# Application Citrix Workspace pour Android

## Contents



# Application Citrix Workspace pour Android

March 22, 2024

L'application Citrix Workspace pour Android vous permet d'accéder en déplacement depuis votre tablette ou téléphone à :

- Virtual Apps and Desktops.
- des applications tactiles pour une utilisation à faible intensité sur des tablettes comme alternative aux ordinateurs de bureau.

Nous préconisons de mettre à jour ou d'installer l'application Citrix Workspace pour Android à partir de Google Play à l'aide d'un appareil Android. Les mises à jour automatiques sont autorisées lorsque de nouvelles versions sont disponibles.

Pour plus d'informations sur les fonctionnalités disponibles dans l'application Citrix Workspace pour Android, consultez Tableau des fonctionnalités de l'application Citrix Workspace.

Pour obtenir des informations détaillées sur les fonctionnalités, les problèmes résolus et les problèmes connus, consultez la page À propos de cette version.

Pour plus d'informations sur les éléments obsolètes, consultez la page Fin de prise en charge.

### Langues prises en charge

L'application Citrix Workspace pour Android a été conçue pour être utilisée dans des langues autres que l'anglais. Pour obtenir la liste des langues prises en charge par l'application Citrix Workspace pour Android, consultez la section Langues prises en charge.

### Ancienne documentation

Pour les versions de produits qui ont atteint leur fin de vie, consultez la section Ancienne documentation.

## À propos de cette version

June 27, 2024

Découvrez les nouvelles fonctionnalités, les améliorations, les problèmes résolus et les problèmes connus.

> **Remarque :**
>
> Vous recherchez des fonctionnalités en version Technical Preview ? Nous avons rassemblé ces fonctionnalités dans une liste afin que vous puissiez les trouver en un seul endroit. Découvrez notre page Fonctionnalités de la version Technical Preview et partagez vos commentaires en utilisant le lien vers le formulaire Podio ci-joint.

## Nouveautés de la version 24.5.0

### Prise en charge de l'authentification à l'aide de FIDO2 lors de la connexion à un magasin cloud

À partir de la version 24.5.0, les utilisateurs peuvent s'authentifier auprès de l'application Citrix Workspace à l'aide de l'authentification sans mot de passe basée sur FIDO2 lors de la connexion à un magasin cloud. Le protocole FIDO2 offre une méthode d'authentification transparente, permettant aux employés de l'entreprise d'accéder aux applications et bureaux pendant les sessions virtuelles sans avoir à saisir de nom d'utilisateur ni de mot de passe. Cette fonctionnalité prend en charge à la fois l'itinérance (USB uniquement) et les authentificateurs de plateforme (code PIN, reconnaissance faciale et empreinte digitale uniquement). Cette fonctionnalité est compatible avec la version 9 et les versions ultérieures d'Android.

L'authentification FIDO2 est prise en charge avec les onglets personnalisés de Chrome. Si vous souhaitez utiliser l'authentification FIDO2 avec WebView, signalez-le à l'aide du formulaire Podio.

> **Remarque :**
>
> Cette fonctionnalité est activée par défaut.

### Scanner de documents

Si vous êtes connecté à l'application Citrix Workspace, vous pouvez utiliser la fonctionnalité de numérisation rapide pour numériser de nombreux documents et les transférer vers la session de bureau virtuel.

> **Remarque :**
>
> - Cette fonctionnalité est activée par défaut.

#### Logiciels requis

- Le mappage des lecteurs clients (CDM) doit être activé pour le magasin.
- La numérisation de documents nécessite un accès en lecture et en écriture sur votre appareil. Pour donner accès, procédez comme suit :

1. Depuis votre profil, touchez **Paramètres** > **Paramètres du magasin** pour l'application.
2. Appuyez sur votre magasin actuel.
3. Appuyez sur **Stockage de l'appareil** et sélectionnez **Accès complet**.

Pour plus d'informations sur l'utilisation de cette fonctionnalité, consultez la section Numérisation de documents dans la documentation d'aide.

#### Annonce de fin de prise en charge

À partir de la version 24.5.0, l'application Citrix Workspace pour Android ne prend pas en charge les versions 9, 10 et 11 du système d'exploitation Android. Pour garantir des résultats optimaux, mettez à jour vos appareils Android vers la dernière version du système d'exploitation.

Pour plus d'informations, consultez Fin de prise en charge.

#### Technical Preview

- Redirection audio avec microphones externes.
- Authentification unique pour les machines virtuelles compatibles avec Microsoft Entra ID

### Problème résolu dans la version 24.5.0

Il n'y a aucun problème résolu dans cette version.

### Problème connu dans la version 24.5.0

- Lorsque vous démarrez une session de bureau virtuel sur un appareil compatible DeX et que vous cliquez sur le bouton **Agrandir** dans la barre d'outils de session, la session est déconnectée et la fenêtre agrandie se ferme.

  Le problème se produit en raison de la configuration du moniteur externe lorsque vous utilisez l'application Citrix Workspace pour Android version 24.4.0 et un appareil Samsung Galaxy Tab S9 Ultra avec OneUI 6.0. [HDX-65584]

### Nouveautés de la version 24.4.0

Cette version apporte certaines modifications afin d'améliorer la stabilité et les performances générales.

#### Annonce de l'obsolescence des protocoles TLS 1.0 et TLS 1.1

Citrix prévoit de rendre obsolète la prise en charge des protocoles TLS 1.0 et TLS 1.1 dans les prochaines versions. Le protocole recommandé est TLS 1.2 ou TLS 1.3. Pour plus d'informations, consultez Fin de prise en charge.

### Problèmes résolus dans la version 24.4.0

Les tentatives d'installation de l'application Citrix Workspace version 24.1.0 échouent et une erreur d'incompatibilité s'affiche. Le problème se produit sur certains appareils Zebra qui ne sont pas équipés d'une caméra. [CVADHELP-24843]

### Problèmes connus dans la version 24.4.0

Il n'y a aucun nouveau problème connu.

> **Remarque :**
>
> Pour obtenir la liste complète des problèmes des versions précédentes, consultez la section Problèmes connus.

### Versions précédentes

Cette section fournit des informations sur les nouvelles fonctionnalités et les problèmes résolus dans les versions précédentes que nous prenons en charge conformément aux étapes du cycle de vie de l'application Citrix Workspace.

#### 24.3.5

#### Nouveautés

Cette version inclut des améliorations apportées à la collecte de journaux. Le fichier journal contient désormais des informations plus complètes qui peuvent aider les administrateurs informatiques et les équipes de support technique à mieux analyser le scénario.

**Transférer les paramètres de l'application Citrix Workspace via UEM** Auparavant, vous pouviez configurer l'URL du magasin dans l'application Citrix Workspace.

À partir de cette version, vous pouvez configurer les paramètres de l'application Citrix Workspace sur les appareils gérés via n'importe quel outil de solution de gestion unifiée des terminaux (UEM) déployé dans votre infrastructure.

> **Remarque :**
>
> En tant qu'administrateur, si vous avez la possibilité de configurer les paramètres de l'application Citrix Workspace à l'aide d'UEM et du Global App Configuration Service (GACS), UEM a toujours la préférence sur GACS.

Pour plus d'informations sur la configuration, consultez la section Transférer les paramètres de l'application Citrix Workspace via UEM.

#### Problèmes résolus

Il n'y a aucun problème résolu dans cette version.

### 24.3.0

#### Nouveautés

**Prise en charge de l'authentification biométrique après une période d'inactivité** Une fois le délai d'inactivité expiré, l'utilisateur final est invité à s'authentifier à l'aide de fonctionnalités biométriques telles que la reconnaissance faciale et la lecture d'empreintes digitales.

La forme d'authentification biométrique la plus robuste disponible pour l'utilisateur final dépend de l'OEM de son périphérique, et il est invité en fonction de celle-ci.

Pour plus d'informations sur la configuration du délai d'inactivité, consultez la section Délai d'inactivité pour les sessions d'application Citrix Workspace.

#### Problèmes résolus

Il n'y a aucun problème résolu dans cette version.

## Problèmes connus

#### Problèmes connus dans la version 22.6.5

- Lorsque vous ouvrez une application Web ou SaaS, les boutons de la barre des tâches et les points de suspension ne fonctionnent pas comme prévu. Le problème se produit lorsque vous activez l'**Interface Web** dans l'écran **Ajouter un compte**. [RFANDROID-10263]

#### Problèmes connus dans la version 21.4.0

Aucun nouveau problème n'a été observé dans cette version.

> **Remarque :**
>
> Lorsque vous êtes inscrit au profil de travail dans l'application Citrix Workspace, le lancement de vos sessions à l'aide du navigateur Chrome à partir d'un fichier ICA dans le profil personnel ne fonctionne plus. Toutefois, le problème n'est pas présent avec Citrix Secure Web lors de l'ajout de l'URL du fichier ICA dans la liste d'exclusion.

#### Problèmes connus dans la version 20.3.0

Sur un périphérique Samsung DeX, il se peut que vous ne puissiez pas annuler la redirection de périphérique USB si vous fermez l'invite d'autorisation sans toucher le bouton **Annuler**. [RFANDROID-5397]

#### Problèmes connus dans la version 20.2.0

Les tentatives de reconnexion échouent lorsque vous touchez **Connexion** dans la boîte de dialogue **Reconnexion automatique des clients**. Le problème se produit dans les sessions connectées à Citrix XenApp et XenDesktop version 7.6 CU 8. [RFANDROID-5151]

### Limitations

Lors du démarrage d'applications Web et SaaS depuis l'application Citrix Workspace, si l'application utilise Google IdP et nécessite que l'utilisateur final se connecte, l'authentification échoue et le message d'erreur « Accès refusé » s'affiche.

### Technical Preview

Les versions Technical Preview sont disponibles dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités en version Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut ou non prendre en considération les commentaires en fonction de leur gravité, criticité et importance.

### Avis de tiers

Les produits Citrix contiennent souvent du code tiers octroyé sous licence à Citrix à des fins d'utilisation et de redistribution sous une licence Open Source. Afin de mieux informer ses clients, Citrix publie le code Open Source inclus dans les produits Citrix dans une liste des codes utilisés sous licence Open Source.

Pour plus d'informations sur les codes utilisés sous licence Open Source, voir Open Source Licensed Code.

L'application Citrix Workspace peut inclure un logiciel tiers distribué sous une licence selon les conditions définies dans le document suivant :

Avis de tiers de l'application Citrix Workspace pour Android

### Fin de prise en charge

Pour plus d'informations sur les éléments obsolètes, consultez la page Fin de prise en charge.

### Ancienne documentation

Pour les versions de produits qui ont atteint leur fin de vie, consultez la section Ancienne documentation.

## Fonctionnalités de la version Technical Preview

June 27, 2024

Les fonctionnalités présentées dans les versions Technical Preview sont disponibles à des fins d'utilisation dans les environnements hors production ou de production limitée, et pour permettre aux clients de partager leurs commentaires. Citrix n'offre pas de support pour les fonctionnalités présentées dans les versions Technical Preview, mais accepte les commentaires pour les améliorer. Citrix peut prendre en considération les commentaires en fonction de leur gravité, criticité et importance.

### Liste des fonctionnalités de la version Technical Preview

Le tableau suivant répertorie les fonctionnalités de la version Technical Preview. Ces fonctionnalités sont des fonctionnalités de prévisualisation sur demande uniquement. Pour activer l'une de ces fonctionnalités et fournir des commentaires sur celles-ci, remplissez les formulaires correspondants.

| Titre | Disponible à partir de la version | Formulaire d'activation (cliquez sur l'icône) | Formulaire de commentaires (cliquez sur l'icône) |
|---|---|---|---|
| Authentification unique pour les machines virtuelles compatibles avec Microsoft Entra ID | 24.5.0 |  |  |
| Redirection audio avec microphones externes | 24.5.0 |  |  |
| Prise en charge de l'audio adaptatif | 23.11.0 |  |  |
| Prise en charge des applications de partage de sessions multi-fenêtres sur Samsung DeX | 2307 |  |  |
| Fenêtre de session distincte de celle de l'application Citrix Workspace pour Samsung DeX | 23.9.0 |  |  |
| Ajout de plusieurs magasins à l'aide de solutions de gestion unifiée des terminaux (UEM) | 23.8.0 |  |  |
| Mode d'image en incrustation | 23.3.5 |  |  |

| Titre | Disponible à partir de la version | Formulaire d'activation (cliquez sur l'icône) | Formulaire de commentaires (cliquez sur l'icône) |
|---|---|---|---|
| Prise en charge d'une expérience d'authentification unique (SSO) améliorée pour les applications Web et SaaS | 22.3.5 |  |  |

### Authentification unique pour les machines virtuelles compatibles avec Microsoft Entra ID

À partir de la version 24.5.0, l'application Citrix Workspace pour Android permet aux utilisateurs de se connecter à des machines virtuelles jointes à Azure AD à l'aide de l'authentification unique. Lors du premier lancement de machines virtuelles (VM) jointes à Azure AD dans l'application Citrix Workspace, les utilisateurs sont invités à s'authentifier en saisissant les informations d'identification de leur compte Azure. Les connexions VDA suivantes se font automatiquement sans avoir à saisir les informations d'identification et ce, jusqu'à l'expiration du jeton d'authentification.

> **Remarques :**
>
> - Cette fonctionnalité ne s'applique qu'aux magasins cloud joints à Azure AD.
> - Elle est désactivée par défaut. Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le formulaire Podio.
> - Vous pouvez nous faire part de vos commentaires sur cette version Technical Preview en utilisant le formulaire Podio.

### Redirection audio avec microphones externes

**Cette fonctionnalité est disponible en version Technical Preview depuis la publication de la version 24.5.0.**

Auparavant, vous ne pouviez utiliser qu'un seul périphérique audio au cours d'une session. À partir de la version 24.5.0, l'application Citrix Workspace pour Android affiche tous les périphériques audio locaux disponibles dans une session avec leur nom. En outre, les appareils audio prêts à l'emploi sont également pris en charge.

> **Remarques :**
>
> - Elle est désactivée par défaut. Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le formulaire Podio.
> - Vous pouvez nous faire part de vos commentaires sur cette version Technical Preview en utilisant le formulaire Podio.

### Prise en charge de l'audio adaptatif

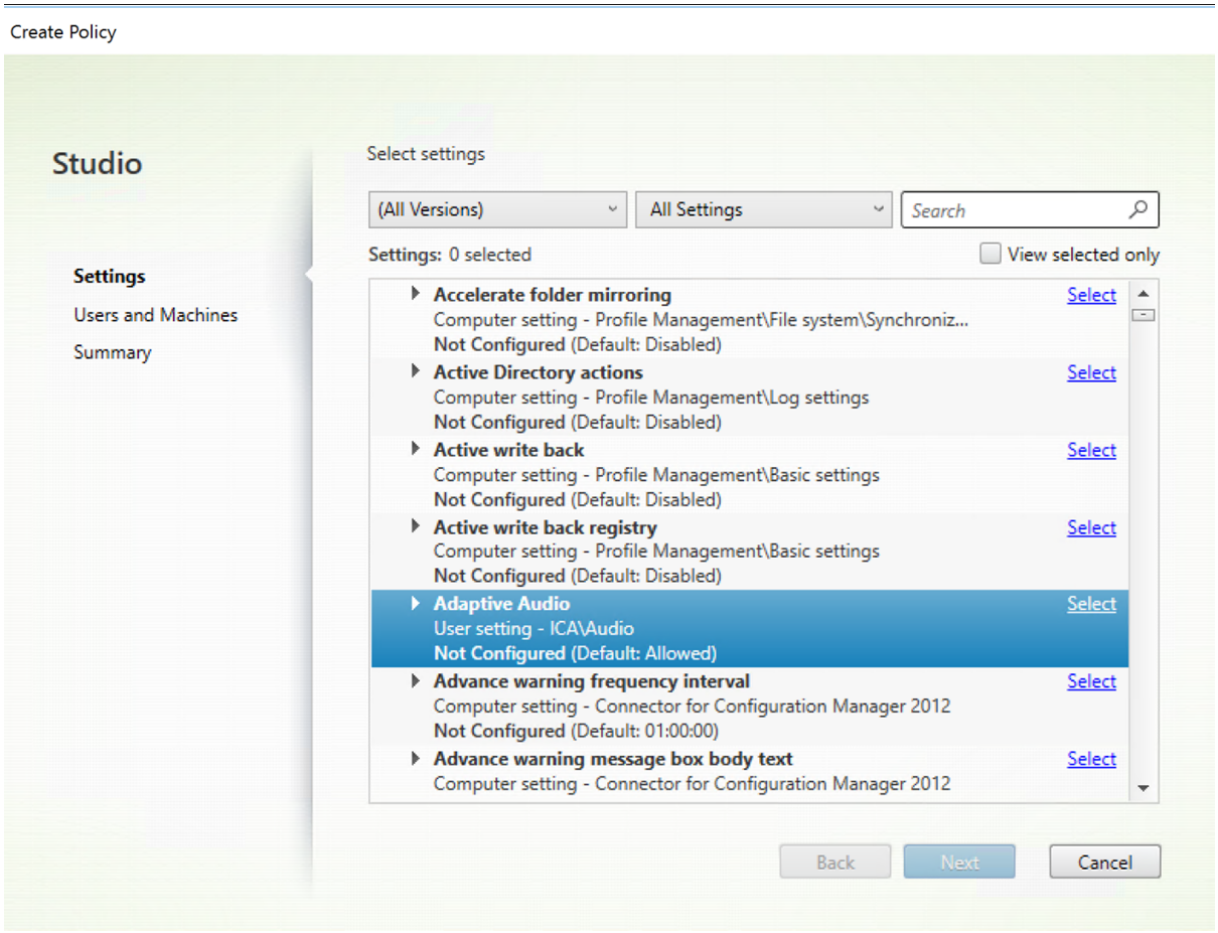
**Cette fonctionnalité est disponible en version Technical Preview depuis la publication de la version 23.11.0.**

L'application Citrix Workspace pour Android prend en charge l'audio adaptatif HDX. Cette fonctionnalité est conçue pour fournir aux utilisateurs une qualité audio exceptionnelle et une faible latence.

> **Remarques :**
>
> - Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le formulaire Podio.
> - Vous pouvez nous faire part de vos commentaires sur cette version Technical Preview en utilisant le formulaire Podio.

Vous pouvez configurer cette fonctionnalité en activant la stratégie **Audio adaptatif**.




Pour plus d'informations, consultez l'article sur les Paramètres de stratégie audio dans la documentation Citrix Virtual Apps and Desktops.

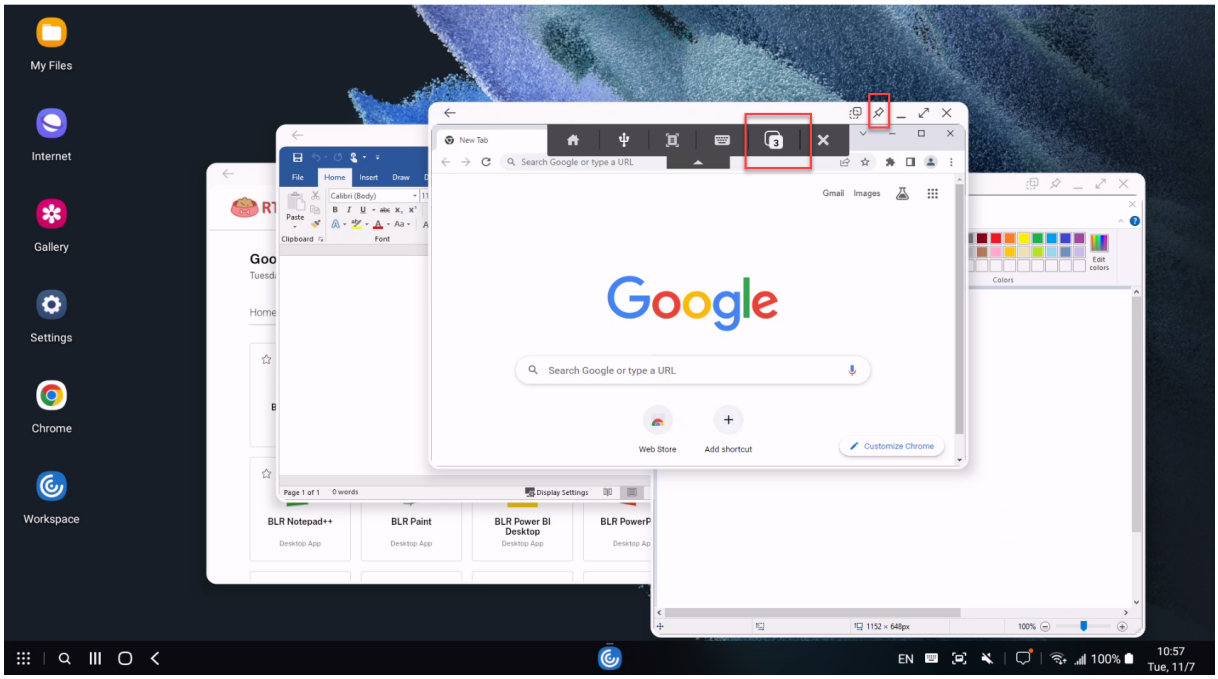
## Prise en charge des applications de partage de sessions multi-fenêtres sur Samsung DeX

**Cette fonctionnalité est disponible en version Technical Preview depuis la publication de la version 23.11.0.**

La version 23.9.5 de l'application Citrix Workspace a introduit une fenêtre de session distincte permettant aux utilisateurs finaux de bénéficier d'une expérience similaire à celle d'un ordinateur de bureau. Cependant, une seule fenêtre de session était prise en charge.

À partir de la version 23.11.0, l'application Citrix Workspace permet un multitâche fluide et offre aux utilisateurs une expérience similaire à celle d'un ordinateur de bureau. Il vous permet d'ouvrir plusieurs applications au cours d'une même session pour les exécuter simultanément. Ces applications s'ouvrent dans des fenêtres distinctes.




Par exemple, lorsque vous ouvrez l'application Citrix Workspace et que vous démarrez le navigateur Google Chrome, Microsoft Paint et Microsoft Word, les trois applications s'ouvrent dans une fenêtre distincte. Pour afficher le nombre de fenêtres de session d'application ouvertes et pour passer à une autre fenêtre de session d'application, utilisez l'icône de **changement d'application** dans la barre d'outils de session.

> **Remarques :**
>
> - Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le formulaire Podio.
> - Vous pouvez nous faire part de vos commentaires sur cette version Technical Preview en utilisant le formulaire Podio.
> - La première application que vous démarrez peut prendre une minute pour se connecter à la session et charger votre profil utilisateur.

### Cas d'utilisation

Lorsque vous ouvrez certaines applications sur l'écran DeX, vous pouvez toujours ouvrir des applications depuis l'application Citrix Workspace installée sur votre appareil mobile. Lorsque vous démarrez une session d'application sur l'écran de votre appareil mobile, une boîte de dialogue apparaît pour fermer la session existante sur DeX. Sur l'appareil mobile, l'application s'ouvre en mode fenêtre unique.

Si vous cliquez sur l'icône de l'application Citrix Workspace sur l'écran DeX lorsqu'une fenêtre d'application est ouverte sur l'écran de l'appareil, mais que l'application est en mode fenêtre unique, vous

devez quitter le mode fenêtre de session de l'application sur l'écran DeX, puis ouvrir à nouveau l'application pour accéder au mode fenêtres de session multiples.

Vous pouvez effectuer les opérations suivantes :

- Cliquez sur le bouton Épingler en haut à droite de la fenêtre pour épingler l'application Windows. La fenêtre épinglée reste toujours sur le dessus.
- Accédez au bouton de la barre d'outils de session dans toutes les fenêtres d'application.
- Réduisez, agrandissez, déplacez et fermez la fenêtre d'application.
- Passez d'une application à l'autre et effectuez plusieurs tâches à la fois en cliquant sur la souris, en double-cliquant, en faisant glisser et en appuyant sur le clavier.

#### Limitations de la fonctionnalité

- Le titre de la fenêtre d'aperçu dans la barre des tâches de Samsung DeX indique **Workspace** au lieu du nom réel de l'application.
- Le changement de taille de fenêtre orienté serveur n'est pas pris en charge. En d'autres termes, si la taille de la fenêtre côté serveur est définie ou limitée, les demandes de modification de la taille provenant du côté client sont infructueuses. Ce paramètre entraîne une différence entre les graphiques de la fenêtre locale et ceux de la fenêtre distante.
- La taille de la fenêtre côté client est minimale. En d'autres termes, la taille minimale d'une fenêtre sur un écran DeX de résolution 1920 x 1080 est de 220 x 220 avec la barre de titre, et la taille du rectangle disponible est de 220 x 189.
- Certaines options de menu peuvent s'étendre et apparaître en dehors des limites de l'application parente. Les options de menu étendues peuvent apparaître dans les autres fenêtres d'application.
- L'image d'aperçu d'une application dans la barre des tâches peut chevaucher et recouvrir l'aperçu d'une autre application.

### Fenêtre de session distincte de celle de l'application Citrix Workspace pour Samsung DeX

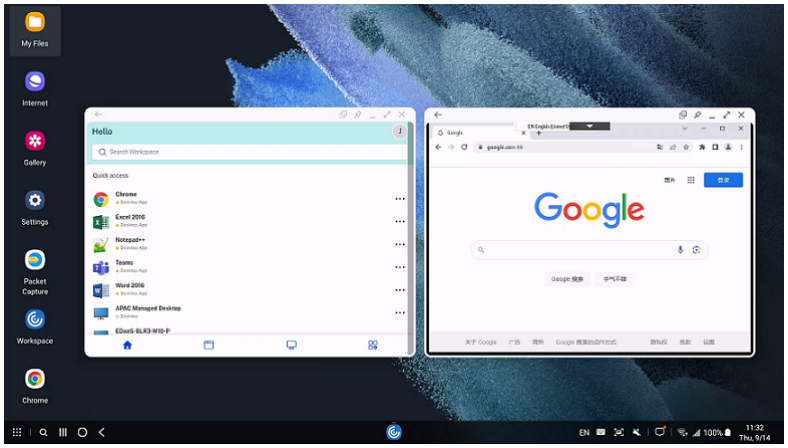
**Cette fonctionnalité est disponible en version Technical Preview depuis la publication de la version 23.9.5.**

Auparavant, lorsque vous démarriez une application virtuelle ou une session de bureau, celle-ci s'ouvrait dans la fenêtre d'interface utilisateur de l'application Citrix Workspace. Avec cette disposition, les utilisateurs finaux devaient appuyer sur l'icône **Accueil** dans la barre d'outils de la session et déconnecter la session pour accéder à une autre application ou à un autre bureau depuis l'application Citrix Workspace. Le mode fenêtre unique limitait l'expérience de bureau sur le Samsung DeX.

À partir de la version 23.9.5, l'application Citrix Workspace introduit une fenêtre de session distincte qui rend le multitâche plus efficace et convivial. Grâce à cette fonctionnalité, vous pouvez profiter d'une expérience similaire à celle d'un ordinateur de bureau.

Par exemple, lorsque vous ouvrez le navigateur Google Chrome, il s'ouvre dans une fenêtre distincte, comme le montre la capture d'écran suivante.




#### Limites connues de cette fonctionnalité

Une seule fenêtre de session est prise en charge. En d'autres termes, la fenêtre de session existante se ferme lors de l'ouverture d'une nouvelle fenêtre de session.

> **Remarques :**
>
> - Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le formulaire Podio.
> - Vous pouvez nous faire part de vos commentaires sur cette version Technical Preview en utilisant le formulaire Podio.

### Ajout de plusieurs magasins à l'aide de solutions de gestion unifiée des terminaux (UEM)

#### Cette fonctionnalité est disponible en version Technical Preview depuis la publication de la version 23.8.0.

Les administrateurs peuvent désormais utiliser les solutions de gestion unifiée des terminaux (UEM) pour configurer plusieurs magasins pour les appareils Android gérés.

> **Remarque :**

> - Vous pouvez nous faire part de vos commentaires sur cette version Technical Preview en utilisant le formulaire Podio.

Les informations de chaque magasin peuvent être ajoutées à un fichier JSON. Ce fichier JSON peut ensuite être chargé lors de la configuration de la politique de configuration de l'application. Les informations incluent :

- l'URL du magasin ;
- le type de boutique (facultatif) ;

  > **Remarque :**
  >
  > – Si le type de magasin n'est pas indiqué, l'interface par défaut est considérée comme native.

- le nom du magasin (facultatif) ;

> **Remarque :**
>
> - l'UEM prend en charge un magasin dans le cloud et de nombreux magasins sur site.

Le fichier JSON doit être au format clé-valeur. Pour en savoir plus, consultez les exemples de données JSON suivants :

> **Remarque :**
>
> - les exemples de données JSON sont liés à Microsoft Intune. Les données JSON peuvent varier pour les autres solutions UEM.

```
{

    "kind": "androidenterprise#managedConfiguration",
    "productId": "app:com.citrix.Receiver",
    "managedProperty": [
        {

            "key": "stores",
            "valueBundleArray": [
                {

                    "managedProperty": [
                        {

                            "key": "url",
                            "valueString": "test.cloud.com"
                         }
 ,
                        {
```

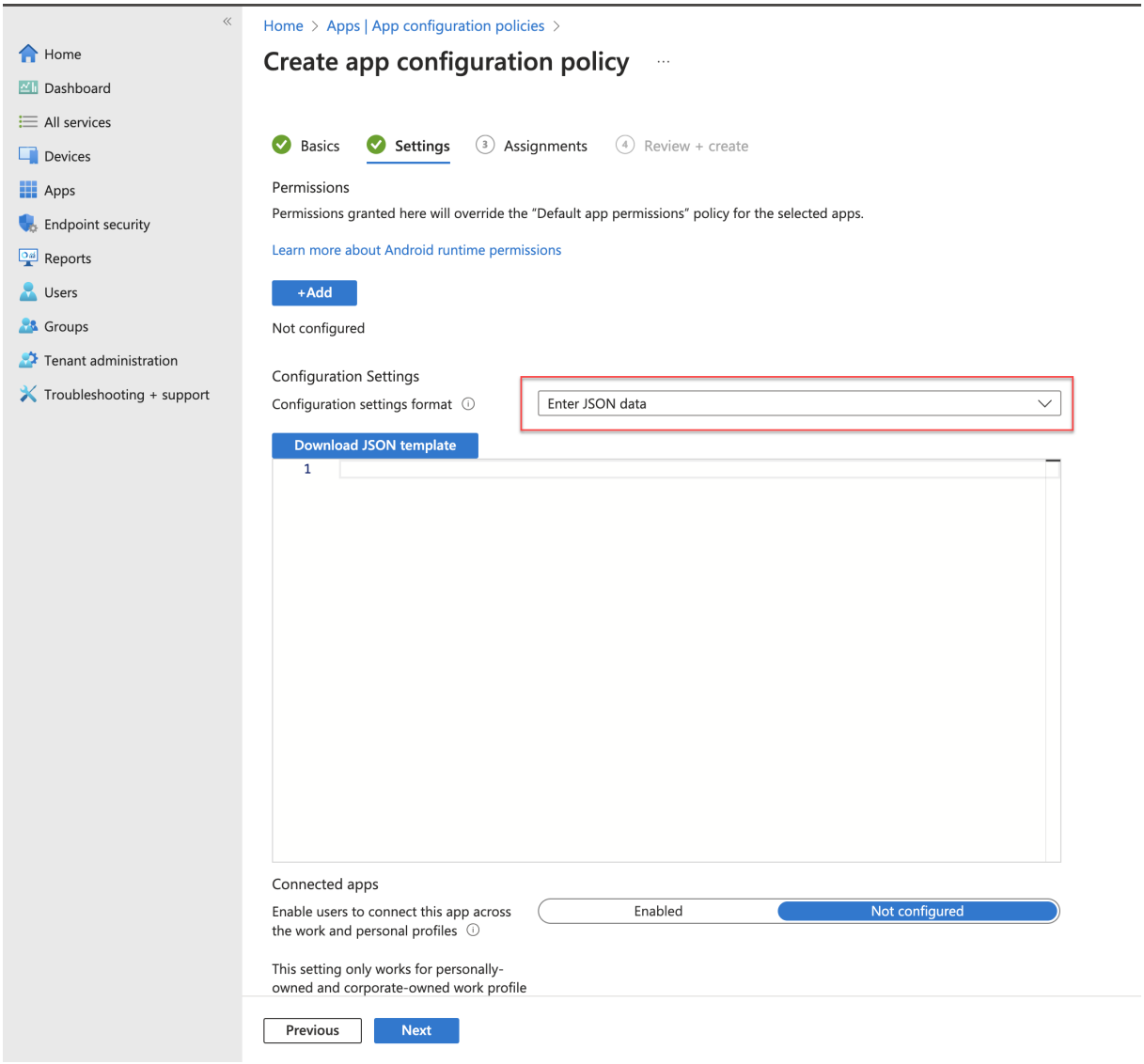
 

```
                                "key": "storeType",
                                "valueInteger": 1
                            }
    ,
                            {

                                "key": "displayName",
                                "valueString": "1"
                            }

                        ]
                    }
    ,
                    {

                        "managedProperty": [
                            {

                                "key": "url",
                                "valueString": "test2.cloud.com"
                            }
    ,
                            {

                                "key": "storeType",
                                "valueInteger": 2
                            }
    ,
                            {

                                "key": "displayName",
                                "valueString": "2"
                            }

                        ]
                    }

                ]
            }
    ,
            {

                "key": "restrict_user_store_modification",
                "valueBool": false
            }

        ]
    }

<!--NeedCopy-->
```

> **Remarques :**
>
> - (défaut) Si le nombre entier est 1, les utilisateurs peuvent voir le magasin natif ou par défaut.
> - Si le nombre entier est 2, les utilisateurs peuvent voir le magasin dans une interface Web.

Pour télécharger le fichier JSON contenant les configurations de magasin, sélectionnez **Saisir les données JSON** dans la liste déroulante du **format des paramètres de configuration**.




## Mode d'image en incrustation

**Cette fonctionnalité est disponible en version Technical Preview depuis la publication de la version 23.3.5.**

L'application Citrix Workspace pour Android prend en charge le mode d'image en incrustation

(Picture-in-Picture, PiP), qui vous permet de réduire votre session de bureau, votre application SaaS ou votre application Web à une fenêtre flottante. Vous pouvez déplacer cette fenêtre librement sur l'écran et la placer n'importe où. Le mode PiP libère l'écran d'accueil de l'application Citrix Workspace pour que vous puissiez effectuer d'autres tâches.

Pour utiliser cette fonctionnalité :

- Dans votre session de bureau, appuyez sur le bouton **Accueil** de la barre d'outils de la session.

  ou

- Lorsque vous utilisez une application SaaS ou Web, touchez le **menu à points de suspension ( ...)** > **Réduire**.

Appuyez sur la fenêtre flottante pour afficher l'application en plein écran et fermez l'application en appuyant sur l'icône **X** de la fenêtre flottante. La fenêtre flottante apparaît automatiquement en plein écran lorsque vous réduisez une autre application.

> **Remarque :**
>
> - Cette fonctionnalité préliminaire est uniquement disponible sur demande. Pour l'activer dans votre environnement, remplissez le formulaire Podio.

La fonctionnalité PiP est prise en charge à la fois sur site et dans le cloud. Toutefois, pour les déploiements dans le cloud, vous pouvez :

- réduire les applications Web à une fenêtre PiP ;
- passer d'une session de bureau à une application Web en appuyant sur la fenêtre flottante.

> **Remarque :**
>
> Vous ne pouvez garder que deux applications actives à la fois. L'une en mode plein écran et l'autre réduite en PiP :
>
> - 2 applications Web ou SaaS
> - 1 application Web ou SaaS et 1 session de bureau ou application virtuelle

## Prise en charge d'une expérience d'authentification unique (SSO) améliorée pour les applications Web et SaaS

**Cette fonctionnalité est disponible en version Technical Preview depuis la publication de la version 22.3.5.**

Cette fonctionnalité simplifie la configuration du SSO pour les applications Web internes et les applications SaaS lors de l'utilisation de fournisseurs d'identité tiers (IdP).

L'expérience SSO améliorée réduit l'ensemble du processus à quelques commandes. Elle élimine le besoin de configurer Citrix Secure Private Access dans la chaîne du fournisseur d'identité pour configurer SSO. Cela améliore également l'expérience utilisateur, à condition que le même IdP soit utilisé pour l'authentification à la fois auprès de l'application Workspace et de l'application Web ou SaaS qui est lancée.

Vous pouvez vous inscrire à cette version Technical Preview en remplissant ce formulaire Podio.

### De la version préliminaire (version Technical Preview) à la disponibilité générale (GA)

| Nom de la fonctionnalité | Version en disponibilité générale |
|---|---|
| Correspondance DPI | 24.1.0 |
| Transférer les paramètres de l'application Citrix Workspace via UEM | 24.3.5 |
| Scanner de documents | 24.5.0 |

## Application Citrix Workspace 22.4.0 pour Android - Aperçu

April 21, 2022

### Nouveautés

Cette version résout un certain nombre de problèmes afin d'améliorer la stabilité et les performances générales.

### Problèmes résolus

Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.

### Problèmes connus

Aucun nouveau problème n'a été observé dans cette version.

### Recommandations et remarques

- L'application Citrix Workspace pour Android 22.4.0 prend en charge Android 12.
- Si vous accédez à des magasins basés sur HTTP, nous vous recommandons de passer à des magasins basés sur HTTPS pour des raisons de sécurité. Pour plus d'informations, consultez HTTPS.

## Conditions préalables à l'installation

June 26, 2024

### Configuration système requise et compatibilité

#### Configuration requise par l'appareil

L'application Citrix Workspace prend en charge les versions Android 12 et ultérieures.

Pour garantir des résultats optimaux, mettez à jour vos appareils Android vers la dernière version du système d'exploitation.

Vous pouvez démarrer des sessions d'application Citrix Workspace à partir de Workspace pour Web lorsque le navigateur Web est compatible avec Workspace pour Web. Si vous ne parvenez pas à démarrer la session, configurez directement votre compte via l'application Citrix Workspace.

> **Important :**
>
> Si une version Technical Preview de l'application Citrix Workspace pour Android est installée, désinstallez-la avant d'installer la nouvelle version.

#### Éléments requis sur les serveurs

StoreFront :

- StoreFront 2.6 ou version ultérieure

  Permet d'accéder directement aux magasins StoreFront. L'application Citrix Workspace pour Android prend également en charge les versions antérieures de StoreFront.

- StoreFront configuré avec un site Workspace pour Web

  Permet d'accéder aux magasins StoreFront à partir d'un navigateur Web. Pour prendre connaissance des limitations de ce déploiement, consultez la documentation de StoreFront.

Activez les stratégies de réécriture fournies par Citrix Gateway.

Citrix Virtual Apps and Desktops (l'un des produits suivants) :

- Citrix Virtual Apps 7.5 ou version ultérieure
- Citrix Virtual Apps and Desktops 7.x ou version ultérieure

### Connexions et certificats

L'application Citrix Workspace prend en charge les connexions HTTP, HTTPS et ICA-over-TLS à un serveur Citrix Virtual Apps par le biais des configurations suivantes.

Pour les connexions LAN :

- StoreFront 2.6 ou version ultérieure
- Site XenApp Services (anciennement Program Neighborhood Agent).

Pour les connexions à distance sécurisées (l'un des produits suivants) :

- Citrix Gateway 12.1 et versions ultérieures (y compris les versions VPX, MPX et SDX).

#### Certificats TLS

Lorsque vous sécurisez les connexions distantes à l'aide du protocole TLS, l'appareil mobile effectue les opérations suivantes :

1. Authentifie le certificat TLS de la passerelle distante par rapport à un magasin local d'autorités de certification racine approuvées.
2. Reconnaît automatiquement les certificats délivrés par des sociétés de distribution (telles que Verisign et Thawte) à condition que le certificat racine de l'autorité de certification existe dans le magasin de clés local.

#### Certificats privés (auto-signés)

Si vous installez un certificat privé sur la passerelle distante, assurez-vous que le certificat racine de l'autorité de certification de l'organisation est installé sur l'appareil mobile. Cette configuration vous permet d'accéder correctement aux ressources Citrix à l'aide de l'application Citrix Workspace pour Android.

> **Remarque :**
>
> Lorsque vous ne pouvez pas vérifier le certificat de la passerelle lors de la connexion (car le certificat racine n'est pas inclus dans le magasin de clés), un avertissement relatif à un certificat non approuvé s'affiche. Si un utilisateur choisit d'ignorer l'avertissement, une liste des applications

> s'affiche. Toutefois, les applications ne démarrent pas.

### Certificats génériques

Les certificats génériques remplacent les certificats de serveur individuel pour n'importe quel serveur situé dans le même domaine. L'application Citrix Workspace pour Android prend en charge les certificats génériques.

### Certificats intermédiaires et Citrix Gateway

Si votre chaîne de certificat contient un certificat intermédiaire, ce dernier doit être ajouté au certificat serveur de Citrix Gateway. Consultez l'article du centre de connaissances qui correspond à votre édition de Citrix Gateway : CTX114146 et CTX124937

### Stratégie de validation des certificats de serveur

La stratégie de validation des certificats de serveur de l'application Citrix Workspace pour Android est plus stricte.

> **Important :**
>
> Avant d'installer l'application Citrix Workspace pour Android, vérifiez que les certificats sur le serveur ou Citrix Gateway sont correctement configurés comme indiqué ci-dessous. Les connexions peuvent échouer si :
>
> - la configuration du serveur ou de Citrix Gateway inclut un certificat racine incorrect ;
> - la configuration du serveur ou de Citrix Gateway n'inclut pas tous les certificats intermédiaires ;
> - la configuration du serveur ou de Citrix Gateway inclut un certificat intermédiaire expiré ou non valide ;
> - la configuration du serveur ou de Citrix Gateway inclut un certificat intermédiaire avec signature croisée.

Lors de la validation d'un certificat de serveur, l'application Citrix Workspace pour Android utilise **tous** les certificats fournis par le serveur (ou Citrix Gateway). Elle vérifie ensuite également si les certificats sont fiables. Si les certificats ne sont pas tous approuvés, la connexion échoue.

Cette stratégie est plus stricte que la stratégie de certificat des navigateurs web. De nombreux navigateurs Web comprennent un grand nombre de certificats racine auxquels ils font confiance.

Le serveur (ou Citrix Gateway) doit être configuré avec le jeu correct de certificats. Un jeu incorrect de certificats peut entraîner l'échec de la connexion à l'application Citrix Workspace pour Android.

Supposons qu'un Citrix Gateway soit configuré avec ces certificats valides. Cette configuration est recommandée pour les clients qui requièrent une validation stricte. Ils peuvent appliquer une validation plus stricte en déterminant précisément quel certificat racine est utilisé par l'application Citrix Workspace pour Android :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »
- « Certificat racine exemple »

L'application Citrix Workspace pour Android vérifie ensuite si tous ces certificats sont valides. L'application Citrix Workspace pour Android vérifie également qu'elle fait déjà confiance à « Certificat racine exemple ». Si l'application Citrix Workspace pour Android ne fait pas confiance à « Certificat racine exemple », la connexion échoue.

> **Important**
>
> Certaines autorités de certification disposent de plus d'un certificat racine. Si vous avez besoin de cette validation plus stricte, assurez-vous que votre configuration utilise le certificat racine approprié. Par exemple, il existe actuellement deux certificats (« DigiCert »/« GTE CyberTrust Global Root » et « DigiCert Baltimore Root »/« Baltimore CyberTrust Root ») qui peuvent valider les mêmes certificats de serveur.
>
> Sur certaines machines utilisateur, les deux certificats racine sont disponibles. Sur les autres machines, seul le certificat « DigiCert Baltimore Root »/« Baltimore CyberTrust Root » est disponible. Si vous configurez « GTE CyberTrust Global Root » sur la passerelle, les connexions à l'application Citrix Workspace pour Android sur ces machines utilisateur échouent. Consultez la documentation de l'autorité de certification pour déterminer quel certificat racine peut être utilisé. Notez également que les certificats racine finissent par expirer, comme tous les certificats.
>
> **Remarque :**
>
> Certains serveurs et Citrix Gateway n'envoient jamais le certificat racine, même si cela est configuré. Une validation plus stricte n'est par conséquent pas possible.

Supposons maintenant qu'une passerelle soit configurée avec ces certificats valides. Cette configuration, sans certificat racine, est généralement recommandée :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »

L'application Citrix Workspace pour Android utilise ces deux certificats. Elle recherche ensuite un certificat racine sur la machine utilisateur. Si elle en trouve un qui est validé et également approuvé (tel que « Certificat racine exemple »), la connexion réussit. Sinon, la connexion échoue. Cette configuration fournit le certificat intermédiaire dont l'application Citrix Workspace pour Android a besoin, mais

permet également à l'application Citrix Workspace pour Android de choisir un quelconque certificat racine valide et approuvé.

Supposons maintenant qu'un Citrix Gateway soit configuré avec ces certificats :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »
- « Certificat racine incorrect »

L'application Citrix Workspace pour Android lit le mauvais certificat racine et la connexion échoue.

Certaines autorités de certification disposent de plus d'un certificat intermédiaire. Dans ce cas, le Citrix Gateway est généralement configuré avec tous les certificats intermédiaires (mais pas le certificat racine) tels que :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple 1 »
- « Certificat intermédiaire exemple 2 »

Certaines autorités de certification utilisent un certificat intermédiaire avec signature croisée. Ce cas de figure est destiné aux situations dans lesquelles il existe plus d'un certificat racine, et qu'un certificat racine antérieur est toujours en cours d'utilisation en même temps qu'un certificat racine plus récent. Dans ce cas, il y a au moins deux certificats intermédiaires. Par exemple, le certificat racine antérieur « Class 3 Public Primary Certification Authority » et le certificat intermédiaire avec signature croisée Verisign Class 3 Public Primary Certification Authority - G5 correspondant.

Toutefois, un certificat racine antérieur « Verisign Class 3 Public Primary Certification Authority - G5 » correspondant est également disponible, et il remplace « Class 3 Public Primary Certification Authority ». Le certificat racine antérieur n'utilise pas de certificat intermédiaire avec signature croisée.

Le certificat intermédiaire avec signature croisée et le certificat racine ont le même nom de sujet (Délivré à). Cependant le certificat intermédiaire avec signature croisée a un nom d'émetteur différent (Délivré par). Cela permet de différencier le certificat intermédiaire avec signature croisée d'un certificat intermédiaire ordinaire (tel « Certificat intermédiaire exemple 2 »).

Cette configuration, sans certificat racine et sans certificat intermédiaire avec signature croisée, est généralement recommandée :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »

Évitez de configurer le Citrix Gateway de manière à utiliser le certificat intermédiaire avec signature croisée, car cela entraîne la sélection du certificat racine antérieur :

- « Certificat de serveur exemple »
- « Certificat intermédiaire exemple »

- « Certificat intermédiaire croisé exemple » [non recommandé]

Il n'est pas recommandé de configurer Citrix Gateway avec le certificat de serveur uniquement :

- « Certificat de serveur exemple »

Lorsque l'application Citrix Workspace pour Android ne peut pas trouver tous les certificats intermédiaires, la connexion échoue.

## Installer, mettre à niveau

June 21, 2023

### Mettre à niveau

Pour mettre à niveau la dernière application Citrix Workspace, effectuez l'une des opérations suivantes :

- Mettez à niveau votre application Citrix Workspace à l'aide de Google Play.
- Téléchargez l'application Citrix Workspace à partir de la page des téléchargements de Citrix et installez l'application pour mettre à niveau Citrix Receiver vers l'application Citrix Workspace.

Pour plus d'informations sur les fonctionnalités disponibles dans l'application Citrix Workspace pour Android, consultez Tableau des fonctionnalités de l'application Citrix Workspace.

Pour accéder à la documentation de Citrix Receiver pour Android, consultez Citrix Receiver.

## Prise en main

March 22, 2024

### Compte

Pour créer un compte, procédez comme suit :

1. Entrez une URL de magasin valide ou votre adresse e-mail dans le champ **Adresse**. Par exemple, storefront.organisation.com. Remplissez les autres champs avec les informations nécessaires.
2. Entrez les informations d'identification de l'utilisateur.

#### Accès à StoreFront via Citrix Gateway

Pour de plus amples informations sur la configuration de l'accès à StoreFront via Citrix Gateway, consultez :

- Configurer et gérer des magasins
- Intégration de StoreFront à Citrix Gateway

### Découverte de compte basée sur une adresse e-mail

Vous pouvez configurer l'application Citrix Workspace de manière à utiliser la découverte de compte basée sur e-mail. Une fois configurée, plutôt que d'entrer une adresse URL de serveur, les utilisateurs entrent leur adresse e-mail durant l'installation et la configuration de l'application Citrix Workspace pour Android.

L'application Citrix Workspace pour Android identifie le serveur Citrix Gateway ou StoreFront associé à l'adresse e-mail en se basant sur les enregistrements SRV de DNS. Elle invite ensuite l'utilisateur à se connecter pour accéder à ses applications, bureaux et données hébergés.

### Fichier de provisioning

Vous pouvez utiliser StoreFront pour créer des fichiers de provisioning contenant les détails des comptes. Vous pouvez mettre ces fichiers à la disposition de vos utilisateurs pour leur permettre de configurer l'application Citrix Workspace pour Android automatiquement.

Après l'installation de l'application Citrix Workspace pour Android, il leur suffit d'ouvrir le fichier **.cr** sur l'appareil pour configurer l'application Citrix Workspace pour Android. Si vous configurez des sites Workspace pour Web, les utilisateurs peuvent également obtenir les fichiers de provisioning de l'application Citrix Workspace pour Android à partir de ces sites.

Pour plus d'informations, veuillez consulter la documentation de StoreFront.

### Fournir aux utilisateurs des informations de compte à entrer manuellement

Si vous fournissez aux utilisateurs des informations de compte à entrer manuellement, assurez-vous de leur communiquer les informations suivantes. Les informations suivantes permettent aux utilisateurs de se connecter correctement à leurs bureaux hébergés :

- L'adresse URL de StoreFront ou du site XenApp et XenDesktop hébergeant les ressources ; par exemple : nomserveur.société.com.

- Pour permettre l'accès à l'aide de Citrix Gateway, fournissez l'adresse de Citrix Gateway et la méthode d'authentification requise.

  Pour plus d'informations, consultez la documentation Citrix Gateway.

Lorsqu'un utilisateur entre les détails d'un nouveau compte, l'application Citrix Workspace tente de vérifier la connexion. En cas de réussite, l'application Citrix Workspace invite l'utilisateur à se connecter au compte.

## Fournir un accès à Citrix Virtual Apps and Desktops et Citrix DaaS

L'application Citrix Workspace nécessite la configuration de StoreFront pour mettre à disposition des applications, des bureaux et des fichiers à partir de votre déploiement Citrix Virtual Apps and Desktops ou Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service).

### StoreFront

Vous pouvez configurer StoreFront pour fournir des services d'authentification et de mise à disposition de ressources pour l'application Citrix Workspace. Cela vous permet de créer des magasins d'entreprise centralisés afin de fournir :

- Bureaux et applications via Citrix Virtual Apps and Desktops ou Citrix DaaS.
- Applications XenMobile Apps et applications mobiles que vous avez préparées pour votre organisation via XenMobile.

L'authentification entre l'application Citrix Workspace et un magasin StoreFront peut être gérée de plusieurs manières :

- Les utilisateurs à l'intérieur de votre pare-feu peuvent se connecter directement à StoreFront.
- Les utilisateurs en dehors de votre pare-feu peuvent se connecter à StoreFront via Citrix Gateway.
- Les utilisateurs en dehors de votre pare-feu peuvent se connecter à StoreFront via Citrix Gateway.

**Connexion à StoreFront** L'application Citrix Workspace pour Android prend en charge le lancement de sessions à partir de Workspace pour Web, à condition que le navigateur Web soit compatible avec Workspace pour Web. Si le lancement échoue, configurez votre compte directement via l'application Citrix Workspace pour Android.

> **Conseil**
>
> Lorsque Workspace pour Web est utilisé à partir d'un navigateur, les sessions ne sont pas

> lancées automatiquement lors du téléchargement d'un fichier **.ICA**. Le fichier **.ICA** doit être ouvert manuellement juste après son téléchargement pour que la session puisse être lancée.

Les magasins que vous créez dans StoreFront se composent de services destinés à fournir une infrastructure d'authentification et de mise à disposition de ressources pour l'application Citrix Workspace. Créez des magasins qui énumèrent et regroupent les bureaux et applications des sites XenDesktop et XenApp, tout en mettant ces ressources à la disposition des utilisateurs.

Pour les administrateurs soucieux d'exercer un contrôle plus rigoureux, Citrix fournit un modèle que vous pouvez utiliser pour créer un site de téléchargement pour l'application Citrix Workspace pour Android.

Configurez les magasins pour StoreFront comme vous le feriez avec Citrix Virtual Apps and Desktops et Citrix DaaS. Aucune configuration spéciale n'est nécessaire pour les appareils mobiles.

#### Se connecter via Citrix Gateway

L'application Citrix Workspace pour Android prend en charge Citrix Gateway 11 et versions supérieures pour l'accès à :

- Sites XenApp et XenDesktop
- Magasins StoreFront 2.6, 3.0, 3.5, 3.6, 3.7, 3.8, 3.9 et 3.11

Vous pouvez créer plusieurs stratégies de session sur le même serveur virtuel en fonction des éléments suivants :

- Type de connexion (par exemple, ICA, VPN sans client ou VPN)
- Type de déploiement Workspace (Workspace pour Web ou application Citrix Workspace installée localement).

Les stratégies peuvent être appliquées à partir d'un serveur virtuel unique.

Lorsque vos utilisateurs créent des comptes sur l'application Citrix Workspace, ils doivent entrer leur adresse e-mail ou le nom de domaine complet du serveur Citrix Gateway. À titre d'exemple, si la connexion échoue lors de l'utilisation du chemin d'accès par défaut, entrez le chemin d'accès complet au serveur Citrix Gateway.

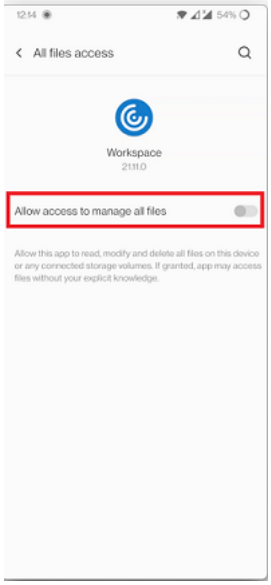
#### Fonctionnalité VPN

Vous pouvez accéder au Web interne, aux applications SaaS (Software-as-a-Service) et aux sites Web hébergés par votre entreprise, quel que soit votre emplacement d'accès. Vous pouvez accéder à ces ressources, hébergées par votre entreprise, sans connexion VPN. Cette fonctionnalité n'est disponible que pour les clients de magasins dans le cloud.

### Autoriser l'accès pour gérer tous les fichiers

Nous avons introduit l'option –**Autoriser l'accès pour gérer tous les fichiers**. Nous vous recommandons d'activer cette autorisation pour bénéficier de performances optimales. Vos fichiers restent sécurisés.




## Configurer

May 17, 2024

### Accès au microphone pour tous les magasins

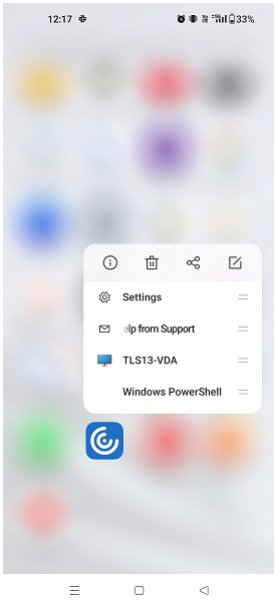
La fonctionnalité Client Selective Trust permet à l'application Citrix Workspace d'approuver l'accès à partir d'une session VDA. Vous pouvez accorder l'accès aux lecteurs clients locaux et aux périphériques matériels tels que les microphones et les webcams.

Auparavant, votre paramètre d'accès au microphone était appliqué à tous les magasins configurés.

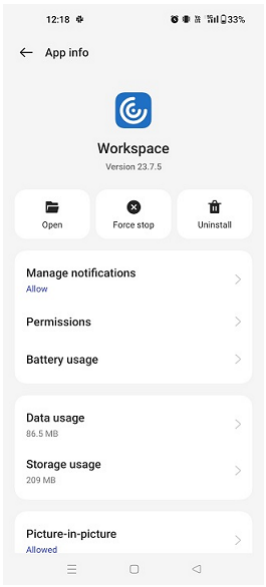
L'application Citrix Workspace requiert désormais l'autorisation de l'utilisateur final pour que chaque magasin puisse accéder au microphone. Autorisez l'accès au microphone comme suit :

1. Appuyez longuement sur l'icône de l'application Citrix Workspace et sur l'icône **Infos sur l'application** .

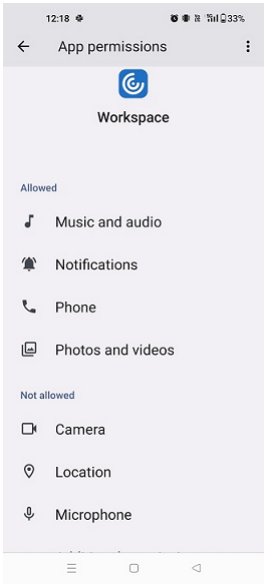



2. Appuyez sur **Autorisations**.

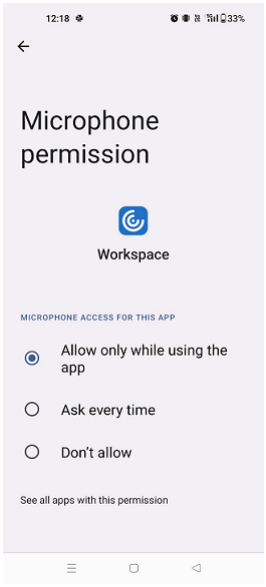



3. Appuyez sur **Microphone**.




4. Sélectionnez **Autoriser uniquement lorsque vous utilisez cette application**.

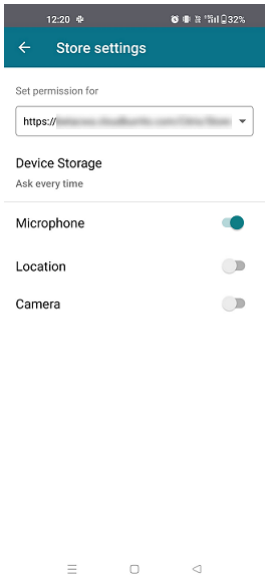



Vous pouvez désormais accéder au microphone lorsque vous utilisez l'application Citrix Workspace.

Configurez les niveaux d'accès comme suit :

1. Ouvrez l'application Citrix Workspace et sélectionnez **Paramètres** > **Paramètres du magasin**.
2. Sous l'option **Définir autorisation pour**, sélectionnez un magasin dans le menu déroulant.




3. Activez **Micro**.

   Le microphone est désormais activé. Vous pouvez vous en servir lorsque vous utilisez l'application Citrix Workspace sur votre appareil Android.

## Accès à l'emplacement pour chaque magasin

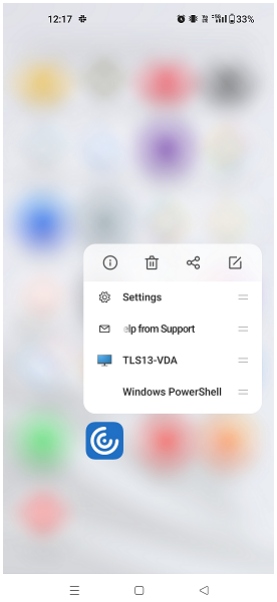
La fonctionnalité Client Selective Trust permet à l'application Citrix Workspace d'approuver l'accès à partir d'une session VDA.

Auparavant, votre paramètre d'accès à l'emplacement était appliqué à tous les magasins configurés.

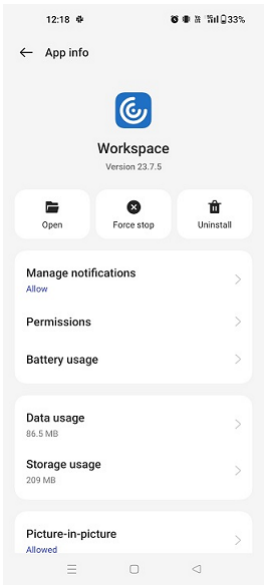
À compter de la version 21.3.0, l'application Citrix Workspace requiert l'autorisation de l'utilisateur final pour que chaque magasin puisse accéder à l'emplacement. Autorisez l'accès à l'emplacement comme suit :

1. Appuyez longuement sur l'icône de l'application Citrix Workspace et sur l'icône **Infos sur l'application** ⓘ.

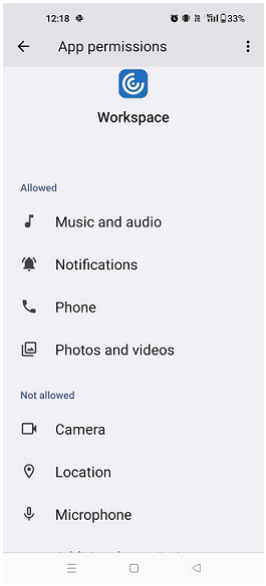



2. Appuyez sur **Autorisations**.

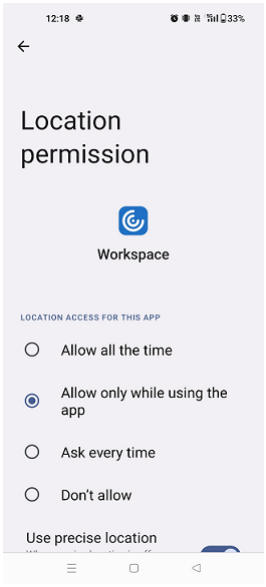



3. Appuyez sur **Localisation**.




4. Sélectionnez **Autoriser uniquement lorsque vous utilisez cette application**.

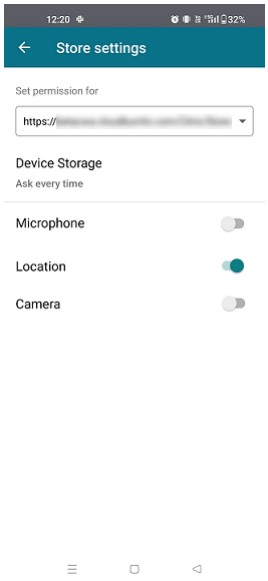



Vous pouvez désormais accéder à l'emplacement lorsque vous utilisez l'application Citrix Workspace.

Configurez les niveaux d'accès comme suit :

1. Ouvrez l'application Citrix Workspace et sélectionnez **Paramètres** > **Paramètres du magasin**.
2. Sous l'option **Définir autorisation pour**, sélectionnez un magasin dans le menu déroulant.




3. Activez **Emplacement**.

   L'emplacement est désormais activé. Vous pouvez vous en servir lorsque vous utilisez l'application Citrix Workspace sur votre appareil Android.

## Accès à la caméra pour tous les magasins

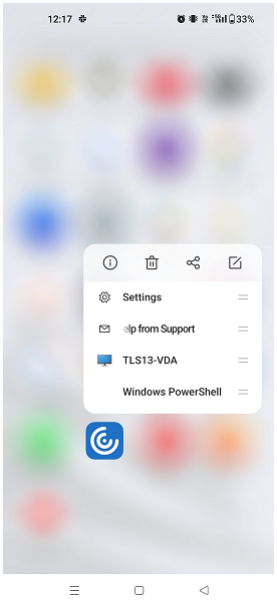
La fonctionnalité Client Selective Trust permet à l'application Citrix Workspace d'approuver l'accès à partir d'une session VDA. Vous pouvez accorder l'accès aux lecteurs clients locaux et aux périphériques matériels tels que les microphones et les webcams.

Auparavant, votre paramètre d'accès à la caméra était appliqué à tous les magasins configurés.

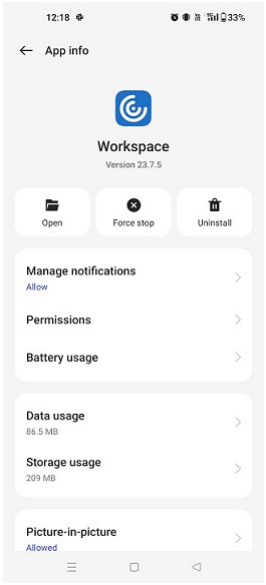
L'application Citrix Workspace requiert désormais l'autorisation de l'utilisateur final pour que chaque magasin puisse accéder à la caméra du téléphone. Autorisez l'accès à la caméra comme suit :

1. Appuyez longuement sur l'icône de l'application Citrix Workspace et sur l'icône **Infos sur l'application** .

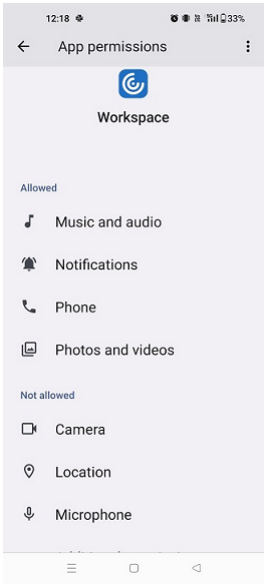



2. Appuyez sur **Autorisations**.

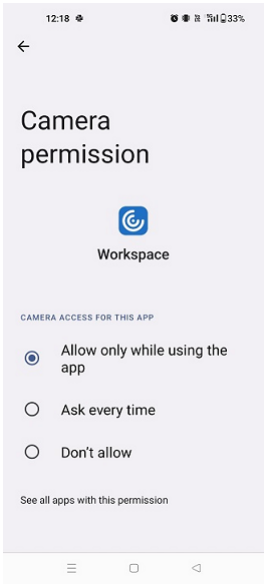



3. Appuyez sur **Caméra**.




4. Sélectionnez **Autoriser uniquement lorsque vous utilisez cette application**.

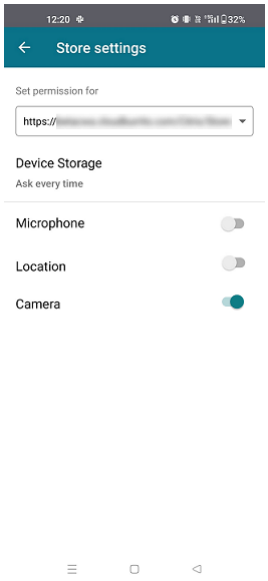



Vous pouvez désormais accéder à la caméra lorsque vous utilisez l'application Citrix Workspace.

Configurez les niveaux d'accès comme suit :

1. Ouvrez l'application Citrix Workspace et sélectionnez **Paramètres** > **Paramètres du magasin**.
2. Sous l'option **Définir autorisation pour**, sélectionnez un magasin dans le menu déroulant.




3. Activez **Caméra**.

   La caméra est désormais activée. Vous pouvez vous en servir lorsque vous utilisez l'application Citrix Workspace sur votre appareil Android.

## Gestion des feature flag

Si un problème survient avec l'application Citrix Workspace en production, nous pouvons désactiver dynamiquement une fonctionnalité affectée dans l'application Citrix Workspace même après la livraison de la fonctionnalité. Pour ce faire, nous utilisons des commutateurs de fonctionnalité et un service tiers appelé LaunchDarkly.

Vous n'avez pas besoin d'effectuer des configurations pour activer le trafic vers LaunchDarkly, sauf si un pare-feu ou un proxy bloque le trafic sortant. Dans ce cas, vous activez le trafic vers LaunchDarkly via des URL ou adresses IP spécifiques, en fonction des exigences de votre stratégie.

Vous pouvez activer le trafic et la communication vers LaunchDarkly des manières suivantes :

### Activer le trafic vers les URL suivantes

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- Firehose.launchdarkly.com
- mobile.launchdarkly.com
- app.launchdarkly.com

#### Répertorier les adresses IP dans une liste verte

Si vous devez répertorier les adresses IP dans la liste verte, consultez la liste des adresses IP publiques de LaunchDarkly pour obtenir une liste de toutes les plages d'adresses IP actuelles. Vous pouvez utiliser cette liste pour vérifier que les configurations du pare-feu sont mises à jour automatiquement en fonction des mises à jour de l'infrastructure. Pour plus d'informations sur l'état des modifications de l'infrastructure, consultez la page LaunchDarkly Status.

#### Configuration système requise pour LaunchDarkly

Vérifiez si les applications peuvent communiquer avec les services suivants si le split tunneling sur Citrix ADC est désactivé :

- Service LaunchDarkly.
- Service d'écoute APNs

#### Disposition pour désactiver le service LaunchDarkly

Vous pouvez désactiver le service LaunchDarkly sur les magasins sur site et dans le cloud.

Dans la configuration cloud, les administrateurs peuvent désactiver le service LaunchDarkly. L'administrateur peut définir l'attribut **enableLaunchDarkly** sur **False** dans le Global App Configuration Service.

```
    {

        "assignedTo": [
         "AllUsersNoAuthentication"
        ],
        "category": "Third Party Services",
        "settings": [
           {

            "name": "Enable Launch Darkly",
            "value": "true"
            }

        ],
        "userOverride": false
     }


<!--NeedCopy-->
```

Pour plus d'informations, consultez la documentation Global App Configuration Service.

Lors du déploiement local, procédez comme suit :

1. Dans un éditeur de texte, ouvrez le fichier **web.config** qui se trouve en général dans le répertoire `C:\inetpub\wwwroot\Citrix\Roaming`.
2. Recherchez l'élément de compte d'utilisateur dans le fichier (Store est le nom du compte de votre déploiement).

   Par exemple, `<account id=... name="Store">`. Avant la balise </account> , accédez aux propriétés de ce compte utilisateur :

   ```
   <properties>
   <clear/>
   </properties>

   <!--NeedCopy-->
   ```

3. Ajoutez la balise **enableLaunchDarkly** et définissez la valeur sur **false**.

   `<property name="enableLaunchDarkly"value="false"/>`

> **Remarque :**
>
> La plupart des fonctionnalités sont associées à un indicateur de fonctionnalité, et LaunchDarkly les contrôle. Dans les environnements où elle est désactivée, vous devez attendre au moins 90 jours pour bénéficier de cette fonctionnalité.

### Association de type de fichier

Pour garantir le bon fonctionnement de cette fonctionnalité, accédez aux paramètres de l'application Citrix Workspace et définissez l'option **Utiliser stockage de l'appareil** sur **Accès complet**. Une option supplémentaire, **Demander à chaque fois**, est également disponible. Elle vous invite à vous authentifier avant d'accéder au stockage de votre appareil dans une session.

> **Remarque :**
>
> L'option **Demander à chaque fois** est un paramètre qui s'applique à chaque session. Elle n'est pas transférée sur la prochaine session.

Quand vous sélectionnez **Demander à chaque fois**, tout accès généré par le système au stockage de votre appareil peut entraîner l'affichage de l'invite **Utiliser stockage de l'appareil** (par exemple, à la fermeture de session). Il s'agit du comportement attendu.

L'application Citrix Workspace lit et applique les paramètres configurés par les administrateurs dans Citrix Studio.
Pour appliquer la FTA dans une session, assurez-vous que les utilisateurs se connectent au serveur Store sur lequel la FTA est configurée.

Sur l'appareil utilisateur, sélectionnez le fichier que vous souhaitez ouvrir dans l'explorateur de fichiers et touchez **Ouvrir**. Le système d'exploitation Android offre une option permettant de lancer le fichier à l'aide de l'application Citrix Workspace (en appliquant la FTA configurée par l'administrateur) ou d'une application différente. En fonction de votre sélection antérieure, une application par défaut peut ou ne peut pas être définie. Vous pouvez changer l'application par défaut en utilisant l'option Changer défaut.

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement sur StoreFront et requiert Citrix Virtual Apps and Desktops version 7 ou ultérieure.

#### Problèmes connus et limitations de cette fonctionnalité

1. L'authentification par carte à puce peut être plus lente que l'authentification avec mot de passe. À titre d'exemple, après la déconnexion à une session, attendez environ 30 secondes avant d'essayer de vous reconnecter. L'application Citrix Workspace peut cesser de répondre si vous vous reconnectez trop rapidement à une session déconnectée.
2. L'authentification par carte à puce n'est pas prise en charge sur les batteries.
3. Certains utilisateurs peuvent disposer d'un code PIN global pour les cartes à puce. Toutefois, lorsque les utilisateurs ouvrent une session à un compte de carte à puce, ils doivent entrer le code PIN de la carte PIV, et non le code PIN global. Il s'agit d'une limitation liée au fournisseur tiers.
4. Citrix vous recommande de quitter et de redémarrer la session de l'application Citrix Workspace après vous être déconnecté du compte de la carte à puce.
5. L'utilisation de plusieurs cartes à puce USB n'est pas prise en charge.
6. Vous pouvez accéder uniquement aux formats de fichier MIME pris en charge par les applications Microsoft Office, Adobe Acrobat Reader et Bloc-notes à l'aide de la fonctionnalité d'association de type de fichier.

## CEIP (programme d'amélioration de l'expérience du client)

| Données collectées | Description | À quelles fins sont-elles utilisées ? |
|---|---|---|
| Données de configuration et d'utilisation | Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation à partir de l'application Citrix Workspace et les envoie automatiquement à Google Analytics pour Firebase. | Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de l'application Citrix Workspace. |

**Informations supplémentaires**

Citrix traite vos données conformément aux termes de votre contrat avec Citrix et les protège comme indiqué dans l'Annexe sur la sécurité des Services Citrix. Cette annexe est disponible sur Citrix Trust Center.

Vous pouvez désactiver l'envoi de données via le programme CEIP à Citrix et Google Analytics pour Firebase (à l'exception des deux éléments de données collectés pour Google Analytics pour Firebase indiqués par un * dans le tableau ci-dessous) comme suit :

1. Lancez l'application Citrix Workspace et sélectionnez **Paramètres**.
2. Sélectionnez **Préférences avancées**.

   La boîte de dialogue **Préférences avancées** s'affiche.
3. Désactivez l'option **Envoyer statistiques d'utilisation**.

> **Remarque :**
>
> - Aucune donnée n'est collectée pour les utilisateurs de l'Union européenne (UE), de l'Espace économique européen (EEE), de la Suisse et du Royaume-Uni (UK).

Les données spécifiques à CEIP collectées par Google Analytics pour Firebase sont les suivantes :

| Version du système d'exploitation* | Version de l'application Workspace* | Configuration de l'authentification | Informations sur l'appareil |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Méthode de lancement de session | Type de magasin Citrix | Configuration du mappage des lecteurs clients | |
| Informations de session | Utilisation de `Recieverconfig.txt` | Configuration de la redirection USB | Informations utilisateur sur HDX RTME |
| Configuration des connexions HTTP et HTTPS | Informations sur le protocole des connexions ICA | Action de révision de l'application Workspace | Désactiver la configuration de Firebase |
| Nombre de magasins ajoutés | Action de capture d'écran | Actions utilisateur liées à la fonctionnalité RSA | Nombre d'utilisateurs de l'application Workspace vs StoreFront |
| Action de mise à jour d'application | Mise à jour du système d'exploitation | Action d'affichage de l'écran | Suppression d'application |
| Connexions à la vue Web | Données effacées de l'application | Exécution d'application | Démarrage de session d'application |

### Migration d'un compte local vers un compte cloud

Les administrateurs peuvent migrer en toute transparence les utilisateurs d'une URL de magasin StoreFront local vers une URL Workspace. Les administrateurs peuvent effectuer la migration avec un minimum d'interaction de l'utilisateur à l'aide du Global App Configuration Service.

Pour configurer :

1. Accédez à l'URL de l'API des paramètres de Global App Configuration Store et saisissez l'URL du magasin cloud.
   Par exemple, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Accédez à **API Exploration** > **SettingsController** > **postDiscoveryApiUsingPOST** > touchez **POST**.
3. Touchez **INVOKE API**.
4. Entrez et chargez les détails de la charge utile. Entrez la date d'expiration du magasin StoreFront dans l'horodatage en millisecondes.

   Par exemple,

```
"migrationUrl": [
{


"url": "<cloud store url>"
"storeFrontValidUntil": "<epoch timestamp in milliseconds>",
 }

]   ,
<!--NeedCopy-->
```

5. Touchez **EXECUTE** pour lancer le service.

### Expérience de l'utilisateur final pour cette fonctionnalité

En tant qu'utilisateur final, si vous utilisez l'application Citrix Workspace pour la première fois, après une authentification réussie, l'écran de migration **Présentation du nouveau Citrix Workspace** s'affiche (s'il est éligible). Après avoir cliqué sur l'option **Essayez le nouveau Citrix Workspace**, la migration commence. Une fois la migration réussie, vous pouvez accéder au magasin Workspace (magasin cloud).

> **Remarque :**
>
> Vous pouvez ignorer la migration à trois reprises. Au-delà, la migration est forcée sans possibilité de l'ignorer.


Après avoir migré vers le magasin Workspace (cloud), vous pouvez afficher à la fois le magasin StoreFront et le magasin Workspace sous **Paramètres**. Lorsque vous passez d'un magasin cloud au magasin StoreFront local, un écran de commentaires s'affiche pour recueillir vos impressions.

> **Remarque :**
>
> Le magasin StoreFront a une date d'expiration. Après la date d'expiration, le magasin est supprimé.

### Utiliser la dernière version

Cette fonctionnalité vous permet d'utiliser la dernière version de l'application Citrix Workspace. Lorsque les utilisateurs utilisent une version de l'application Citrix Workspace antérieure à la version Playstore, l'invite intégrée à l'application leur demande d'effectuer une mise à jour avec la dernière version.

Lorsque vous appuyez sur **Mettre à jour**, la mise à jour s'effectue en arrière-plan et vous pouvez continuer à utiliser l'application. Vous pouvez voir la progression sur le Snackbar. Une fois le téléchargement terminé, la boîte de dialogue suivante s'affiche :

Appuyez sur **Relancer maintenant** pour utiliser la dernière version. Si vous appuyez sur **Plus tard**, l'invite de redémarrage de l'application s'affiche lors du prochain lancement de l'application.

### Prise en charge des canaux de Global App Configuration Service

À partir de la version 23.4.5, les administrateurs peuvent utiliser le Global App Configuration Service pour définir les paramètres et les tester avant de déployer la configuration auprès de tous les utilisateurs finaux. Ce processus garantit que les fonctionnalités ont été testées et validées avant le déploiement dans un environnement de production.

> **Remarque :**
>
> - L'application Citrix Workspace pour Android prend en charge les configurations **Valeur par défaut** et **Canal de test**. Par défaut, tous les utilisateurs utilisent le canal **Valeur par défaut**.

Pour plus d'informations, consultez la documentation Global App Configuration Service.

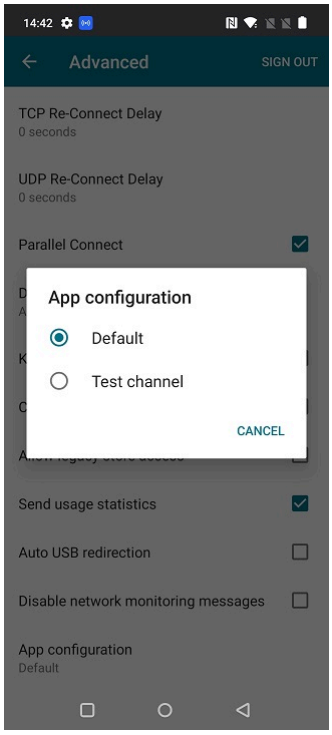
#### Comment utiliser cette fonctionnalité

Pour tester les configurations, procédez comme suit :

1. Accédez aux **paramètres** de l'application Citrix Workspace > **Avancé** > **Configuration d'applications**.

2. Sélectionnez le **canal de test**.




Vous pouvez maintenant démarrer le test.

> **Remarque :**
>
> - Assurez-vous que les configurations de l'application sont présentes sur le **canal de test**. Contactez l'administrateur de votre organisation pour obtenir de l'aide.

## Configurer l'application Citrix Workspace à l'aide des solutions de gestion unifiée des terminaux

April 18, 2024

### Prise en charge de la configuration du magasin à l'aide de solutions de gestion unifiée des terminaux

L'application Citrix Workspace pour Android prend désormais en charge la configuration à distance de l'URL de votre magasin Workspace à l'aide de solutions de gestion unifiée des terminaux. En tant qu'administrateur, vous pouvez gérer les URL des magasins à distance à l'aide de paires clé-valeur basées sur AppConfig à l'aide de solutions de gestion unifiée des terminaux.

Pour configurer l'URL de votre Workspace Store à l'aide de solutions de gestion unifiée des terminaux, procédez comme suit :

### Configurer votre magasin à l'aide de solutions de gestion unifiée des terminaux

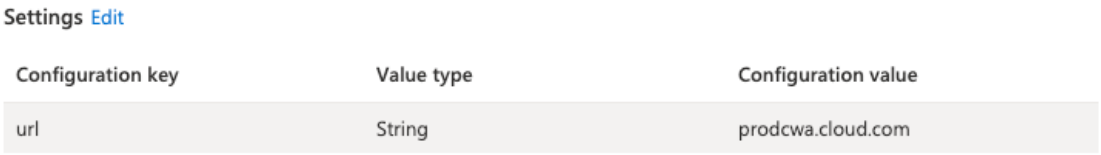
L'application Citrix Workspace pour Android prend en charge la configuration à distance de l'URL de votre magasin Workspace à l'aide de solutions de gestion unifiée des terminaux.

Pour configurer à distance l'URL de votre Workspace Store à l'aide de solutions de gestion unifiée des terminaux, procédez comme suit :

1. Connectez-vous à votre fournisseur de solutions de gestion unifiée des terminaux.
2. Créez une stratégie de configuration pour votre application.
3. Ajoutez une paire clé-valeur à la liste des propriétés JSON et renseignez les valeurs suivantes :

    - **clé :** url
    - **type de valeur :** chaîne
    - **valeur :** URL de votre magasin (par exemple, prodcwa.cloud.com)

> **Remarque :**
>
> - À des fins de démonstration, Microsoft Intune est utilisée comme solution de gestion unifiée des terminaux dans cet exemple. L'interface utilisateur affichée varie en fonction de votre fournisseur de solutions de gestion unifiée des terminaux.




### Limitations

- Si un magasin cloud est déjà configuré et que l'administrateur en configure un nouveau, votre magasin cloud existant et toutes les données ou tous les paramètres associés sont supprimés. Vous recevez une notification pour vous informer de la suppression dans Citrix Workspace. Vous devez ensuite vous reconnecter pour que le nouveau magasin cloud soit ajouté à Citrix Workspace.
- Pour appliquer de nouvelles configurations, vous devez fermer et rouvrir l'application Citrix Workspace.

### Prise en charge de la configuration du type de magasin

À partir de la version 23.6.0, l'application Citrix Workspace pour Android prend en charge la configuration du type de magasin à l'aide d'une paire clé-valeur basée sur AppConfig pour configurer l'application Citrix Workspace. Les administrateurs peuvent désormais contrôler l'affichage de l'application.

La paire clé-valeur se présente comme suit :

- **Clé :** storeType
- **Type de valeur :** entier
- **valeur :**

  Si ce paramètre est défini sur 1, les utilisateurs peuvent voir le magasin natif ou par défaut.
  Si ce paramètre est défini sur 2, les utilisateurs peuvent voir le magasin dans une interface Web.

> **Remarque :**
>
> Cette fonctionnalité ne nécessite pas d'activation.

### Contrôler les configurations des magasins à l'aide de solutions de gestion unifiée des terminaux

L'application Citrix Workspace pour Android a commencé à prendre en charge la configuration à distance de l'URL du magasin Workspace à l'aide de solutions de gestion unifiée des terminaux à partir de la version 23.4.5. En tant qu'administrateur, vous pouvez gérer les URL des magasins à distance à l'aide de paires clé-valeur basées sur AppConfig à l'aide de solutions de gestion unifiée des terminaux.

Pour plus d'informations, consultez la section Prise en charge de la configuration du magasin à l'aide de solutions de gestion unifiée des terminaux.

À partir de la version 23.7.5, les administrateurs peuvent configurer si les utilisateurs finaux peuvent modifier les URL des magasins à l'aide d'une paire clé-valeur basée sur AppConfig :

- **clé :** restrict_user_store_modification
- **type de valeur :** Boolean
- **valeur :**

  Si ce paramètre est défini sur **true**, les utilisateurs ne peuvent pas modifier le magasin (ajouter ou supprimer ou modifier).

  Si ce paramètre est défini sur **false**, les utilisateurs peuvent modifier le magasin.

> **Remarque :**
>
> Si l'indicateur **restrict_user_store_modification** est défini sur **true**, tous les magasins existants sont supprimés avant d'ajouter un nouveau magasin configuré pour la gestion unifiée des terminaux.

## Détection et prévention des captures d'écran grâce aux solutions Unified Endpoint Management

À partir de la version 23.10.0, les administrateurs peuvent empêcher les utilisateurs finaux de prendre des captures d'écran au niveau de l'application Citrix Workspace. Cette fonctionnalité empêche les fuites d'informations sensibles ou privées. Les administrateurs peuvent configurer cette fonctionnalité à l'aide d'une paire clé-valeur basée sur AppConfig :

- clé : restrictScreenshot
- type de valeur : Boolean
- valeur :

  Si ce paramètre est défini sur True, les utilisateurs finaux ne peuvent pas prendre de captures d'écran.

  Si ce paramètre est défini sur False, les utilisateurs finaux peuvent prendre des captures d'écran.

## Transférer les paramètres de l'application Citrix Workspace via UEM

Auparavant, vous pouviez configurer l'URL du magasin dans l'application Citrix Workspace.

À partir de cette version, vous pouvez configurer les paramètres de l'application Citrix Workspace sur les appareils gérés via n'importe quel outil de solution de gestion unifiée des terminaux (UEM) déployé dans votre infrastructure.

> **Remarque :**
>
> En tant qu'administrateur, si vous avez la possibilité de configurer les paramètres de l'application Citrix Workspace à l'aide d'UEM et du Global App Configuration Service (GACS), UEM a toujours la préférence sur GACS.

### Configurations

Les données JSON suivantes sont un exemple de MS Intune qui montre comment configurer cette fonctionnalité.

```
{

    "kind": "androidenterprise#managedConfiguration",
    "productId": "app:com.citrix.Receiver",
    "managedProperty": [
        {

            "key": "stores",
            "valueBundleArray": [
                {

                    "managedProperty": [
                        {

                            "key": "url",
                            "valueString": ""
                         }
,                        {

                            "key": "storeType",
                            "valueInteger": 1
                         }
,                        {

                            "key": "displayName",
                            "valueString": ""
                         }

                    ]
                }

            ]
         }
,        {

            "key": "url",
            "valueString": "prodcwa.cloud.com"
         }
,        {

            "key": "storeType",
            "valueInteger": 1
         }
,        {

            "key": "displayName",
            "valueString": ""
         }
```

```
,
        {

            "key": "restrict_user_store_modification",
            "valueBool": false
         }
,
        {

            "key": "restrictScreenshot",
            "valueBool": true
         }
,
        {

            "key": "appSettings",
            "valueBundleArray": [
                {

                    "managedProperty": [
                        {

                            "key": "name",
                            "valueString": ""
                         }
,
                        {

                            "key": "value",
                            "valueString": ""
                         }
,
                        {

                            "key": "userOverride",
                            "valueBool": false
                         }

                    ]
                }

            ]
         }

    ]
}


<!--NeedCopy-->
```

**Tableau des paires clé-valeur**

Le tableau suivant fournit des informations sur les paires clé-valeur :

| Paramètre | Description | Clé | Valeur | Type de valeur | Valeur par défaut |
|---|---|---|---|---|---|
| Audio | Permet aux utilisateurs de contrôler la connexion audio et microphone dans l'application ou le bureau. | audioRecordingSettingsKey | Lecture et enregistrement | Chaîne | Lecture et enregistrement |
| Prédiction de texte | Active les suggestions de texte pendant que l'utilisateur tape. | predictiveText | FAUX | Booléen | FAUX |
| Clavier étendu | Active la prise en charge du clavier étendu dans une session. | showExtendedKeyboard | TRUE | Booléen | TRUE |
| Redirection USB générique | Active la redirection automatique de périphériques USB arbitraires de la machine cliente vers le VDA. | autoUSB | TRUE | Booléen | FAUX |

| Paramètre | Description | Clé | Valeur | Type de valeur | Valeur par défaut |
|---|---|---|---|---|---|
| Confirmation de la déconnexion de la session par l'utilisateur (Demander avant de quitter) | Affiche une boîte de dialogue de confirmation qui permet à l'utilisateur de confirmer avant de déconnecter une session. | askBeforeExiting | TRUE | Booléen | TRUE |
| Redirection du Presse-papiers (Presse-papiers) | Permet à l'utilisateur d'utiliser les opérations du presse-papiers, telles que Couper, Copier et Coller dans une session. | clipboardAccess | TRUE | Booléen | FAUX |
| Transport adaptatif (EDT) | Active Enlightened Data Transport comme protocole préféré par rapport à TCP pour optimiser le transport des données. | edtSetting | TRUE | Booléen | TRUE |

| Paramètre | Description | Clé | Valeur | Type de valeur | Valeur par défaut |
|---|---|---|---|---|---|
| Orientation de l'affichage | Permet aux utilisateurs de sélectionner l'orientation de l'affichage en fonction de la position de l'appareil. | displayOrientationKey | Mode Paysage | Chaîne | Automatique |
| Garder l'écran activé | Maintient l'affichage actif et l'écran allumé. | keepscreenOnKey | TRUE | Booléen | FAUX |
| Validation stricte des certificats | Applique un contrôle plus strict de la validation du certificat du serveur. | strictcertificatevalidation | TRUE | Booléen | FAUX |
| Accès aux anciens magasins | Permet aux utilisateurs d'accéder aux versions antérieures du magasin. | allowlegacystoreaccess | TRUE | Booléen | FAUX |
| RealTime Media Engine | Active la prise en charge des appels audio et vidéo haute définition. | RTMEAccess | TRUE | Booléen | FAUX |

| Paramètre | Description | Clé | Valeur | Type de valeur | Valeur par défaut |
|---|---|---|---|---|---|
| Redirection USB automatique | Active la redirection automatique de périphériques USB arbitraires de la machine cliente vers le VDA. | autoUSB | TRUE | Booléen | FAUX |
| Messages de surveillance du réseau | Désactive les messages d'alerte qui fournissent des détails sur les performances du réseau. | DisableChannelMonitoringWarnings | FAUX | Booléen | FAUX |
| Touches étendues | Raccourcis à utiliser pour le clavier de session. | key_map | ["strAltTab", "strAlt", "str-Backspace", "strAltF4"] | MultiList | null |
| LaunchDarkly | Active l'indicateur LaunchDarkly sur les fonctionnalités de l'application Citrix Workspace. | enableLaunchDarkly | TRUE | Booléen | TRUE |

Voici un exemple de données JSON. L'exemple affiche ici différentes valeurs de réglage, telles que :

- Booléen
- Entier
- Chaîne
- Liste des chaînes

```
{

    "kind": "androidenterprise#managedConfiguration",
    "productId": "app:com.citrix.Receiver",
    "managedProperty": [
        {

            "key": "stores",
            "valueBundleArray": [
                {

                    "managedProperty": [
                        {

                            "key": "url",
                            "valueString": ""
                         }
,                        {

                            "key": "storeType",
                            "valueInteger": 1
                         }
,                        {

                            "key": "displayName",
                            "valueString": ""
                         }

                    ]
                }

            ]
         }
,        {

            "key": "url",
            "valueString": "your_store_url"
         }
,        {

            "key": "storeType",
            "valueInteger": 1
         }
,        {

            "key": "displayName",
            "valueString": ""
         }
```

```
,
        {

            "key": "restrict_user_store_modification",
            "valueBool": false
         }
,
        {

            "key": "restrictScreenshot",
            "valueBool": true
         }
,
        {

            "key": "appSettings",
            "valueBundleArray": [
                {

                    "managedProperty": [
                        {

                            "key": "name",
                            "valueString": "showExtendedKeyboard"
                         }
,
                        {

                            "key": "value",
                            "valueString": "false"
                         }
,
                        {

                            "key": "userOverride",
                            "valueBool": false
                         }

                    ]
                 }
,
                {

                    "managedProperty": [
                        {

                            "key": "name",
                            "valueString": "enterRegion"
                         }
,
                        {

                            "key": "value",
```

```
                                "valueString": "-40"
                            }
    ,
                            {

                                "key": "userOverride",
                                "valueBool": false
                            }

                        ]
                    }
    ,
                    {

                        "managedProperty": [
                            {

                                "key": "name",
                                "valueString": "displayOrientationKey"
                            }
    ,
                            {

                                "key": "value",
                                "valueString": "Landscape mode"
                            }
    ,
                            {

                                "key": "userOverride",
                                "valueBool": false
                            }

                        ]
                    }
    ,
                    {

                        "managedProperty": [
                            {

                                "key": "name",
                                "valueString": "askBeforeExiting"
                            }
    ,
                            {

                                "key": "value",
                                "valueString": "true"
                            }
    ,
                            {

```

```
                                "key": "userOverride",
                                "valueBool": false
                            }

                        ]
                    }
    ,
                   {

                        "managedProperty": [
                            {

                                "key": "name",
                                "valueString": "key_map"
                            }
    ,
                            {

                                "key": "value",
                                "valueString": "['strAltTab','strAlt','
                                   strBackspace','strAltF4']"
                            }
    ,
                            {

                                "key": "userOverride",
                                "valueBool": true
                            }

                        ]
                    }

                ]
            }

        ]
    }

<!--NeedCopy-->
```

## Périphériques

May 17, 2024

## Mode de saisie Scancode pour clavier externe

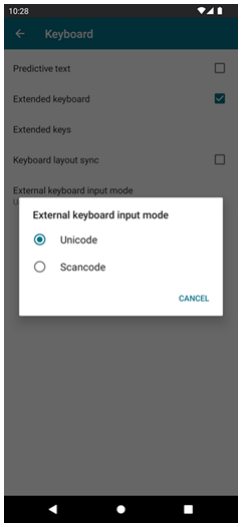
À partir de la version 24.1.0, vous pouvez sélectionner Scancode comme mode de saisie au clavier lorsque vous utilisez un clavier physique externe. Cette fonctionnalité est utile lorsque vous utilisez des appareils Android dotés du clavier standard d'un PC Windows externe. Son utilisation est semblable à celle de la fonctionnalité Samsung DeX.

Avec Scancode, vous pouvez utiliser la disposition du clavier du VDA au lieu de celle du clavier logiciel d'Android. De cette façon, vous pouvez suivre complètement le style de saisie de Windows au lieu de celui d'Android. C'est utile lorsque vous effectuez des saisies dans des langues d'Asie de l'Est, car cela améliore considérablement l'expérience utilisateur globale. L'utilisateur final peut se retrouver à utiliser la disposition du clavier du serveur au lieu de celle du client. Pour en savoir plus, consultez la section Cas d'utilisation de cet article.

### Comment utiliser cette fonctionnalité

Pour utiliser la fonctionnalité Scancode, procédez comme suit :

1. Ouvrez l'application Citrix Workspace pour Android et accédez à **Paramètres** > **Général** > **Clavier**.
2. Appuyez sur **Mode de saisie du clavier externe**.




3. Sélectionnez l'une des options suivantes :
    - **Scancode :** la position des touches du clavier côté client est envoyée au VDA et le VDA génère le caractère correspondant. Applique la disposition du clavier côté serveur.
    - **Unicode** : la touche du clavier côté client est envoyée au VDA et le VDA génère le même caractère dans le VDA. Applique la disposition du clavier côté client.

Par défaut, **Unicode** est sélectionné comme mode de saisie du clavier externe.

4. Appuyez sur **Scancode**.

   En cours de session, vous pouvez changer de clavier distant à l'aide de la fonction IME et saisir les données dans la disposition du clavier du serveur.

#### Cas d'utilisation

Par exemple, imaginez un scénario dans lequel vous utilisez une disposition de clavier internationale américaine connectée à votre appareil Android.

Lorsque vous choisissez **Scancode** et que vous appuyez sur la touche à côté de Verr Maj sur votre clavier externe, le Scancode 1E est envoyé au VDA. Le VDA utilise ensuite 1E pour afficher le caractère a.

Si vous choisissez **Unicode** et que vous appuyez sur la touche à côté de Verr Maj sur votre clavier externe, le caractère a est envoyé au VDA. Ainsi, même si le VDA utilise une autre disposition de clavier comportant un caractère différent à la même position, le caractère a apparaît à l'écran.

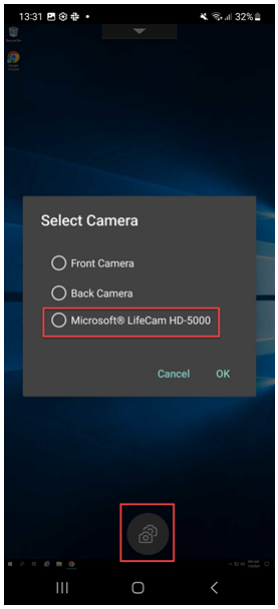
> **Remarque :**
>
> Unicode est le mode de saisie à privilégier lorsque vous utilisez un clavier tactile sur vos appareils mobiles. En effet, les touches d'un clavier tactile ne génèrent généralement pas de Scancode.

### Prise en charge de la webcam externe

L'application Citrix Workspace pour Android prend désormais en charge les webcams connectées en externe lors de vos sessions. Connectez une webcam USB et utilisez-la pour la visioconférence en appuyant sur l'icône de la caméra, puis en sélectionnant le nom de la webcam externe. Cela améliore l'expérience de session des utilisateurs en utilisant des ressources qui leur sont disponibles.

> **Remarque :**
>
> Le nom de la webcam externe ne s'affiche que lorsqu'une caméra externe est détectée.




La prochaine fois que vous utiliserez une application de visioconférence, le système mémorisera et appliquera les préférences d'utilisation de la caméra. Par exemple, si vous avez effectué votre dernier appel vidéo avec la préférence Webcam externe, la prochaine fois, la Webcam externe est sélectionnée par défaut.

Vous pouvez modifier vos préférences de caméra en appuyant sur l'icône de la caméra affichée sur votre écran. Il est également possible de modifier les préférences de caméra pendant les appels.

> **Remarque :**
>
> - Lorsque vous retirez la caméra externe, l'icône flottante à plusieurs caméras se transforme en une. La boîte de dialogue **Sélectionner une caméra** se ferme si elle est ouverte et que la vue de la caméra externe sur le VDA ne répond plus.
> - Cette fonctionnalité est applicable aux déploiements locaux et dans le cloud.

### Mappage des lecteurs clients

L'application Citrix Workspace informe le serveur des lecteurs clients disponibles. Par défaut, les lecteurs clients sont mappés sur des lettres de lecteur serveur de façon à sembler être directement connectés à la session. Ces mappages sont accessibles à l'utilisateur actuel et dans la session en cours uniquement.

> **Remarque :**
>
> Cette fonctionnalité est prise en charge uniquement sur les versions d'Android exécutant le SDK version 24 et versions ultérieures.

Le mappage des lecteurs clients (CDM) autorise l'utilisation de périphériques de stockage plug-and-

play dans une session. Ainsi, vous pouvez utiliser des périphériques de stockage de masse (par exemple des clés mémoire) pour copier et coller des documents entre une clé mémoire et la machine utilisateur.

En outre, si le paramètre CDM est défini sur Accès complet ou Accès en lecture, vous pouvez utiliser la mémoire interne de l'appareil comme lecteur mappé à la session.

**Limitations des fonctionnalités :**

- Il a été observé que les API Android étaient lentes, ce qui ralentit certaines opérations.
- Le CDM pour le stockage externe n'est pas pris en charge sur les Pixel.
- L'association de type de fichier n'est pas prise en charge sur les périphériques de stockage externes.

**Problème connu dans cette fonctionnalité :**

- L'écran de l'application Workspace peut passer du premier plan à l'arrière-plan lorsque vous branchez un périphérique de stockage externe.

#### Amélioration du mappage des lecteurs clients

Précédemment, une option de stockage de périphérique sélectionnée était appliquée à tous les magasins configurés.

À compter de la version 20.8.0, l'application Citrix Workspace vous permet de sélectionner un espace de stockage dédié pour chaque magasin configuré.

Vous obtenez une invite pour sélectionner le type de stockage de périphérique ainsi que les détails du magasin lors du lancement de la session. Vous pouvez effectuer l'une des opérations suivantes :

- Sélectionnez l'une des options de périphérique de stockage et touchez **OK**. Le choix ne s'applique qu'à la session en cours. Une invite s'affiche pour sélectionner le type de stockage de périphérique à chaque lancement.
- Sélectionnez l'une des options de périphérique de stockage, sélectionnez **Ne plus demander** et touchez **OK**. Le choix s'applique à toutes les ouvertures de session pour ce magasin. Aucune autre invite ne s'affiche.
- Sélectionnez **Annuler** - Vous êtes invité à sélectionner un type de stockage de périphérique à chaque lancement et au sein d'une session. La session n'a pas accès au stockage de périphérique.

> **Remarque :**
>
> Cette fonctionnalité s'applique uniquement aux lancements ICA directs et aux magasins config-

> urés pour Citrix Gateway. Les magasins avec configuration SSL de bout en bout sont pris en charge.

## Citrix Casting

Citrix Casting combine des environnements numériques et physiques pour fournir des applications et des données dans un espace intelligent sécurisé. Le système complet connecte des appareils (ou objets), comme des applications mobiles et des capteurs, pour créer un environnement intelligent et réactif.

Citrix Ready Workspace Hub est basé sur la plate-forme Raspberry Pi 3. L'appareil exécutant l'application Citrix Workspace se connecte au Citrix Ready Workspace Hub et diffuse les applications ou les bureaux sur un écran plus grand.

Citrix Casting vous permet de :

- Itinérer votre session sans lancer de session VDA sur les appareils mobiles.
- Afficher la liste des Workspace Hub disponibles en appuyant sur **Afficher la liste des hubs** dans la boîte de dialogue de **Workspace Hub**.

### Configurer Citrix Casting

Citrix Casting est activé lorsque toutes les conditions suivantes sont remplies :

- Application Citrix Workspace 1809 pour Android installée ou version supérieure
- Bluetooth activé
- Emplacement activé
- Appareil mobile et hub d'espace de travail utilisant le même réseau Wi-Fi

Pour activer la fonctionnalité Citrix Casting, appuyez sur **Paramètres** et **Citrix Casting** sur votre appareil.

Pour plus d'informations sur Citrix Ready Workspace Hub dans l'application Citrix Workspace, consultez la section Configurer Citrix Ready Workspace Hub.

Pour plus d'informations sur Citrix Ready Workspace Hub, consultez la documentation relative à Citrix Ready Workspace Hub.

## Carte à puce USB

L'application Citrix Workspace prend en charge les lecteurs de carte à puce USB avec StoreFront. Vous pouvez utiliser des cartes à puce USB aux fins suivantes :

- Ouverture de session par carte à puce - Authentifie les utilisateurs auprès de l'application Citrix Workspace.
- Prise en charge des applications recourant à une carte à puce - Permet aux applications publiées recourant à une carte à puce d'accéder aux lecteurs de carte à puce locaux.

L'application Citrix Workspace prend en charge cette fonctionnalité sur tous les appareils Android répertoriés par Biometric Associates.

L'application Citrix Workspace prend en charge les types de cartes à puce USB suivants :

- Cartes Personal Identity Verification (PIV).
- Cartes CAC

Les cartes à puce USB sont prises en charge sur le système d'exploitation Android de la version 7.x à 11.x.

Vous pouvez également activer l'authentification par carte à puce USB à partir de **Paramètres** > **Gérer les comptes**.

#### Configuration de cartes à puce USB

**Conditions préalables :**

- Téléchargez et installez le service Android PC/SC-Lite à partir du Google Play Store.

1. Connectez le lecteur de carte à puce USB au périphérique mobile. Pour plus d'informations sur la connexion des lecteurs de carte à puce, reportez-vous aux spécifications du lecteur de carte à puce fournies par le fabricant.
2. Ajoutez un compte StoreFront compatible avec la carte à puce.
3. Sur la page d'ouverture de session de l'application Citrix Workspace, appuyez sur **Ajouter un compte**. Appuyez sur l'option **Utiliser carte à puce**.
4. Pour modifier un compte existant afin d'utiliser l'authentification par carte à puce USB, appuyez sur **Comptes** > **Modifier**, puis sur l'option **Utiliser carte à puce**.

### Prise en charge de la redirection de webcam

Vous pouvez désormais rediriger la caméra frontale de votre appareil vers la session. Les applications 32 bits et 64 bits sont prises en charge. Par défaut, la redirection automatique de la webcam est désactivée.

### Prise en charge de la redirection des caméras avant et arrière

L'application Citrix Workspace pour Android vous permet désormais de changer la position de la caméra de l'avant vers l'arrière et inversement, au cours de la session HDX. Les applications 32 bits et 64 bits sont prises en charge.

Un bouton flottant apparaît lorsque vous appelez la caméra. Appuyez une fois sur le bouton flottant pour basculer entre les positions avant et arrière de la caméra. Vous pouvez également déplacer librement le bouton flottant sur l'écran et le placer n'importe où.

#### Problèmes connus liés à cette fonctionnalité

- Le bouton flottant est partiellement ou totalement obstrué lorsque la fonction de casting ou de numérisation de documents est activée.

### Prise en charge des microphones externes

Auparavant, l'application Citrix Workspace pour Android ne prenait en charge que la redirection audio via le microphone de l'appareil.

À partir de la version 23.10.5, l'application Citrix Workspace pour Android prend en charge les microphones externes. Les microphones peuvent être des périphériques USB ou Bluetooth.

Une fois que vous avez connecté un microphone USB ou Bluetooth, le son est redirigé du microphone externe vers la session. Lorsque vous retirez le microphone externe de l'appareil, le son est automatiquement redirigé vers le microphone de l'appareil.

Cette fonctionnalité est utile lorsque vous connectez un microphone externe, par exemple, à :

- un téléphone ;
- une tablette ;
- une smart TV ;
- un moniteur externe dans une salle de conférence.

## Étendre l'affichage

March 22, 2024

### Prise en charge de Zebra Workstation Connect

Avec cette version, nous introduisons la compatibilité avec les fonctionnalités de la tablette Zebra : lanceur de bureau et expérience en mode bureau. L'expérience utilisateur de la tablette Android est reflétée sur le moniteur client avec Zebra Workspace Connector.

L'application Citrix Workspace prend en charge les appareils Zebra suivants :

- Ordinateurs portables EC50, EC55, ET56
- TC52x,
- TC57x,
- TC52ax,
- TC52x-HC
- TC52ax-HC

Pour plus d'informations sur la gestion des appareils Zebra, consultez la section Gérer les appareils Zebra Android dans la documentation Citrix Analytics for Performance.

### Prise en charge de plusieurs écrans sur Samsung DeX

La fonctionnalité Samsung DeX (Desktop eXperience) est disponible sur certains appareils portables Samsung haut de gamme. La fonctionnalité DeX vous permet de bénéficier d'une expérience similaire à celle d'un ordinateur de bureau sur votre appareil en connectant un clavier, une souris et un moniteur.

Vous pouvez connecter votre appareil compatible DeX et l'écran externe pour étendre la session de bureau sur l'écran externe. L'écran externe doit prendre en charge le protocole DeX. Vous pouvez étendre ou afficher un contenu différent sur l'écran Samsung DeX et l'écran externe.

> **Important :**
>
> - Cette fonctionnalité s'applique uniquement à la plateforme Samsung DeX et non à ChromeOS ou aux autres appareils Android.
> - Cette fonctionnalité s'applique uniquement aux sessions de bureau Citrix et non aux sessions d'application.
> - L'icône **Étendre** n'est disponible que sur l'écran DeX. Démarrez la session de bureau à partir de l'écran DeX.
> - La résolution de l'écran externe dépend de l'appareil Samsung DeX, de l'écran externe et des autres matériels utilisés.

#### Configurer le mode Étendre

Pour activer le mode **Étendre** :

1. Connectez l'appareil compatible avec le protocole Samsung DeX au moniteur externe à l'aide du câble. Vous pouvez également connecter un appareil compatible Samsung DeX à un moniteur Samsung. Le moniteur Samsung doit prendre en charge le protocole DeX en mode sans fil.

   > **Remarque :**
   >
   > La configuration fonctionne mieux avec les adaptateurs USB Type-C HDMI et USB-C Dock.

2. Ouvrez l'application Citrix Workspace et démarrez une session de bureau à partir de l'écran Samsung DeX.
3. Accédez à la barre d'outils et appuyez sur l'icône **Étendre**.
   

   > **Conseil :**
   >
   > Pour supprimer l'extension d'écran, appuyez de nouveau sur l'icône **Étendre**.
   > 

4. Utilisez la fonction glisser-déposer pour déplacer la fenêtre de l'application vers le moniteur externe.

   > **Limitation :**
   >
   > Relâchez le pointeur de la souris sur le bord de l'écran lorsque vous faites glisser une fenêtre sur un autre écran. Poursuivez l'action de glisser-déposer à l'aide de la souris depuis l'écran cible pour déplacer la fenêtre.

> **Remarque :**
>
> - Vous pouvez faire pivoter l'écran de l'appareil en fonction de vos besoins.
> - Ajustez la taille de police pour une meilleure lisibilité dans les paramètres d'affichage de session sous la section **Mise à l'échelle et disposition**.

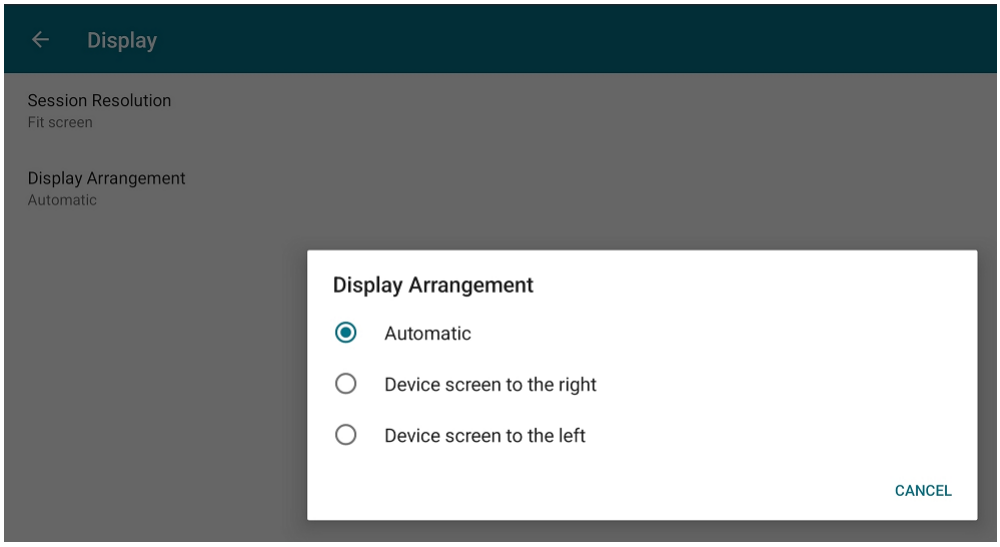
#### Configurer la disposition de l'affichage

Pour configurer la disposition de l'affichage :

> **Conditions préalables**
> :
> Configurez la disposition de l'affichage avant de démarrer la session.

1. Ouvrez l'application Citrix Workspace et accédez à l'icône **Paramètres** > **Paramètres** > **Général** > **Affichage** > **Disposition de l'affichage**.




2. Sélectionnez une option appropriée.
   L'écran de l'appareil apparaît à droite ou à gauche.

> **Important :**
>
> - L'écran Samsung DeX est l'écran principal.
> - Seul un écran peut afficher l'interface utilisateur de l'application Citrix Workspace.
> - Vous ne pouvez brancher qu'un seul écran externe.
> - L'application Citrix Workspace se ferme lorsque vous démarrez une session.

## Expérience utilisateur

March 22, 2024

### Délai d'inactivité pour les sessions d'application Citrix Workspace

L'administrateur peut spécifier la durée d'inactivité autorisée. Après expiration du délai d'inactivité, une invite d'authentification s'affiche.

La valeur du délai d'inactivité définie doit être comprise entre 1 et 24 heures. Par défaut, le délai d'inactivité n'est pas configuré. Les administrateurs peuvent configurer la propriété **inactivityTimeoutInMinutesMobile** à l'aide d'un module PowerShell. Touchez ici pour télécharger les modules PowerShell nécessaires à la configuration de l'application Citrix Workspace.

Lorsque vous atteignez la valeur du délai d'inactivité spécifiée, l'expérience utilisateur est la suivante en fonction du type d'authentification configuré :

- Une fois le délai d'inactivité dépassé, vous serez invité à fournir une authentification biométrique pour accéder à nouveau à l'application Citrix Workspace.
- Si vous pouvez annuler l'invite d'authentification biométrique, le message suivant s'affiche :

  **L'application Citrix Workspace est verrouillée.**

  Vous devez vous authentifier pour continuer à utiliser l'application Workspace.
- Si le code d'accès n'est pas configuré sur Android, vous devez vous connecter avec des informations d'identification après l'expiration du délai d'inactivité.

> **Remarque :**
>
> Cette fonctionnalité s'applique uniquement aux clients de Workspace (Cloud).

### Prise en charge de l'authentification biométrique après une période d'inactivité

Une fois le délai d'inactivité expiré, l'utilisateur final est invité à s'authentifier à l'aide de fonctionnalités biométriques telles que la reconnaissance faciale et la lecture d'empreintes digitales.

La forme d'authentification biométrique la plus robuste disponible pour l'utilisateur final dépend de l'OEM de son périphérique, et il est invité en fonction de celle-ci.

Pour plus d'informations sur la configuration du délai d'inactivité, consultez la section Délai d'inactivité pour les sessions d'application Citrix Workspace.

### Option pour désactiver l'affichage des messages d'erreur

Vous pouvez maintenant désactiver l'affichage du message d'erreur suivant lié à la surveillance du réseau :

« La connexion peut être temporairement lente. »

Pour désactiver le message d'erreur relatif aux problèmes réseau dans une session, accédez à **Avancé** et sélectionnez l'option **Désactiver les messages de surveillance du réseau**.

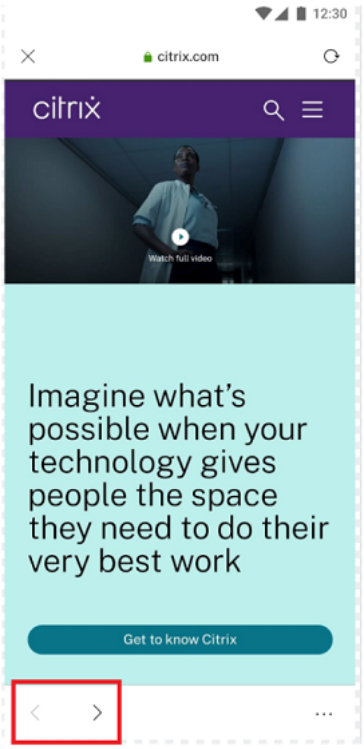
### Améliorations apportées à l'interface utilisateur

- À compter de la version 20.7.0, vous pouvez maintenant supprimer les détails du compte d'un magasin depuis l'option **Modifier**. Touchez **Supprimer le compte** pour supprimer les détails du compte.
- À compter de la version 20.7.5, l'onglet **Récent** affiche les applications mobiles natives ainsi que les applications et les bureaux publiés.

- À compter de la version 20.10.0, l'application Citrix Workspace prend en charge les exigences actuelles de l'API cible de Google Play pour Android 10.
- À compter de la version 20.10.0, vous recevez une notification concernant une connexion non sécurisée lorsque vous essayez d'ajouter un magasin HTTP.
- À compter de la version 21.3.5, vous pouvez naviguer dans les deux sens dans les applications Web et SaaS (Software-as-a-Service).

  Les boutons de navigation s'affichent en bas à gauche de votre session d'application SaaS et d'espace de travail Web sur votre téléphone mobile.



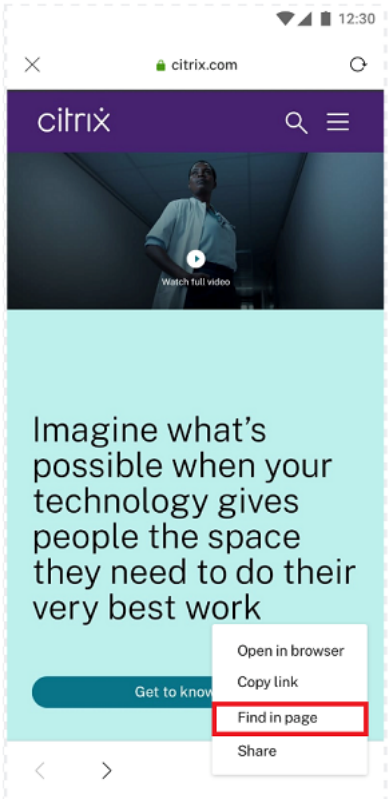

  Les boutons de navigation apparaissent en haut à gauche de la session d'application SaaS de votre tablette.

- À compter de la version 21.4.0, vous pouvez rechercher des mots ou des phrases dans vos applications Web et SaaS (Software-as-a-Service).

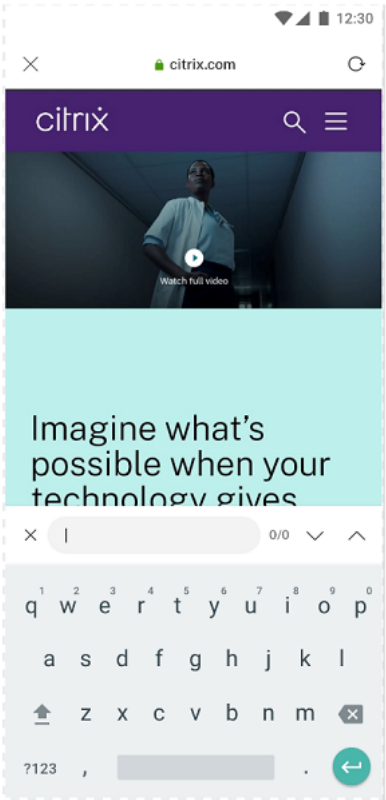
  Pour effectuer une recherche, procédez comme suit.

  1. Touchez le bouton représentant des points de suspension en bas à droite et sélectionnez **Rechercher dans la page**.

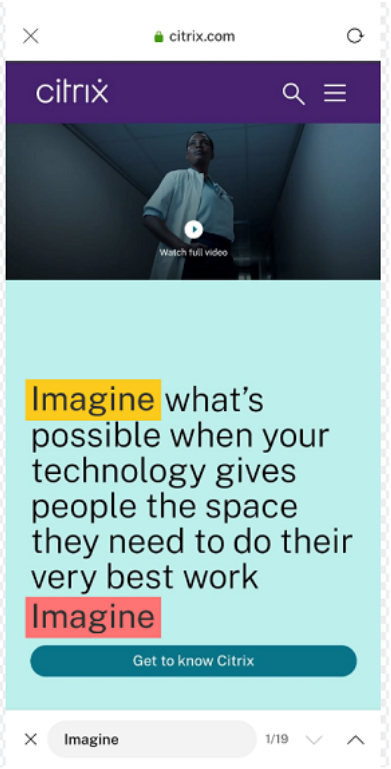



1. Le clavier apparaît.



1. Une fois le texte entré, votre résultat de recherche apparaît (par exemple, le mot « imagine »).




- À compter de la version 21.6.0, vous pouvez télécharger des fichiers texte, audio et vidéo (avec et sans liens directs). Pour les fichiers texte, audio et vidéo avec des liens directs, téléchargez-les directement en appuyant sur le lien. Vous pouvez prévisualiser les fichiers audio et vidéo avant de les télécharger.

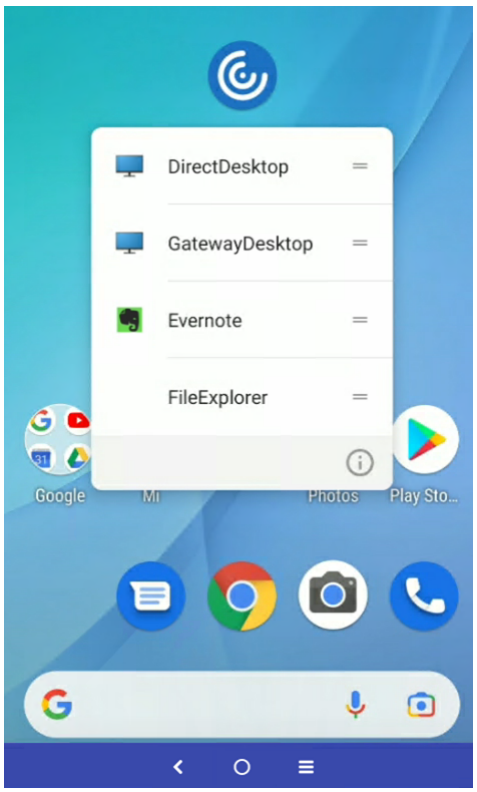
  Pour télécharger des fichiers sans lien direct, appuyez sur le bouton de points de suspension en bas à droite et sélectionnez **Télécharger.**


Une fois le téléchargement terminé, une notification indique que le fichier est enregistré dans votre dossier de téléchargements.

- À compter de la version 21.8.5, nous prenons désormais en charge Android 12 Beta 4 dans l'application Citrix Workspace pour Android. La mise à niveau vers l'application Citrix Workspace version 21.8.5 garantit une prise en charge ininterrompue des appareils mis à jour vers Android 12 Beta 4.
- À compter de la version 21.9.0, l'application Citrix Workspace prend en charge Android 12 Beta 4. Si vous accédez à des magasins basés sur HTTP, nous vous recommandons de passer à des magasins basés sur HTTPS pour des raisons de sécurité. Pour plus d'informations, consultez HTTPS.
- À partir de la version 22.2.0, vous pouvez accéder à la liste des applications récemment lancées pour un accès rapide lorsque vous appuyez longuement sur l'icône de l'application Citrix Workspace.




### Intégration avec l'Assistant Google

Vous pouvez interagir avec l'Assistant Google pour lancer des ressources telles que des applications et des bureaux sans lancer l'application Citrix Workspace à chaque fois. Toutes les ressources récemment consultées sont répertoriées sous les raccourcis de l'Assistant Google. Sélectionnez celles que vous préférez ajouter en tant que raccourci.

Pour configurer :

1. Lancez l'application Citrix Workspace et ouvrez une ressource que vous souhaitez ajouter en

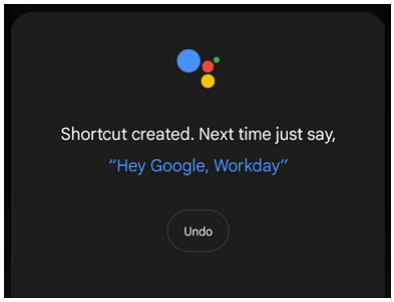
tant que raccourci.

2. Ouvrez les paramètres de l'Assistant Google depuis votre appareil.

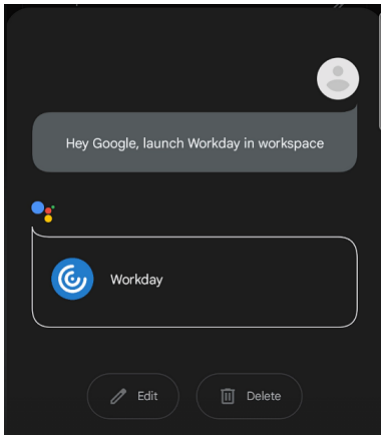
   > **Remarque :**
   >
   > L'accès aux paramètres de l'Assistant Google peut varier en fonction de la version d'Android et de l'appareil Android que vous utilisez.

   Il est conseillé d'utiliser la commande vocale pour ouvrir les paramètres de l'Assistant Google.

3. Faites défiler et touchez **Raccourcis**.
4. Appuyez sur **l'application Citrix Workspace** et sélectionnez la ressource que vous souhaitez ajouter en tant que raccourci.
   Vous pouvez désormais utiliser des commandes vocales pour lancer la ressource.

5. (Facultatif) Vous pouvez modifier et mettre à jour la commande vocale.

## Expérience de session

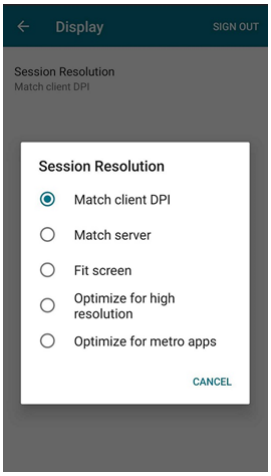
June 26, 2024

### Correspondance DPI

La fonctionnalité de correspondance DPI garantit que la session virtuelle est générée en fonction du DPI de l'appareil. Auparavant, même sur les téléphones portables et les tablettes à haute résolution, le DPI de l'appareil n'était pas pris en compte pour l'affichage des sessions. À partir de la version 24.1.0, un nouveau paramètre d'affichage permet d'obtenir une correspondance DPI.

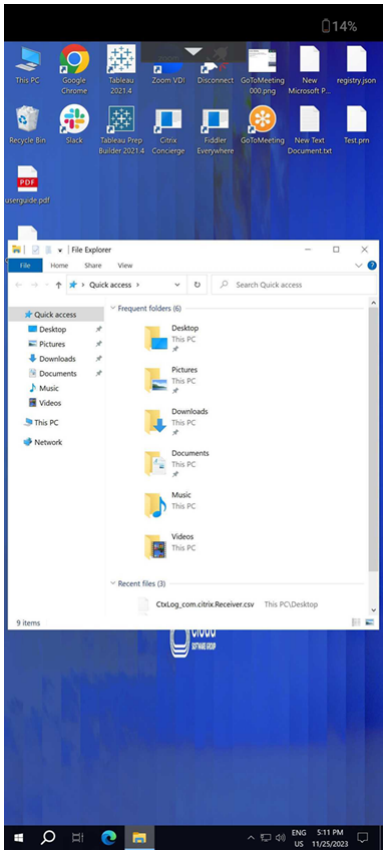
Sur votre appareil, accédez à l'application Citrix Workspace pour Android > **Paramètres** > **Général** > **Affichage** > **Résolution de session** > et sélectionnez l'option **Faire correspondre au PPP du client**.




En d'autres termes, l'application Citrix Workspace tente de faire correspondre automatiquement la résolution d'affichage et les paramètres d'échelle DPI de l'appareil Android à la session Citrix. Cette fonctionnalité améliore l'expérience utilisateur en affichant les sessions en fonction du DPI du téléphone ou de la tablette. La clarté des icônes de session, du texte et des images est désormais plus nette et plus facile à lire.

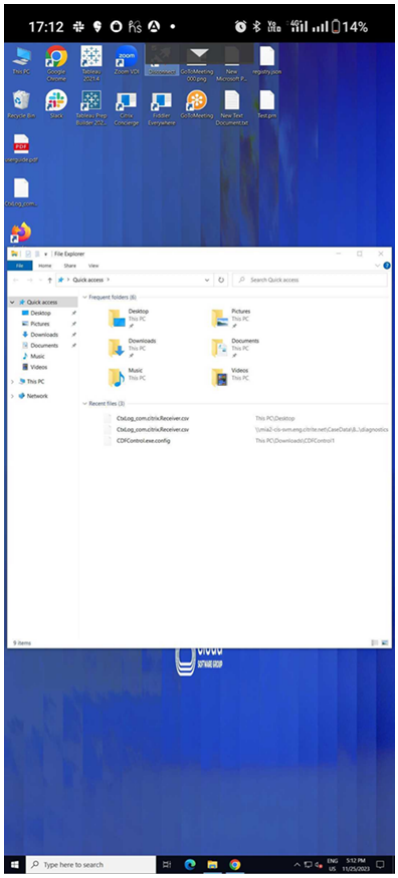
Par exemple, lorsque vous sélectionnez l'option **Faire correspondre au PPP du client**, les icônes de session, le texte et les images sont clairs.




Au contraire, lorsque vous sélectionnez l'option **Ajuster l'écran**, les icônes de session, le texte et les images sont plus petits.




> **Remarque :**
>
> Lorsque vous connectez un moniteur externe, le rendu de la session continue avec le DPI de l'appareil principal en raison des limites d'Android.

## Enlightened Data Transport (EDT)

Dans les versions antérieures, les lancements de sessions échouaient lorsque les connexions EDT (Enlightened Data Transport) ne pouvaient pas être établies entre Citrix Gateway et le VDA. À compter de la version 21.5.0, les connexions EDT infructueuses sont transférées vers TCP.

### Paramètres de pile EDT activés par défaut

À compter de la version 21.7.0, les paramètres de pile EDT sont activés par défaut. Par conséquent, nous avons supprimé l'option **Paramètres de pile EDT** dans **Paramètres > Avancé**.

À ce jour, l'option permettant de désactiver les paramètres de pile EDT était disponible pour les utilisateurs. Avec cette option disponible, certains clients ne respectaient pas systématiquement les exigences MSS (taille de segment maximale) EDT personnalisées. En conséquence, une fragmentation se produisait avec une dégradation des performances HDX et des problèmes liés à l'établissement de

sessions pour ces clients. Avec les paramètres de pile EDT maintenant activés par défaut, l'expérience utilisateur globale et la satisfaction sont désormais améliorées.

#### Connexion en parallèle

À compter de la version 21.7.0, nous introduisons la fonctionnalité de connexion EDT et TCP en parallèle. Cette fonctionnalité entraîne une réduction des temps de connexion.

Auparavant, lors de l'établissement d'une connexion, l'application Citrix Workspace essayait de se connecter à l'aide d'EDT. L'échec des tentatives de connexion EDT était dû au protocole TCP, lequel provoquait les problèmes suivants qui sont désormais résolus :

- Temps de connexion accru dans les scénarios de secours.
- La fiabilité de session et la reconnexion automatique des clients avaient tendance à privilégier TCP.
- Une interruption de connexion était requise pour réessayer TCP.

#### Capacités de découverte MTU ajoutées à EDT

Nous avons ajouté des fonctionnalités de découverte d'unité de transmission maximale (MTU) à Enlightened Data Transport (EDT). Par conséquent, vous pouvez désormais profiter d'une expérience HDX toujours stable, fournie par EDT.

Auparavant, EDT échouait dans plusieurs scénarios tels qu'avec les connexions VPN, Wi-Fi, 4G ou 3G, et sur Microsoft Azure. L'échec était causé par une perte de paquets due à leur taille.

Lorsque vous tentiez de lancer une session, la fragmentation des paquets entraînait l'abandon des sessions. Pour contourner le problème, il était nécessaire d'ajuster la taille de segment maximale (MSS) EDT dans le fichier StoreFront, ce qui signifiait une configuration supplémentaire. L'ajout de *fonctionnalités de découverte MTU* à EDT résout ces problèmes.

Les fonctionnalités de découverte MTU ajoutées à EDT fonctionnent dans les sessions hébergées sur des VDA 1912 et versions ultérieures.

### Lancement automatique du fichier ICA

Vous pouvez lancer vos applications et bureaux publiés en touchant la ressource. Cette fonctionnalité nécessite StoreFront (local) version 1912 ou ultérieure.

### Lancement de session amélioré

Les applications et les bureaux publiés sont lancés dans des fenêtres séparées. Cette amélioration vous permet d'utiliser et d'interagir avec la fenêtre d'énumération de magasin sans avoir à vous déconnecter ou fermer la session.

**Limitations :**

- Après avoir modifié des paramètres utilisateur, vous devez relancer la session pour que les modifications prennent effet.
- Les applications et les bureaux sont nommés « Espace de travail » dans la barre des tâches - pas après la session.

### Indicateur d'état de la batterie

L'état de la batterie de l'appareil s'affiche désormais dans la zone de notification d'une session Citrix Desktop.

> **Remarque :**
>
> L'indicateur d'état de la batterie n'est pas affiché pour le serveur VDA.

### Redirection de périphérique USB

À partir de la version 20.9.0, la fonctionnalité de redirection USB est désormais entièrement fonctionnelle et disponible. Par défaut, la fonctionnalité de redirection USB est désactivée.

Cette fonctionnalité permet de rediriger des périphériques USB arbitraires de machines clientes vers Citrix Virtual Apps and Desktops et Citrix DaaS. Elle vous permet d'interagir avec un large choix de périphériques USB génériques au sein d'une session comme s'ils y étaient physiquement connectés.

Pour gérer cette fonctionnalité à l'aide de Citrix Global App Config Service, définissez la fonctionnalité de redirection USB sur **Activé** sur le Delivery Controller. Pour plus d'informations sur la configuration de la redirection USB sur le Delivery Controller, consultez la section Périphériques USB génériques dans la documentation de Citrix Virtual Apps and Desktops.

Citrix Global App Configuration Service permet aux administrateurs Citrix de fournir des URL de service Citrix Workspace et des paramètres d'application Citrix Workspace via un service géré de manière centralisée.

La fonctionnalité de redirection USB est intégrée et configurable via Citrix Global App Config Service. Vous pouvez gérer la fonctionnalité à l'aide de Citrix Global App Config Service pour les réseaux non joints à un domaine.

Pour plus d'informations sur la configuration de la fonctionnalité à l'aide de cette méthode, consultez Global App Configuration Service dans la documentation destinée aux développeurs.

> **Remarque :**
>
> Cette fonctionnalité est disponible à partir de la version 20.9.0. Dans les versions 20.8.1 et antérieures, elle est disponible uniquement à la demande.

La stratégie de redirection USB doit être définie sur **Autorisé** sur le Delivery Controller. Pour plus d'informations sur la configuration de la redirection USB dans Citrix Studio, consultez Configurer la redirection USB générique dans la documentation de Citrix Virtual Apps and Desktops.

**Pour imprimantes et scanners :**

Installez les pilotes spécifiques du fournisseur sur le périphérique. Lorsque l'installation est terminée, le logiciel fournisseur peut vous demander de reconnecter le périphérique USB. Reconnectez le périphérique USB pour le rediriger.

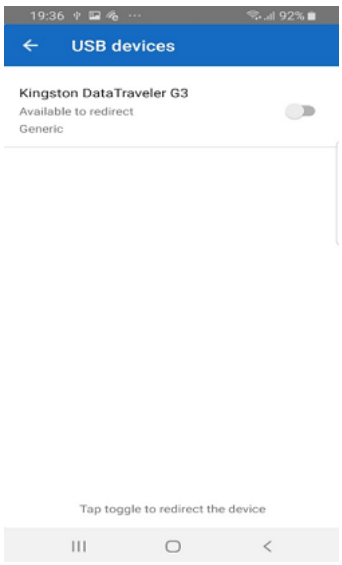
### Configuration de la redirection USB sur les téléphones mobiles, les tablettes et Samsung DeX

1. Ajoutez un magasin compatible avec la stratégie de redirection USB et lancez une session.
2. Touchez l'icône de la barre d'outils de session comme illustré dans la boîte de dialogue ci-dessous :


3. Touchez l'**icône USB** dans la barre d'outils de session.

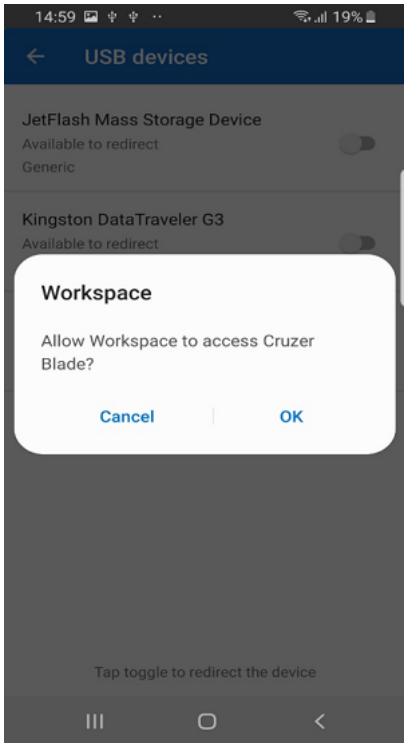
 

4. Les périphériques USB connectés sont répertoriés dans la fenêtre Périphériques USB comme suit :




5. Pour rediriger un périphérique USB particulier, touchez l'option « Basculer » en regard du périphérique.

   Une boîte de dialogue d'autorisation Workspace s'affiche.

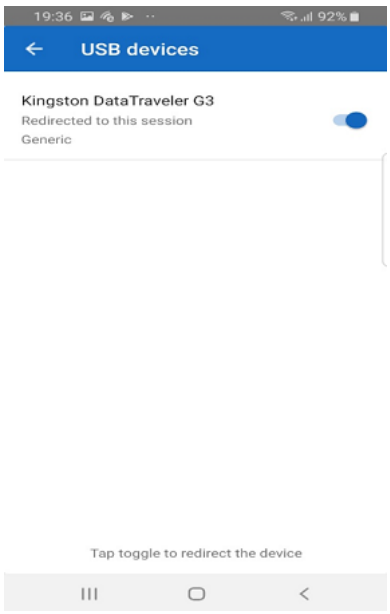



6. Touchez **OK** pour accorder l'autorisation à l'application Citrix Workspace de rediriger le périphérique.

> **Remarque :**
>
> Cette étape est obligatoire pour rediriger le périphérique USB.

Le périphérique USB est redirigé et l'état est affiché comme suit :




> **Remarque :**
>
> - Si une clé USB est redirigée, elle apparaît comme répertoriée dans une session.
> - Si une imprimante ou un scanner est redirigé, il s'affiche dans la section **Périphériques** du panneau de configuration.

**Périphériques USB testés**

| Appareil | Fabricant | Modèle |
|---|---|---|
| Imprimante | HP | LaserJet P2014 |
| Scanneur | HP | Scanjet G3010 |
| Scanneur | Canon | CanoScan LiDE 700 F |
| Space Navigator | 3Dconnexion | |
| Imprimante | Brother | QL-580N |
| Scanneur | HP | Scanjet 200 |

**Problèmes connus :**

- Un seul périphérique USB est pris en charge à la fois.
- Les périphériques USB audio et vidéo ne sont pas actuellement pris en charge.

### Redirection automatique des périphériques USB

L'application Citrix Workspace vous permet de rediriger automatiquement les périphériques USB lorsque vous les connectez. Lorsque vous connectez un périphérique USB, une invite s'affiche pour vous demander l'autorisation. Après avoir accordé l'autorisation, le périphérique USB est redirigé automatiquement.

> **Remarque :**
>
> Cette fonctionnalité est disponible uniquement à la demande et n'est prise en charge que si la fonctionnalité de redirection de périphérique USB est activée.

### Améliorations apportées à la redirection audio

Auparavant, la redirection audio dans une session de bureau nécessitait d'accéder à plusieurs niveaux de paramètres du microphone, et les étapes de configuration des autorisations n'étaient pas intuitives. Désormais, les paramètres d'autorisation du microphone sont simplifiés et conviviaux. Vous pouvez également activer les autorisations pendant que vous êtes dans une session.

Par défaut, le commutateur audio sous l'**application Citrix Workspace** > **Paramètres** > **Audio** est activé. La session peut désormais détecter si un haut-parleur est déjà connecté. Les administrateurs peuvent activer ou désactiver la redirection audio à l'aide de Global App Configuration Service.

> **Remarque :**
>
> Par défaut, l'autorisation de microphone est désactivée à la fois dans les paramètres de l'application Citrix Workspace et sur la page des paramètres du magasin.

Vous pouvez rencontrer l'un des scénarios suivants lorsque l'application Citrix Workspace ou le magasin désactive le microphone :

- Lorsque les paramètres de l'application Citrix Workspace et du magasin désactivent l'autorisation de microphone, le message **Autoriser Workspace à enregistrer l'audio** s'affiche lorsque vous démarrez la session de bureau et utilisez le microphone. Appuyez sur **Pendant l'utilisation de l'application**.
- Lorsque l'application Citrix Workspace est activée, mais que les paramètres du magasin désactivent l'autorisation de microphone, le message **Autoriser l'accès au microphone** s'affiche lorsque vous démarrez la session de bureau et utilisez le microphone. Appuyez sur **Autoriser**.

### Synchronisation de la disposition du clavier

L'application Citrix Workspace vous permet d'activer la synchronisation de la disposition du clavier sous **Paramètres** > **Général** > **Clavier** > **Synchronisation de la disposition du clavier**.

L'option **Synchronisation de la disposition du clavier** permet de synchroniser automatiquement la disposition du clavier entre le VDA et le périphérique client.

Sur une nouvelle installation et par défaut, l'éditeur IME côté client est automatiquement activé pour les langues japonaise, chinoise et coréenne et l'option de **synchronisation de la disposition du clavier** est définie sur **Désactivé.**

Pour activer la synchronisation dynamique de la disposition du clavier, définissez l'option **Synchronisation de la disposition du clavier**sur **Activé**.

Lorsque la **synchronisation de la disposition du clavier** est désactivée, l'éditeur IME côté VDA (distant) et l'éditeur IME côté client prennent effet en fonction de la méthode de saisie actuelle de votre appareil. Par exemple, si l'éditeur IME côté client est en anglais et que l'éditeur IME côté VDA est en japonais, l'éditeur IME côté VDA (distant) s'applique.

Lorsque la **synchronisation de la disposition du clavier** est activée, l'éditeur IME côté client a priorité. Si vous modifiez la langue de saisie au niveau de l'éditeur IME côté client, l'éditeur IME côté VDA change en conséquence. Par exemple, si vous remplacez l'éditeur IME côté client par le japonais, l'éditeur IME côté VDA passe automatiquement au japonais. Dans le même temps, l'éditeur IME japonais de votre appareil client est utilisé pendant la session.

**Pré-requis :**

- Pour les VDA Linux, activez les stratégies **Synchronisation de la disposition du clavier client** et **améliorations apportées à l'éditeur IME**.
- Pour les VDA Windows, activez les stratégies **Mappage de disposition du clavier Unicode**, **Synchronisation de la disposition du clavier client** et **Améliorations apportées à l'éditeur IME**.
- Le VDA doit être la version 7.16 ou ultérieure.

**Limitations des fonctionnalités :**

- Cette fonctionnalité ne fonctionne que sur les claviers logiciels des appareils, et non sur les claviers externes.
- La synchronisation de la disposition du clavier ne prend pas en charge Gboard (le clavier Google).
- La disposition du clavier peut uniquement être synchronisée du client au serveur. Lorsque vous modifiez la disposition du clavier côté serveur, la disposition du clavier client ne peut pas être modifiée.
- Lorsque vous modifiez la disposition du clavier client sur une disposition non compatible, la disposition peut être synchronisée du côté VDA, mais la fonctionnalité ne peut pas être confirmée.

**Prise en charge de la disposition du clavier pour VDA Windows et VDA Linux**

| Disposition du clavier sur Android | Langue du clavier | Disposition du clavier sur Windows | Disposition du clavier sur Linux |
|---|---|---|---|
| Biélorusse (Biélorussie) | Biélorusse (Biélorussie) | Clavier biélorusse (Biélorussie) | by |
| Bulgare | Bulgare | Clavier bulgare (machine à écrire) | bg |
| Chinois (Simplifié) | Chinois (simplifié, Chine) | Citrix IME - Chinois (simplifié, Chine) | zh |
| Chinois (traditionnel) | Chinois (traditionnel, Taïwan) | Citrix IME - Chinois (traditionnel, Taïwan) | tw |
| Croate | Croate (Croatie) | Clavier croate | hr |
| Tchèque | Tchèque | Clavier tchèque | cz |
| Danois | Danois | Clavier danois | df |
| Néerlandais | Néerlandais (Pays-Bas) | Clavier américain - international | us |
| Néerlandais (Belgique) | Néerlandais | Clavier belge (d' époque) | be |
| Anglais (Australie) | Anglais (Australie) | Clavier américain | us |
| Anglais (Canada) | Anglais (Canada) | Clavier américain | us |
| Anglais (Royaume-Uni) | Anglais (Royaume-Uni) | Clavier britannique | gb |
| Anglais (États-Unis) | Anglais (États-Unis) | Clavier américain | us |
| Estonien | Estonien | Clavier estonien | ee |
| Finnois | Finnois | Clavier finnois | fi |
| Français (Canada) | Français (Canada) | Clavier français | fr |
| Français (Suisse) | Français (France) | Clavier français de Suisse | ch |
| Français (français) | Français (France) | Clavier français | fr |
| Allemand (Autriche) | Allemand (Autriche) | Clavier allemand | at |
| Allemand (Suisse) | Allemand (Suisse) | Clavier suisse allemand | ch |
| Allemand (Allemagne) | Allemand (Allemagne) | Clavier allemand | at |
| Grec | Grec | Clavier grec | gr |

| Disposition du clavier sur Android | Langue du clavier | Disposition du clavier sur Windows | Disposition du clavier sur Linux |
|---|---|---|---|
| Hongrois | Hongrois | Clavier hongrois | hu |
| Islandais | Islandais | Clavier islandais | is |
| Irlandais | Irlandais | | ie |
| Italien | Italien (Italie) | Clavier italien | it |
| Japonais | Japonais | Citrix IME - japonais | jp |
| Coréen | Coréen | Citrix IME - Coréen | kr |
| Letton | Letton | Clavier letton | lv |
| Norvégien | Norvégien (Bokmål) | Clavier norvégien | non |
| Polonais | Polonais | Clavier polonais (programmeurs) | pl |
| Portugais (Brésil) | Portugais (Brésil) | Clavier portugais (ABNT du Brésil) | br |
| Portugais (Portugal) | Portugais (Portugal) | Clavier portugais | pt |
| Roumain | Roumain (Roumanie) | Clavier roumain (ancien) | ro |
| Russe (Russie) | Russe | Clavier russe | ru |
| Slovaque | Slovaque | Clavier slovaque | sk |
| Slovène | Slovène | Clavier slovène | si |
| Espagnol (Mexique) | Espagnol (Mexique) | Clavier latino-américain | latam |
| Espagnol (Espagne) | Espagnol (Espagne) | Clavier espagnol | es |
| Suédois (Suède) | Suédois (Suède) | Clavier suédois | se |
| Turc | Turc | Clavier turc F | tr |
| Ukrainien | Ukrainien | Clavier ukrainien | ua |

### Continuité du service

La fonction Continuité du service supprime ou réduit la dépendance à l'égard de la disponibilité des composants impliqués dans le processus de connexion. Les utilisateurs peuvent lancer leurs applications et bureaux virtuels quel que soit l'état d'intégrité des services cloud.

Pour plus d'informations, consultez la section Continuité du service dans la documentation de Citrix

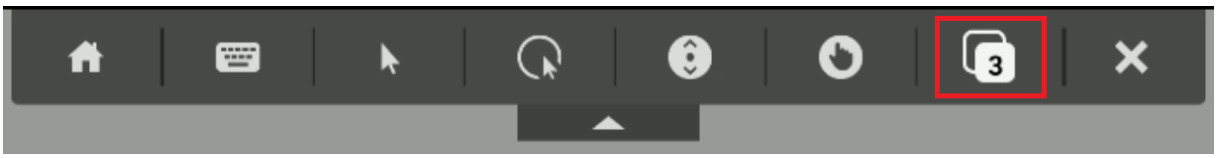
 

Workspace.

### Changement d'applications

Cette fonctionnalité permet à l'utilisateur final de basculer entre plusieurs applications publiées qui se trouvent dans la même session. Lorsque vous appuyez sur l'icône **Basculer**, vous pouvez faire défiler l'écran pour sélectionner une application et l'application qui a le focus est mise en surbrillance. Vous pouvez afficher le titre de l'application, une image d'aperçu et le titre de la fenêtre.

Lorsque vous ouvrez ou fermez une application, le nombre d'applications est mis à jour en conséquence. Si certaines applications sont ouvertes dans une autre session, le nombre d'applications inclut toutes celles ouvertes.

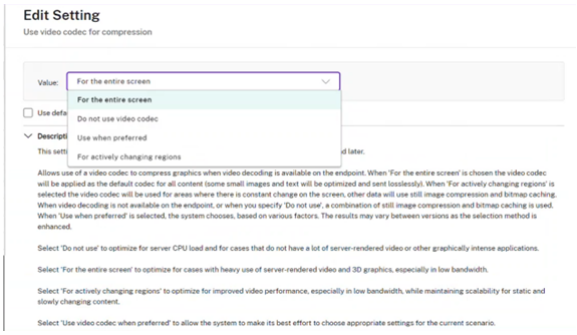



### Prise en charge de l'affichage en plein écran

À compter de la version 23.8.0, le codec H264 prend en charge un rendu vidéo amélioré en mode plein écran. Si vous regardez fréquemment des vidéos ou si vous dépendez grandement du contenu vidéo, cette fonctionnalité est recommandée pour vous. Elle est conçue pour améliorer votre expérience vidéo en termes de performances, de qualité vidéo et d'utilisation des ressources.

#### Configuration

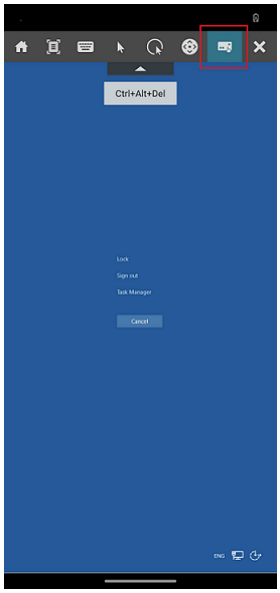
Sur la machine DDC, définissez la stratégie **Utiliser le codec vidéo pour la compression** sur **Pour l'ensemble de l'écran** afin d'améliorer la compression vidéo jusqu'à 60 images par seconde.



### Ajout du raccourci Ctrl+Alt+Suppr à la barre d'outils de la session

À partir de la version 23.9.5, la barre d'outils de la session dispose d'une option permettant d'utiliser la fonction Ctrl+Alt+Suppr en appuyant simplement sur un bouton. Cette option permet aux utilisateurs de se déconnecter, de changer d'utilisateur, de verrouiller l'appareil ou d'accéder au Gestionnaire des tâches.




### Prise en charge du mode plein écran pour les sessions d'applications

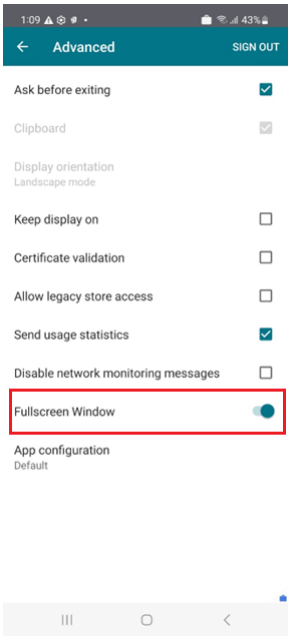
Auparavant, lorsque vous démarriez une session d'application, vous pouviez l'afficher en mode fenêtré.

À partir de la version 23.9.5, l'application Citrix Workspace pour Android introduit une nouvelle option permettant d'afficher la session de l'application en mode plein écran. Cette fonctionnalité est utile lorsque vous :

- démarrez une session en mode immersion totale avec des appareils tactiles
- essayez de dupliquer l'écran et de le diffuser
- affichez l'application Citrix Workspace sur un écran plus petit

Pour activer cette option, accédez à l'application Citrix Workspace pour Android, **Paramètres** > **Avancé** > **Fenêtre plein écran** et activez cette option. La capture d'écran suivante montre l'option :




## Accessibilité et TalkBack

L'application Citrix Workspace offre une expérience utilisateur améliorée grâce à la fonctionnalité TalkBack. La fonctionnalité TalkBack aide les utilisateurs finaux qui ont des difficultés à voir l'écran. Le narrateur lit à haute voix les éléments figurant à l'écran lors de l'utilisation de l'interface utilisateur.

Pour utiliser la fonctionnalité Talkback d'Android, les utilisateurs finaux doivent l'activer depuis Android, **Paramètres** > **Accessibilité** > **Talkback**.

Pour plus d'informations, consultez la section Accessibilité et TalkBack dans la documentation d'aide.

### Problèmes connus liés à cette fonctionnalité

- Lorsque vous connectez un clavier externe à votre appareil :
  - Si vous utilisez la touche Caps Verr comme touche du narrateur, il est possible que l'action ne fonctionne pas comme prévu. Pour contourner ce problème, appuyez sur la touche Insérer. [HDX-55347]
  - Si vous utilisez la combinaison de touches Win+Ctrl+Entrée pour activer le narrateur, l'action ne prend pas effet dans la session de bureau virtuel. Pour contourner ce problème, utilisez la touche Win ou le menu Démarrer et saisissez le mot Narrateur. [HDX-55380]

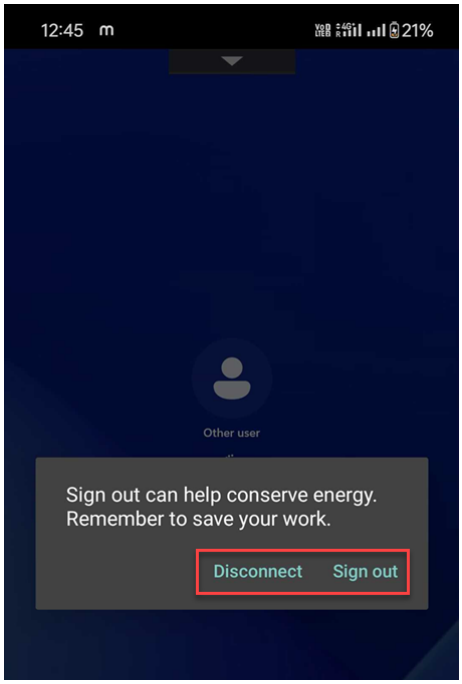
 

### Initiative de développement durable pour l'application Citrix Workspace

Auparavant, les bureaux virtuels étaient déconnectés lorsque les utilisateurs les fermaient en appuyant sur le bouton d'accueil. Cela consommait de l'énergie inutilement.

À partir de la version 24.2.0, nous avons introduit une initiative de développement durable qui encourage les utilisateurs à économiser l'énergie qui pourrait être consommée par l'exécution de bureaux virtuels inutilisés.

Lorsque cette fonctionnalité est activée et que les utilisateurs appuient sur l'icône **X** pour déconnecter la session, une invite s'affiche pour se déconnecter de la session de bureau. Cette fonctionnalité peut être utile dans les entreprises qui utilisent des stratégies de système d'exploitation Windows pour arrêter les machines virtuelles lorsqu'aucun utilisateur n'est connecté.




Les utilisateurs finaux peuvent quitter la session de deux manières :

- **Déconnexion** pour économiser de l'énergie. Cette action durable arrête la machine virtuelle et permet d'économiser de l'énergie. Les utilisateurs finaux doivent s'assurer de sauvegarder leur travail avant de se déconnecter.
- **Déconnecter** pour fermer la fenêtre de session de bureau virtuel. Cependant, la session virtuelle reste active jusqu'à la prochaine connexion. Les utilisateurs finaux peuvent facilement reprendre leur travail.

En tant qu'administrateur, vous pouvez personnaliser le message sur le développement durable. Pour plus d'informations sur l'activation et la personnalisation de cette fonctionnalité, consultez l'article Initiative de développement durable pour l'application Citrix Workspace dans la documentation de l'application Citrix Workspace pour Windows.

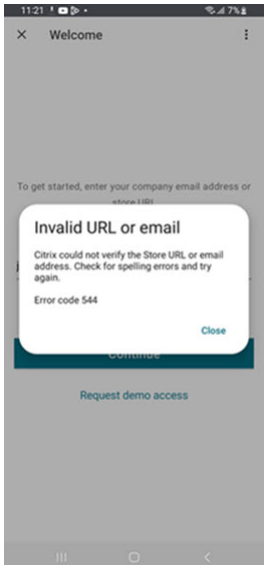
 

### Messages d'erreur améliorés

Auparavant, les messages d'erreur ne contenaient pas suffisamment de descriptions exploitables.

À partir de la version 23.12.0, les messages d'erreur incluent un titre clair et convivial, une description spécifique pour chaque erreur et des codes d'erreur, dans la mesure du possible. Les codes d'erreur aident les administrateurs à résoudre le problème. Les messages améliorés destinés aux utilisateurs fournissent suffisamment de détails pour résoudre les problèmes. En cas de problèmes non résolus, nous suggérons aux utilisateurs de contacter leur administrateur informatique pour obtenir de l'aide.

Par exemple, lorsque l'utilisateur ne parvient pas à se connecter, le message d'erreur suivant s'affiche :

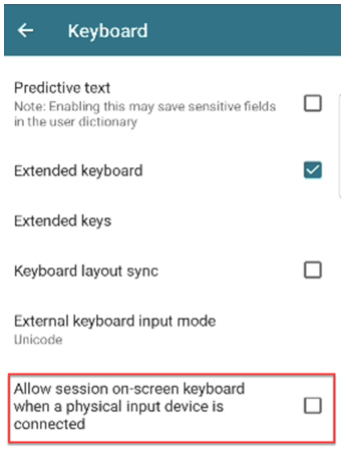



### Prise en charge du clavier logiciel pour un lecteur de code-barres

Auparavant, lorsque des lecteurs de code-barres (par exemple, des scanneurs Zebra) étaient détectés au cours d'une session, le clavier logiciel n'apparaissait pas. Le problème était dû à son identification en tant que clavier externe.

À partir de la version 24.2.0, le clavier logiciel s'affiche lorsque les lecteurs de code-barres sont connectés en tant que périphérique de saisie physique. Un nouveau réglage du clavier a été ajouté pour prendre en charge cette fonctionnalité. Les utilisateurs finaux peuvent accéder au menu **Paramètre** > **Clavier** de l'application Citrix Workspace, puis sélectionner l'option **Autoriser clavier à l'écran de session lorsqu'un périphérique d'entrée physique est connecté**.




### Gérer le texte prédictif

Le texte prédictif contribue à améliorer l'expérience de saisie en suggérant des mots au fur et à mesure que vous tapez. Lorsque vous activez cette fonctionnalité au cours d'une session d'application ou de bureau, il est possible que des mots de passe apparaissent sur le ruban de prédiction. Pour contrôler ce comportement, cette fonctionnalité est désactivée par défaut.

> **Remarques :**
>
> - Dans les paramètres de clavier par défaut de votre appareil, si l'option **Texte prédictif** est désactivée, vous ne pouvez pas utiliser cette fonctionnalité même si vous l'activez via l'application Citrix Workspace pour Android.
> - Au cours d'une session, lorsque la disposition de saisie CJK est définie par défaut sur le clavier GBoard, la disposition anglaise apparaît à la place de la disposition CJK. Pour voir la disposition du clavier CJK, sélectionnez **Paramètres** > **Clavier** dans l'application, puis activez l'option **Texte prédictif**. [CVADHELP-23667]

### Scanner de documents

Si vous êtes connecté à l'application Citrix Workspace, vous pouvez utiliser la fonctionnalité de numérisation rapide pour numériser de nombreux documents et les transférer vers la session de bureau virtuel.

> **Remarque :**
>
> - Cette fonctionnalité est activée par défaut.

**Logiciels requis**

- Le mappage des lecteurs clients (CDM) doit être activé pour le magasin.
- La numérisation de documents nécessite un accès en lecture et en écriture sur votre appareil. Pour donner accès, procédez comme suit :

  1. Depuis votre profil, touchez **Paramètres** > **Paramètres du magasin** pour l'application.
  2. Appuyez sur votre magasin actuel.
  3. Appuyez sur **Stockage de l'appareil** et sélectionnez **Accès complet**.

Pour plus d'informations sur l'utilisation de cette fonctionnalité, consultez la section Numérisation de documents dans la documentation d'aide.

## Expérience de magasin

February 21, 2024

### Utilisateurs non authentifiés

L'application Citrix Workspace prend en charge les utilisateurs non authentifiés (anonymes). Les utilisateurs anonymes peuvent lancer des sessions Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) avec succès.

### Paramètres de sécurité

Citrix recommande d'utiliser des magasins sécurisés. En outre, il est recommandé d'activer le paramètre HTTP Strict Transport Security (HSTS) pour les magasins sécurisés.

Suivez les étapes suivantes pour activer le paramètre **HSTS** :

1. Dans **Citrix StoreFront**, sous **Magasins**, touchez le lien du magasin en question pour activer les paramètres de sécurité.
2. La boîte de dialogue **Gérer les sites Receiver pour Web** apparaît.
3. Touchez **Configurer**.
4. La boîte de dialogue **Modifier le site Receiver pour Web** apparaît.
5. Touchez l'onglet **Paramètres avancés** et sélectionnez **Activer une sécurité de transport stricte**.

# Authentification

June 26, 2024

## Cartes à puce

L'application Citrix Workspace pour Android prend en charge l'authentification via Citrix Gateway à l'aide des méthodes suivantes, selon l'édition que vous possédez :

- Aucune authentification (versions Standard et Enterprise uniquement)
- Authentification de domaine
- Authentification par code d'accès SMS (code PIN à usage unique)
- Authentification par carte à puce

L'application Citrix Workspace pour Android prend désormais en charge les configurations et produits suivants.

**Lecteurs de cartes à puce :**

- Lecteur de carte à puce USB BaiMobile 3000MP

**Cartes à puce :**

- Cartes PIV
- Cartes CAC

**Configurations :**

- Authentification par carte à puce à Citrix Gateway avec StoreFront 2 ou 3 et Citrix Virtual Apps and Desktops 7.x et versions supérieures.

> **Remarque :**
>
> - Les autres solutions d'authentification à base de jeton peuvent être configurées à l'aide de RADIUS. Pour l'authentification par jeton SafeWord, consultez Configuration de l'authentification SafeWord.

### Comment utiliser les cartes à puce

> **Conditions préalables**
>
> - Installez l'application C4E depuis le Play Store pour utiliser des cartes à puce. Adresse e-mail de contact : < android@citrix.com > pour les licences.

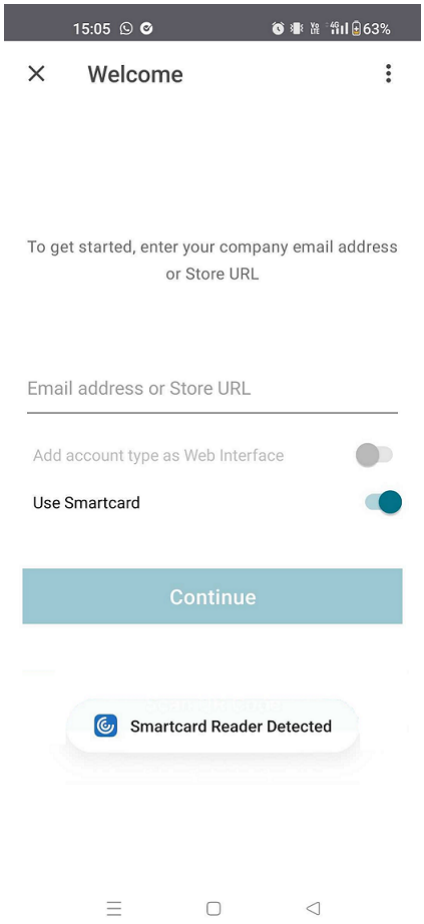
 

Pour utiliser des cartes à puce pour accéder aux applications :

1. Si vous souhaitez configurer l'application Citrix Workspace automatiquement pour accéder aux applications lors de la création d'un compte, dans le champ **Adresse**, entrez l'URL valide de votre magasin. Par exemple :

    - .organization.com
    - netscalervserver.organization.com

2. Insérez la carte à puce ainsi que le lecteur compatible dans votre appareil Android. L'application Citrix Workspace détecte automatiquement la carte à puce.




3. Sélectionnez l'option **Utiliser carte à puce** pour vous authentifier.

> **Remarque :**
>
> - Votre accès au magasin reste valide pendant environ une heure. Passé ce délai, vous devez vous connecter pour actualiser votre accès ou démarrer d'autres applications.

### Prise en charge de l'authentification basée sur FIDO2 lors de la connexion à une session HDX

À compter de la version 23.8.0, l'application Citrix Workspace pour Android prend désormais en charge l'authentification sans mot de passe au sein d'une session Citrix Virtual Apps and Desktops à l'aide de méthodes d'authentification basées sur FIDO2.

Cette fonctionnalité permet aux utilisateurs de se connecter à un site Web compatible avec WebAuth depuis un navigateur. Par exemple, Google Chrome ou Microsoft Edge utilisent des authentificateurs de plateforme compatibles avec FIDO2, tels que l'empreinte digitale et le code PIN de l'appareil. Le simple fait d'ouvrir un site Web compatible avec WebAuthn déclenche une authentification sans mot de passe.

La connexion à l'application Citrix Workspace ou à une session de bureau à l'aide d'une authentification sans mot de passe n'est pas prise en charge sur FIDO2.

> **Remarque :**
>
> Les applications d'authentification itinérantes telles que YubiKey ou Smart Card ne sont pas prises en charge dans l'application Citrix Workspace pour Android.

Pour plus d'informations sur les conditions requises pour cette fonctionnalité, consultez la section Autorisation locale et authentification virtuelle à l'aide de FIDO2 dans la documentation de Citrix Virtual Apps and Desktops.

### Délai d'inactivité pour les sessions d'application Citrix Workspace

L'administrateur peut spécifier la durée d'inactivité autorisée. Après expiration du délai d'inactivité, une invite d'authentification s'affiche.

Pour plus d'informations, consultez la section Délai d'inactivité pour les sessions d'application Citrix Workspace.

### Prise en charge de l'authentification biométrique après une période d'inactivité

Une fois le délai d'inactivité expiré, l'utilisateur final est invité à s'authentifier à l'aide de fonctionnalités biométriques telles que la reconnaissance faciale et la lecture d'empreintes digitales.

La forme d'authentification biométrique la plus robuste disponible pour l'utilisateur final dépend de l'OEM de son périphérique, et il est invité en fonction de celle-ci.

### Prise en charge de l'authentification à l'aide de FIDO2 lors de la connexion à un magasin cloud

À partir de la version 24.5.0, les utilisateurs peuvent s'authentifier auprès de l'application Citrix Workspace à l'aide de l'authentification sans mot de passe basée sur FIDO2 lors de la connexion à un magasin cloud. Le protocole FIDO2 offre une méthode d'authentification transparente, permettant aux employés de l'entreprise d'accéder aux applications et bureaux pendant les sessions virtuelles sans avoir à saisir de nom d'utilisateur ni de mot de passe. Cette fonctionnalité prend en charge à la fois l'itinérance (USB uniquement) et les authentificateurs de plateforme (code PIN, reconnaissance faciale et empreinte digitale uniquement). Cette fonctionnalité est compatible avec la version 9 et les versions ultérieures d'Android.

L'authentification FIDO2 est prise en charge avec les onglets personnalisés de Chrome. Si vous souhaitez utiliser l'authentification FIDO2 avec WebView, signalez-le à l'aide du formulaire Podio.

> **Remarque :**
>
> Cette fonctionnalité est activée par défaut.

## Sécuriser

December 11, 2023

### ProGuard activé pour plus de sécurité

Nous avons activé ProGuard pour sécuriser Citrix Workspace pour Android grâce à l'obfuscation. ProGuard renomme différentes parties du code pour empêcher l'inspection des traces de pile et sécurise l'application Workspace. ProGuard réduit également la taille de l'application en raccourcissant les noms des classes, des méthodes et des champs des applications.

### Cryptographie

Cette fonctionnalité est un changement important au protocole de communication sécurisé. Les suites de chiffrement avec le préfixe TLS_RSA_ ne proposent pas la fonctionnalité Forward Secrecy et sont considérées comme faibles.

Les suites de chiffrement `TLS_RSA_` ont été supprimées. Les versions 20.6.5 et ultérieures prennent en charge les suites de chiffrement `TLS_ECDHE_RSA_` avancées. Si votre environnement n'est pas

configuré avec les suites de chiffrement TLS_ECDHE_RSA_, vous ne pouvez pas lancer le client en raison de chiffrements faibles.

Les suites de chiffrement avancées suivantes sont prises en charge :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

TLS v1.0 prend en charge les suites de chiffrement suivantes :

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS v1.2 prend en charge les suites de chiffrement suivantes :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

TLS v1.3 prend en charge les suites de chiffrement suivantes :

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256

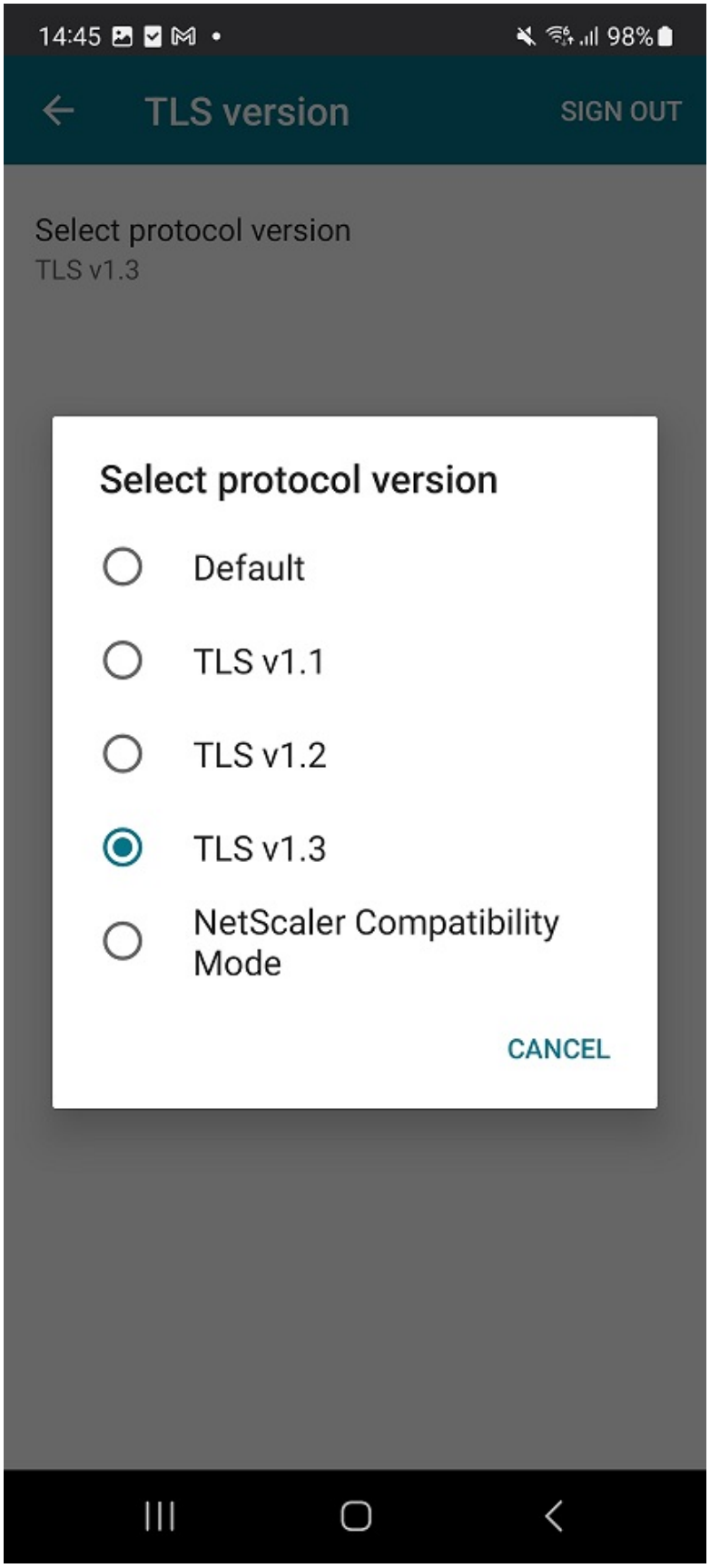
### Prise en charge du protocole TLS 1.3

L'application Citrix Workspace pour Android prend désormais en charge le protocole Transport Layer Security (TLS) 1.3. Celui-ci offre une performance et une efficacité accrues. Le protocole TLS 1.3 garantit une sécurité de haut niveau grâce à ses suites de chiffrement complexes et à ses clés de session uniques.

Les utilisateurs finaux peuvent l'activer sur l'application Citrix Workspace pour Android comme suit :

1. Accédez aux **Paramètres** de l'application Citrix Workspace > **Version TLS**.
2. Appuyez sur l'option **Sélectionner la version du protocole** et sélectionnez **TLS v1.3**.



Pour en savoir plus, voir Cryptographie

Pour plus d'informations sur la documentation d'aide, consultez la version TLS.

# Dépannage

March 22, 2024

## Comment vérifier la version de l'application

Pour savoir quelle version de l'application Citrix Workspace vous utilisez, consultez l'article Comment vérifier la version de l'application dans la documentation d'aide.

## Comment effectuer la mise à niveau vers la dernière version

Pour mettre à niveau manuellement l'application Citrix Workspace vers la dernière version, procédez comme suit :

1. Ouvrez Play Store.
2. Recherchez Citrix Workspace.

   Si une mise à jour est disponible, touchez **Mettre à jour**.

### Mise à jour automatique de l'application

Par défaut, les applications sont mises à jour automatiquement lorsque les conditions suivantes sont remplies :

- L'appareil est connecté à un réseau Wi-Fi.
- L'appareil est en cours de chargement.
- L'appareil est inactif (non utilisé activement).
- L'application Citrix Workspace ne s'exécute pas au premier plan.

> **Remarque :**
>
> Google Play Store recherche les mises à jour d'applications une fois par jour. L'ajout d'une mise à jour d'application à la file d'attente des mises à jour peut donc prendre jusqu'à 24 heures. Une fois qu'une application est ajoutée à la file d'attente, elle sera automatiquement mise à jour la prochaine fois que les conditions seront remplies.

### Comment réinitialiser l'application Citrix Workspace

Pour réinitialiser l'application, vous pouvez effectuer l'une des opérations suivantes :

- Effacez les données de stockage de l'application Citrix Workspace. Accédez aux **paramètres** de l'appareil Android > **Applications** > sélectionnez **Application Citrix Workspace** > **Stockage** > **Effacer le cache**.

  ou

- Désinstallez l'application Citrix Workspace actuelle et installez la dernière version de l'application Citrix Workspace pour Android depuis Google Play, qui contient le dernier correctif.

> **Remarque**
>
> La suppression de comptes existants de l'application Citrix Workspace réinitialise le compte et non l'application Citrix Workspace elle-même.

### Comment collecter des journaux

La collecte de journaux est importante, car elle peut aider à identifier les problèmes. Pour plus d'informations, consultez Comment collecter des journaux dans la documentation d'aide.

### Comment fournir des commentaires

Vous pouvez nous envoyer des commentaires sur l'application Citrix Workspace pour Android et signaler des problèmes à l'aide de la même interface. Pour plus d'informations, consultez Comment envoyer des commentaires dans la documentation d'aide.

### Comment demander des améliorations

Pour demander des améliorations des fonctionnalités de l'application Citrix Workspace pour Android, remplissez le formulaire Podio.

### Comment accéder aux fonctionnalités de version Technical Preview

Pour en savoir plus sur les fonctionnalités de version Technical Preview, consultez Fonctionnalités de la version Technical Preview.

### Comment fournir des commentaires sur la version EAR

Pour nous faire part de vos commentaires sur la version EAR, appuyez ici.

## Problèmes courants et conseils de dépannage

### Application non disponible dans l'App Store

Si vous ne parvenez pas à installer l'application Citrix Workspace pour Android à partir de Google Play Store, vous pouvez télécharger l'application depuis la page de téléchargement de produits Citrix.

### Échecs d'installation

Si l'application Citrix Workspace n'est pas prise en charge par défaut sur Android TV, contactez-nous via le formulaire de demande d'amélioration.

### Authentification et ajout de magasin

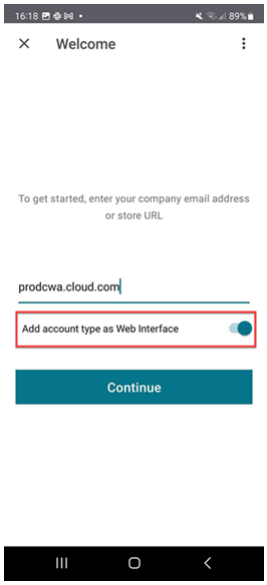
Si vous rencontrez des problèmes d'authentification ou d'ajout de magasin, recherchez les causes suivantes.

**Saisie non valide** Vous avez peut-être saisi :

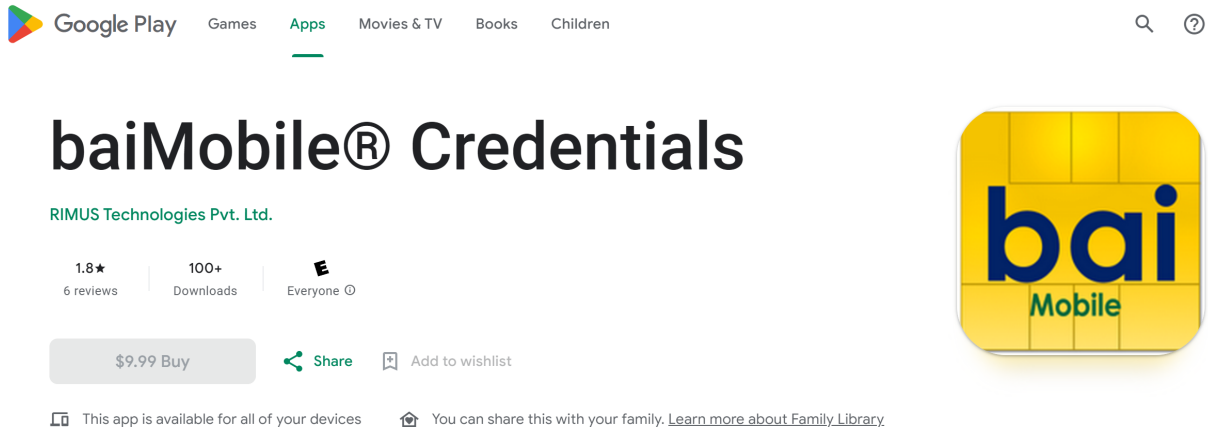
- Des informations d'identification non valides
- Une URL de magasin incorrecte
- Des informations d'identification ou une URL de magasin comportant avec des fautes de frappe
- HTTP au lieu de HTTPS.

**Mode Interface Web** Vous pouvez également essayer d'utiliser le mode **Interface Web**. Sur la première page de l'application, touchez **Commencer**. Sur la page d'**accueil**, saisisszez l'URL du magasin et activez **Ajouter un type de compte en tant qu'Interface Web**.




**Carte à puce** Si l'authentification par carte à puce ne fonctionne pas, installez l'application **baiMobile Credentials**. Si l'application baiMobile Credentials détecte votre carte à puce, contactez-nous afin que nous puissions étudier le problème de manière plus approfondie.




**Configuration des stratégies NetScaler** Pour résoudre les problèmes de connexion, consultez l'article NetScaler Gateway pour appareils mobiles du centre de connaissances.

### Lancement de session

Pour consulter les statistiques de session :

- depuis la barre d'outils de session, appuyez quatre fois sur l'icône du pointeur de la souris

  ou

- exécutez la commande `ctxsession -v` dans le terminal de session.

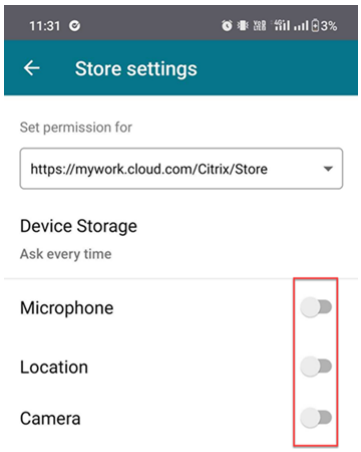
**Impossible de lancer le bureau** Pour résoudre les problèmes, consultez les articles suivants du centre de connaissances :

- Code d'erreur 2524
- Code d'erreur 2523
- Code d'erreur 2502
- Code d'erreur 2517

### Autorisations d'accès aux périphériques

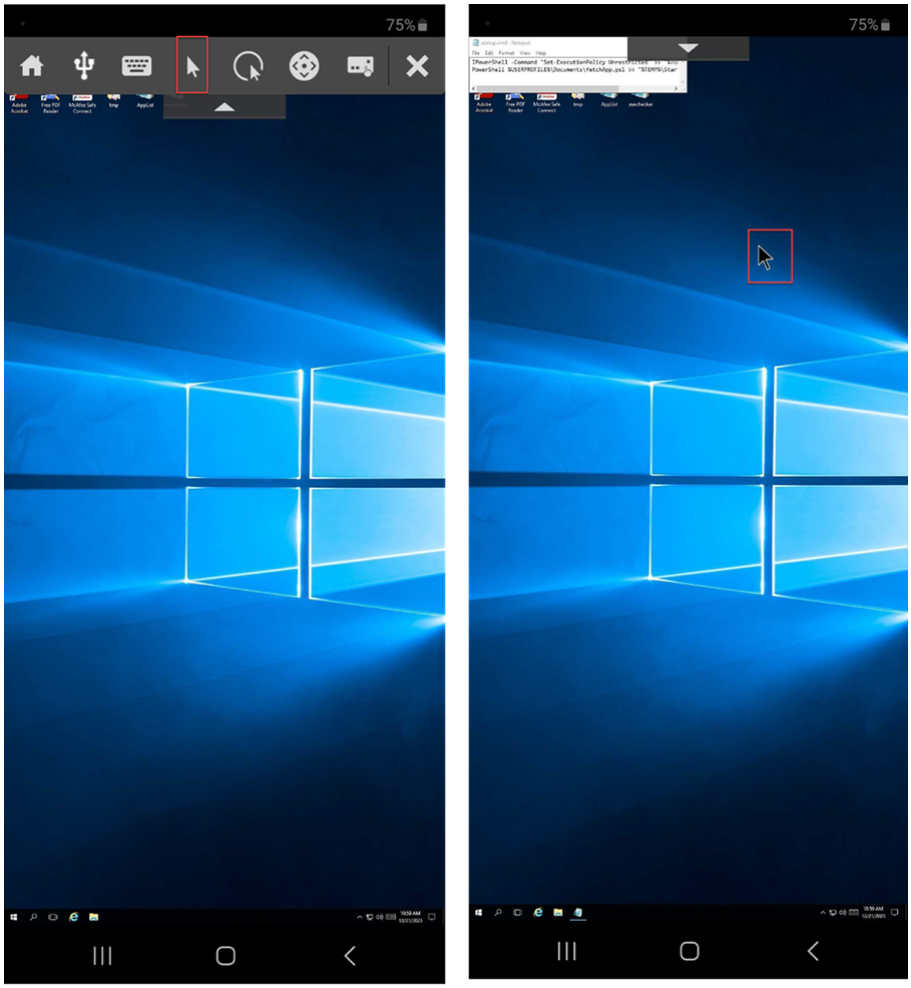
Activez les autorisations de réglage appropriées.

**Client Selective Trust** Activez les paramètres du microphone, de l'emplacement et de la caméra. Accédez à > **Paramètres** de l'application Citrix Workspace > **Paramètres du magasin**, puis activez les paramètres CST pour un magasin sélectionné.




**Activer le pointeur de la souris** Après avoir démarré une session, touchez la barre d'outils, puis l'icône du pointeur de la souris pour activer ce dernier.

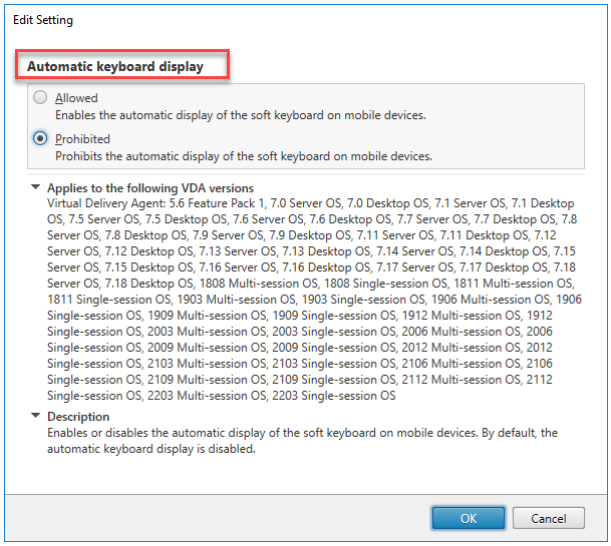
 



**Activer le clavier** Si l'administrateur de votre organisation n'a pas activé la fonctionnalité d'affichage automatique du clavier par défaut, contactez-le pour obtenir de l'aide.

Les administrateurs doivent activer la stratégie d'**affichage automatique du clavier** dans le paramètre DDC (Desktop Delivery Controller).




## FAQ

- Comment améliorer l'expérience vidéo des utilisateurs de l'application et du bureau virtuels sur les appareils à faible consommation ou les appareils mobiles ?
  - Pour plus d'informations, consultez l'article du Centre de connaissances sur l'expérience vidéo des utilisateurs.
- Accès aux ressources - Je ne vois pas mes applications ou bureaux après m'être connecté à l'application Citrix Workspace.
  - Contactez le service d'assistance de votre entreprise ou l'administrateur de votre équipe de support informatique pour obtenir de l'aide.
- Comment dépanner les problèmes de connexion lente ?
  - Suivez la solution de contournement si vous rencontrez l'un des problèmes suivants :
  - connexions lentes au site Citrix Virtual Apps and Desktops
  - Icônes d'applications manquantes
  - Messages **d'erreur du pilote de protocole** récurrents

  Solution :
  - Désactivez les propriétés de l'**adaptateur Ethernet Citrix PV** pour l'interface réseau sur :
  - Serveur Citrix Virtual Apps
  - Citrix Secure Web Gateway
  - Serveur d'Interface Web

  - Les propriétés de l'**adaptateur Ethernet Citrix PV** incluent (toutes activées par défaut) :
  - Large Send Offload
  - Offload IP Checksum
  - Offload TCP Checksum
  - Offload UDP Checksum

  Il n'est pas nécessaire de redémarrer le serveur. Cette solution s'applique à Windows Server 2003 et 2008 32 bits. Ce problème n'affecte pas Windows Server 2008 R2.

- Problème avec les touches numériques et les caractères spéciaux
  - Si les touches numériques ou les caractères IME chinois ne fonctionnent pas correctement, désactivez l'option **Clavier Unicode**. Pour ce faire, accédez à **Paramètres** > **Options du clavier** > et définissez **Utiliser clavier Unicode** sur **Désactivé**.

### Dépannage des codes d'erreur

Le tableau suivant répertorie les codes d'erreur et propose une solution probable :

| Code d'erreur | article du Centre de connaissances Citrix |
|---|---|
| Code d'erreur 437 | https://support.citrix.com/article/CTX463401 |
| Code d'erreur 41E | https://support.citrix.com/article/CTX235177 |
| Code d'erreur 546 ou 547 | https://support.citrix.com/article/CTX231798 |
| Code d'erreur 518 | https://support.citrix.com/article/CTX277571 |
| Code d'erreur 42B | https://support.citrix.com/article/CTX260992 |
| Code d'erreur 548 | https://support.citrix.com/article/CTX250706<br>https://support.citrix.com/article/CTX578359 |
| Adresse du serveur incorrecte + Code d'erreur 548 | https://support.citrix.com/article/CTX554245 |
| Code d'erreur 451 | https://support.citrix.com/article/CTX256708 |
| Erreur générale | https://support.citrix.com/article/CTX219073 |
| Essayer de vous reconnecter | Désactivez l'option UDP. Accédez aux **paramètres** de l'application > **Avancés** > **EDT** |

### Messages d'erreur et description

Le tableau suivant fournit une liste des erreurs et leur description. La solution la plus probable est de contacter le support technique de Citrix pour obtenir de l'aide :

| Erreur | Description |
|---|---|
| SessionManager.Launch.EngineLoadFailed | Le moteur ICA n'a pas pu être chargé ou initialisé. |
| SessionManager.Launch.ConnectionFailed | Le moteur ICA a été interrompu avant la connexion. |
| SessionManager.Launch.LogonFailed | Session déconnectée avant la fin de l'ouverture de session |
| SessionManager.LeaseResolution.Failed | Tentative de lancement du bail impossible. |
| SessionManager.clxmtp.SoftDeny | Échec de la négociation CLXMTP du moteur (refus flexible). |
| SessionManager.clxmtp.SoftDeny_Implicit | Échec de la connexion CLXMTP du moteur (refus flexible implicite). |
| Transport.Connect.NoCGP_Fail | Connexion impossible (Common Gateway Protocol désactivé). |
| Transport.Connect.FallbackFail | Connexion impossible, solution de secours ICA tentée. |
| Transport.Connect.Fail | Connexion indisponible. |

## SDK et API

December 11, 2023

### SDK du canal virtuel Citrix

Le SDK du canal virtuel Citrix prend en charge l'écriture de pilotes du côté serveur et du côté client afin de fournir d'autres canaux virtuels à l'aide du protocole ICA. Les applications de canal virtuel côté serveur se trouvent sur des serveurs Citrix Virtual Apps and Desktops.

Cette version du SDK prend en charge l'écriture de nouveaux canaux virtuels pour l'application Citrix Workspace pour Android. Si vous souhaitez écrire des pilotes virtuels pour d'autres plates-formes clientes, contactez le support technique Citrix.

Le SDK du canal virtuel offre ce qui suit :

- Les interfaces AIDL Citrix Android Virtual Driver : **IVCService.aidl** et **IVCCallback.aidl** utilisées avec les fonctions de canal virtuel dans le SDK de l'API Citrix Server (WFAPI SDK) pour créer de nouveaux canaux virtuels.
- Une classe helper **Marshall.java** conçue pour faciliter l'écriture de vos propres canaux virtuels.
- Un code source opérationnel pour trois exemples de programmes de canal virtuel qui illustrent les techniques de programmation.

Le SDK de canal virtuel requiert le SDK WFAPI pour écrire sur le côté serveur du canal virtuel. Pour plus d'informations sur la documentation du SDK, veuillez consulter Citrix Virtual Channel SDK for Citrix Workspace app for Android.

## Fin de prise en charge

June 26, 2024

Les annonces de cet article visent à vous avertir à l'avance des plates-formes, des produits Citrix et des fonctionnalités qui vont disparaître. Grâce à ces annonces, vous pouvez prendre les décisions appropriées en temps opportun.

Citrix surveille l'utilisation des clients et leurs commentaires pour déterminer quand les retirer. Les annonces peuvent être modifiées dans les versions ultérieures et peuvent ne pas contenir chaque fonctionnalité amenée à disparaître.

Les éléments obsolètes ne sont pas retirés immédiatement. Citrix continue de les prendre en charge dans cette version, mais ils seront retirés à l'avenir.

| Élément | Abandon annoncé dans la version de l'application Citrix Workspace | Supprimé dans la version de l'application Citrix Workspace | Solution alternative |
|---|---|---|---|
| Systèmes d'exploitation Android antérieurs à la version 12.0 | 24.5.0 | 24.7.0 | Prise en charge d'Android 12.0 et versions ultérieures |
| Prise en charge des protocoles TLS 1.0 et TLS 1.1 | 24.4.0 | Future version | Protocole TLS 1.2 ou TLS 1.3 |

| Élément | Abandon annoncé dans la version de l'application Citrix Workspace | Supprimé dans la version de l'application Citrix Workspace | Solution alternative |
|---|---|---|---|
| XenApp Services (également connus sous le nom de PNAgent) | 24.3.5 | Future version | Dans l'application Workspace, connectez-vous aux magasins à l'aide de l'URL du magasin plutôt que de l'URL de XenApp Services |
| Systèmes d'exploitation Android antérieurs à la version 9.0 | 24.1.0 | 24.3.0 | Prise en charge d'Android 9.0 et versions ultérieures |
| Application Citrix Workspace pour Android sur ChromeOS | 23.8.0 | 23.12.0 | Pour utiliser l'application Citrix Workspace sur ChromeOS, installez l'extension. |
| Workspace avec intelligence | - | 23.2.0 | - |
| Prise en charge pour Android Enterprise | - | 23.2.0 | - |
| Expérience Workspace Mobile | - | 23.2.0 | - |
| Authentification RSA SecurID | 2008 | - | - |
| Systèmes d'exploitation Android antérieurs à la version 7.0 | 1903 | 1906 | La version 7.0 (Nougat) et les versions ultérieures sont prises en charge |