAN (WOL) est activé.
`root/users/user/XHostCheck`	Si la valeur est définie sur 1, seuls les systèmes répertoriées sous `root/users/user/xhosts` sont autorisés à contrôler le client léger à distance.
`root/users/user/apps/hptc-ad-change-password/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Change Domain Password** (Changer le mot de passe du domaine) du Panneau de configuration.
`root/users/user/apps/hptc-ad-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Active Directory** du Panneau de configuration.
`root/users/user/apps/hptc-agent-mgr/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Agent HPDM** du Panneau de configuration.

Clé de registre	Description
`root/users/user/apps/hptc-auto-update/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Automatique Update** (Mise à jour automatique) du Panneau de configuration.
`root/users/user/apps/hptc-background-mgr/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Gestionnaire d'arrière-plan** du Panneau de configuration.
`root/users/user/apps/hptc-cert-mgr/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Gestionnaire des certificats** du Panneau de configuration.
`root/users/user/apps/hptc-compatibility/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Vérification de la compatibilité** du Panneau de configuration.
`root/users/user/apps/hptc-component-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Component Manager** (Gestionnaire de composant) du Panneau de configuration.
`root/users/user/apps/hptc-config-wizard/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Initial Setup Wizard** (Assistant de configuration initiale) du menu Démarrer.
`root/users/user/apps/hptc-connection-wizard/authorized`	Si la valeur est définie sur 1, les utilisateurs finaux peuvent accéder à **Create a Connection** (Créer une connexion).
`root/users/user/apps/hptc-control-panel/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder au **Panneau de configuration**.
`root/users/user/apps/hptc-date-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Date and Time** (Date et heure) du Panneau de configuration.
`root/users/user/apps/hptc-dhcp-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **DHCP Options** (Options DHCP) du Panneau de configuration.
`root/users/user/apps/hptc-display-prefs/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Display** (Affichage) du Panneau de configuration.
`root/users/user/apps/hptc-easy-update/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Mise à jour simplifiée** du Panneau de configuration.
`root/users/user/apps/hptc-factory-reset/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Factory Reset** (Réinitialisation d'usine) du Panneau de configuration.
`root/users/user/apps/hptc-firewalld-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Firewall Manager** (Gestionnaire de pare-feu) du Panneau de configuration.
`root/users/user/apps/hptc-i18n-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Language** (Langue) du Panneau de configuration.
`root/users/user/apps/hptc-ibus-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Méthode d'entrée Ibus** du Panneau de configuration.
`root/users/user/apps/hptc-imprivata-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Imprivata Setup** (Configuration Imprivata) du Panneau de configuration.
`root/users/user/apps/hptc-keyboard-layout/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Keyboard Layout** (Disposition du clavier) du Panneau de configuration.
`root/users/user/apps/hptc-kiosk/authorized`	Si la valeur est définie sur 1, les utilisateurs finaux peuvent accéder à **Connection Manager** (Gestionnaire de connexion).

Clé de registre	Description
`root/users/user/apps/hptc-licenses/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **HP License Agreement** (Accord de licence HP).
`root/users/user/apps/hptc-mixer/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Sound** (Son) du Panneau de configuration.
`root/users/user/apps/hptc-mouse/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Souris** du Panneau de configuration.
`root/users/user/apps/hptc-network-mgr/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Gestionnaire réseau** du Panneau de configuration.
`root/users/user/apps/hptc-power-mgr/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Gestionnaire d'alimentation** du Panneau de configuration.
`root/users/user/apps/hptc-printer-mgr/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Imprimantes** du Panneau de configuration.
`root/users/user/apps/hptc-regeditor/authorized`	Si la valeur est définie sur 1, les utilisateurs finaux peuvent accéder à **Registry Editor** (Éditeur de registre).
`root/users/user/apps/hptc-restore/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Snapshots** (Instantanés) du Panneau de configuration.
`root/users/user/apps/hptc-scep-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **SCEP Manager** (Gestionnaire SSHD) du Panneau de configuration.
`root/users/user/apps/hptc-security/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Sécurité** du Panneau de configuration.
`root/users/user/apps/hptc-serial-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Serial Manager** (Gestionnaire de série) du Panneau de configuration.
`root/users/user/apps/hptc-shortcut-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Keyboard Shortcuts** (Raccourcis clavier) du Panneau de configuration.
`root/users/user/apps/hptc-snipping-tool/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Snipping Tool** (Outil Capture) du menu Démarrer.
`root/users/user/apps/hptc-sshd-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **SSHD Manager** (Gestionnaire SSHD) du Panneau de configuration.
`root/users/user/apps/hptc-switch-admin/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Switch to Administrator/User** (Basculer en Administrateur/Utilisateur).
`root/users/user/apps/hptc-sysinfo/authorized`	dSi la valeur est définie sur 1, les utilisateurs finaux peuvent accéder à **System Information** (Informations système).
`root/users/user/apps/hptc-task-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Task Manager** (Gestionnaire des tâches) du menu Démarrer.
`root/users/user/apps/hptc-text-editor/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Text Editor** (Éditeur de texte) du menu Démarrer.
`root/users/user/apps/hptc-thinstate/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **ThinState** du Panneau de configuration.
`root/users/user/apps/hptc-touchscreen/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Écran tactile** du Panneau de configuration.
`root/users/user/apps/hptc-update/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Check for Updates** (Rechercher des mises à jour).

Clé de registre	Description
`root/users/user/apps/hptc-usb-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **USB Manager** (Gestionnaire SSHD) du Panneau de configuration.
`root/users/user/apps/hptc-user-rights/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **Customization Center** (Centre de personnalisation) du Panneau de configuration.
`root/users/user/apps/hptc-vncshadow/authorized`	Si la clé est définie sur 1, les utilisateurs finaux peuvent accéder à l'élément **VNC Shadow** du Panneau de configuration.
`root/users/user/apps/hptc-wlsstat/authorized`	Si la valeur est définie sur 1, les utilisateurs finaux peuvent accéder à **Wireless Statistics** (Statistiques sans-fil).
`root/users/user/apps/hptc-xen-general-mgr/authorized`	Si définie sur 1, les utilisateurs finaux peuvent accéder aux paramètres généraux Citrix.
`root/users/user/apps/hptc-xterm/authorized`	Si la valeur est définie sur 1, les utilisateurs finaux peuvent accéder à **X Terminal** (Terminal X). **ATTENTION :** L'activation de l'accès au terminal X constitue un risque de sécurité et est déconseillé dans un environnement de production. Le terminal X doit uniquement être activé lors du débogage dans un environnement protégé hors production.
`root/users/user/desktopScaling`	Indique le pourcentage pour augmenter ou diminuer la taille des éléments du bureau. Si la valeur est définie sur 100 (par défaut), la mise à l'échelle standard est utilisée. Si la valeur est définie sur 50, la moitié de la taille de mise à l'échelle standard est utilisée. Si la valeur est définie sur 200, le double de la taille de mise à l'échelle standard est utilisée.
`root/users/user/enablePassword`	Lorsqu'elle est activée, les connexions au compte partagé local `utilisateur` sont activées.
`root/users/user/hideDesktopPanel`	Si la valeur est définie sur 1, les panneaux de bureau comme la barre des tâches ne sont pas démarrés ou affichés sur le bureau.
`root/users/user/kioskMode`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/users/user/launchConnectionManager`	Si la clé est définie sur 1, le gestionnaire de connexion se lance au démarrage du système.
`root/users/user/rightclick`	Si la valeur est définie sur 1, le menu contextuel (clic droit) du bureau est activé.
`root/users/user/ssoconnectiontype`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/users/user/switchAdmin`	Si la clé est définie sur 1, le basculement en mode Administrateur est activé.
`root/users/user/theme`	Réservé à une utilisation ultérieure.
`root/users/user/xhosts/<UUID>/xhost`	Spécifie l'adresse IP ou le nom d'hôte d'un système qui est autorisé à contrôler à distance le client léger lorsque `XHostCheck` est activé.

vncserver

Clé de registre	Description
`root/vncserver/coreSettings/enableVncShadow`	Si la valeur est définie sur 1, le serveur utilisé pour le contrôle à distance VNC du client léger est activé.
`root/vncserver/coreSettings/userNotificationMessage`	Définit le message de notification qui s'affiche à l'écran lorsque quelqu'un tente de se connecter au client léger à l'aide de VNC.
`root/vncserver/coreSettings/vncAllowLoopbackOnly`	Si la valeur est définie sur 1, seule une adresse d'hôte local ou de boucle est autorisée pour les connexions VNC.
`root/vncserver/coreSettings/vncDefaultNumLockStatus`	Si la valeur est définie sur 1, le verrouillage numérique est activé par défaut. Si la valeur est définie sur 0, le verrouillage numérique est désactivé par défaut.
`root/vncserver/coreSettings/vncNotifyShowTimeout`	Si la valeur est définie sur 1, une délai d'expiration est appliqué à la boîte de dialogue de notification qui s'affiche à l'écran lorsque quelqu'un tente de se connecter au client léger à l'aide de VNC.
`root/vncserver/coreSettings/vncNotifyTimeout`	Définit le délai d'expiration en secondes de la boîte de dialogue de notification qui s'affiche à l'écran lorsque quelqu'un tente de se connecter au client léger à l'aide de VNC.
`root/vncserver/coreSettings/vncNotifyUser`	Si la valeur est définie sur 1, une notification s'affiche à l'écran lorsque quelqu'un tente de se connecter au client léger à l'aide de VNC.
`root/vncserver/coreSettings/vncPassword`	Définit le mot de passe pour le contrôle à distance VNC. La clé `vncUsePassword` doit également être activée.
`root/vncserver/coreSettings/vncReadOnly`	Si la valeur est définie sur 1, le contrôle à distance VNC fonctionne en mode affichage uniquement.
`root/vncserver/coreSettings/vncRefuseInDefault`	Si la valeur est définie sur 1, les requêtes VNC sont refusées automatiquement si l'utilisateur n'interagit pas avec la boîte de dialogue de notification avant l'expiration du délai.
`root/vncserver/coreSettings/vncStopButton`	Si la valeur est définie sur 1, un bouton toujours en haut s'affiche dans le coin gauche de l'écran. Sélectionner ce bouton déconnecte la session VNC.
`root/vncserver/coreSettings/vncTakeEffectRightNow`	Si la valeur est définie sur 1, les paramètres VNC prennent effet immédiatement après avoir modifiés.
`root/vncserver/coreSettings/vncUseHTTP`	Si la valeur est définie sur 1, le port HTTP 5800 est ouvert pour les connexions VNC.
`root/vncserver/coreSettings/vncUsePassword`	Si la valeur est définie sur 1, le mot de passe spécifié dans `vncPassword` est requis pour le contrôle à distance VNC.
`root/vncserver/coreSettings/vncUseSSL`	Si la valeur est définie sur 1, SSL est utilisé pour les connexions VNC.
`root/vncserver/gui/VNCShadowManager/name`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/vncserver/gui/VNCShadowManager/status`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/vncserver/gui/VNCShadowManager/title`	Cette clé de registre est utilisée en interne ou réservée pour une utilisation ultérieure. Sa valeur ne doit pas être modifiée.
`root/vncserver/gui/VNCShadowManager/widgets/enableVncShadow`	Contrôle l'état du widget **Activer VNC Shadow** dans l'outil VNC Shadow. Si la clé est définie sur `active`, le widget est visible

Clé de registre	Description
	dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/vncserver/gui/VNCShadowManager/widgets/userNotificationMessage`	Contrôle l'état du widget **Message de notification de l'utilisateur** dans l'outil VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/vncserver/gui/vncAllowLoopbackOnly`	Contrôle l'état du widget **Autoriser uniquement les connexions en boucle** dans l'utilitaire VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut interagir avec. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `lecture seule`, le widget est visible en lecture seule.
`root/vncserver/gui/VNCShadowManager/widgets/vncNotifyShowTimeout`	Contrôle l'état du widget **Durée d'affichage de la notification VNC** dans l'outil VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/vncserver/gui/VNCShadowManager/widgets/vncNotifyTimeout`	Contrôle l'état du widget numérique dans l'outil VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/vncserver/gui/VNCShadowManager/widgets/vncNotifyUser`	Contrôle l'état du widget **VNC prévient l'utilisateur pour lui permettre de refuser** dans l'outil VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/vncserver/gui/VNCShadowManager/widgets/vncPassword`	Contrôle l'état du widget **Définir le mot de passe** dans l'outil VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/vncserver/gui/VNCShadowManager/widgets/vncReadOnly`	Contrôle l'état du widget **VNC en lecture seule** dans l'outil VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/vncserver/gui/VNCShadowManager/widgets/vncRefuseInDefault`	Contrôle l'état du widget **Refuser les connexions par défaut** dans l'outil VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/vncserver/gui/vncStopButton`	Contrôle l'état du widget **bouton VNC Stop Shadow** dans l'utilitaire VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut interagir avec. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `lecture seule`, le widget est visible en lecture seule.

Clé de registre	Description
`root/vncserver/gui/VNCShadowManager/widgets/vncTakeEffectRightNow`	Contrôle l'état du widget **Réinitialiser le serveur VNC maintenant** dans l'outil VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.
`root/vncserver/gui/VNCShadowManager/widgets/vncUseHTTP`	Contrôle l'état du widget **VNC Use HTTP Port 5800** dans l'outil VNC Shadow. Si définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut interagir avec. Si définie sur `inactive`, le widget est masqué. Si définie sur `lecture seule`, le widget est visible en lecture seule.
`root/vncserver/gui/VNCShadowManager/widgets/vncUsePassword`	Contrôle l'état du widget **VNC Use Password** (VNC utilise un mot de passe) dans l'outil VNC Shadow. Si définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut interagir avec. Si définie sur `inactive`, le widget est masqué. Si définie sur `lecture seule`, le widget est visible en lecture seule.
`root/vncserver/gui/VNCShadowManager/widgets/vncUseSSL`	Contrôle l'état du widget **VNC utilise SSL** dans l'outil VNC Shadow. Si la clé est définie sur `active`, le widget est visible dans l'interface utilisateur et l'utilisateur peut l'utiliser. Si la clé est définie sur `inactive`, le widget est masqué. Si la clé est définie sur `read-only`, le widget est visible en lecture seule.

zero-login

Clé de registre	Description
`root/zero-login/buttons/configure/authorized`	Si la valeur est définie sur 1, le bouton **Configurer** est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.
`root/zero-login/buttons/info/authorized`	Si la valeur est définie sur 1, le bouton **Informations sur le système** est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.
`root/zero-login/buttons/keyboard/authorized`	Si la valeur est définie sur 1, la sélection **Disposition du clavier** est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.
`root/zero-login/buttons/locale/authorized`	Si la valeur est définie sur 1, la sélection **Locale** est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.
`root/zero-login/buttons/mouse/authorized`	Si la valeur est définie sur 1, la sélection **Souris** est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.
`root/zero-login/buttons/onscreenKeyboard/authorized`	Si la valeur est définie sur 1, l'option de clavier à l'écran est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.
`root/zero-login/buttons/power/authorized`	Si la valeur est définie sur 1, le bouton **Alimentation** est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.

Clé de registre	Description
`root/zero-login/buttons/poweroff/authorized`	Si la valeur est définie sur 1, l'option **Extinction** est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.
`root/zero-login/buttons/reboot/authorized`	Si la valeur est définie sur 1, l'option **Redémarrer** est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.
`root/zero-login/buttons/show/authorized`	Si la valeur est définie sur 1, les boutons sont affichés dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.
`root/zero-login/buttons/sleep/authorized`	Si la valeur est définie sur 1, l'option **Veille** est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion.
`root/zero-login/buttons/touchscreen/authorized`	Si la valeur est définie sur 1, la sélection **Écran tactile** est disponible dans la boîte de dialogue Informations d'identification Smart Zero ou de connexion. **REMARQUE :** La clé `root/touchscreen/enabled` doit également être définie.

Index

R

S

T

V

X