Application Citrix Workspace

Contents

Application Citrix Workspace

April 25, 2024

À propos de l'application Citrix Workspace

L'application Citrix Workspace fournit un accès instantané, sécurisé et transparent à toutes les ressources dont vos utilisateurs finaux ont besoin pour rester productifs. L'application Citrix Workspace inclut l'accès aux bureaux virtuels, aux applications virtuelles, aux applications Web et SaaS, ainsi qu'à des fonctionnalités telles que la navigation intégrée et l'authentification unique (en tout lieu et indépendamment de l'appareil utilisé).

L'application Citrix Workspace est une application cliente qui peut être déployée sur des appareils à la fois dans des environnements cloud et locaux. Elle s'appuie sur les fonctionnalités de ce qui était auparavant connu sous le nom de Citrix Receiver et inclut des technologies du client Citrix telles que HDX, les plug-ins Citrix Gateway et Secure Private Access.

L'application cliente est optimisée pour fonctionner sur tous les systèmes d'exploitation clients tels que Windows, macOS, Linux, iOS et Android. Il est également possible d'y accéder via un navigateur. Pour en savoir plus sur les navigateurs pris en charge, consultez l'article Compatibilité Workspace Browser.

L'application Citrix Workspace, basée sur le protocole Citrix et HDX (expérience haute définition), fournit des sessions d'applications et de bureaux virtuel de qualité. Elle a été améliorée pour offrir une connexion et une expérience de navigation Internet sécurisées, une gestion facile de vos applications et de vos bureaux, des fonctionnalités de recherche avancées, etc.

> **Remarque :**
>
> L'interface utilisateur de l'application peut varier en fonction du déploiement des ressources, c'est-à-dire sur Cloud (avec la plate-forme Workspace) ou sur site (avec la plate-forme StoreFront).

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

Pour plus d'informations sur les différences entre les versions actuelles et LTSR, consultez la section Étapes clés du cycle de vie de l'application Citrix Workspace.

L'application Citrix Workspace est disponible pour les systèmes d'exploitation suivants :

- Application Citrix Workspace pour Android
- Application Citrix Workspace pour ChromeOS
- Application Citrix Workspace pour HTML5

- Application Citrix Workspace pour iOS
- Application Citrix Workspace pour Linux
- Application Citrix Workspace pour Mac
- Application Citrix Workspace pour Windows
- Application Citrix Workspace pour Windows (Store)

> **Important**
>
> **Données collectées pour les mises à jour de l'application Citrix Workspace :**
>
> En ce qui concerne les périphériques connectés à Internet, l'application Citrix Workspace peut, sans préavis, rechercher les mises à jour disponibles au téléchargement et à l'installation sur le périphérique, et informer l'utilisateur de leur disponibilité. Seules les informations autres que les informations d'identification personnelle sont transmises lorsque cela se produit, sauf dans la mesure où les adresses IP peuvent être considérées comme d'identification personnelle dans certaines juridictions.

Configurer l'application Citrix Workspace à l'aide de Global App Configuration Service

Global App Configuration Service fournit une interface centralisée permettant de configurer les paramètres de l'application Citrix Workspace pour les utilisateurs. Vous pouvez configurer les paramètres des magasins dans le cloud et sur site à partir d'une interface unique. Ces paramètres s'appliquent aux appareils gérés et non gérés (BYOD). Pour plus d'informations, consultez Global App Configuration Service.

Langues prises en charge

Les applications Citrix Workspace sont conçues pour être utilisées dans des langues autres que l'anglais. Cette section répertorie les langues prises en charge dans la dernière version des applications Citrix Workspace.

Le tableau suivant répertorie les langues prises en charge par l'application Citrix Workspace sur différents systèmes d'exploitation ou plates-formes. Le symbole ☑ indique que l'application est disponible dans cette langue.

Langue	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Windows Store
Anglais	☑	☑	☑	☑	☑	☑	☑	☑
Danois	☑			☑				

Langue	Android	ChromeOS	HTML5	iOS	Linux	macOS	Windows	Windows Store
Néerlandais	☑	☑	☑	☑	☑	☑	☑	☑
Français	☑	☑	☑	☑	☑	☑	☑	☑
Allemand	☑	☑	☑	☑	☑	☑	☑	☑
Italien	☑	☑	☑	☑	☑	☑	☑	☑
Japonais	☑	☑	☑	☑	☑	☑	☑	☑
Coréen	☑	☑	☑	☑	☑		☑	☑
Portugais (Brésil)	☑	☑	☑	☑	☑	☑	☑	☑
Russe		☑	☑		☑		☑	☑
Chinois simplifié	☑	☑	☑	☑	☑	☑	☑	☑
Espagnol	☑	☑	☑	☑	☑	☑	☑	☑
Suédois	☑			☑				
Chinois traditionnel		☑	☑				☑	☑

Indicateur de fonctionnalités (feature flag)

Cet article traite de la gestion des feature flag et des différentes applications Citrix Workspace prenant en charge les feature flag.

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.

Le tableau suivant présente les différentes applications prenant en charge les feature flag et les versions dans lesquelles des feature flag ont été introduits dans ces applications.

Application	Prise en charge des feature flag	Version	Documentation
Application Citrix Workspace pour Android	Oui	10.7.5	Gestion des feature flag pour l'application Citrix Workspace pour Android
Application Citrix Workspace pour ChromeOS	Oui	1908	Gestion des feature flag pour l'application Citrix Workspace pour ChromeOS
Application Citrix Workspace pour HTML5	Oui	1908	Gestion des feature flag pour l'application Citrix Workspace pour HTML5
Application Citrix Workspace pour iOS	Oui	10.4.10	Gestion des feature flag pour l'application Citrix Workspace pour iOS
Application Citrix Workspace pour Linux	Oui	2109	Gestion des feature flag pour l'application Citrix Workspace pour Linux
Application Citrix Workspace pour Mac	Oui	2010	Gestion des feature flag pour l'application Citrix Workspace pour Mac
Application Citrix Workspace pour Windows	Oui	2012	Gestion des feature flag pour l'application Citrix Workspace pour Windows

Mise à jour importante sur Citrix Receiver

L'application Citrix Workspace remplace Citrix Receiver depuis août 2018. Bien que vous puissiez toujours télécharger les anciennes versions de Citrix Receiver, les nouvelles fonctionnalités et améliorations sont publiées pour l'application Citrix Workspace.

L'application Citrix Workspace est un nouveau client Citrix qui fonctionne de manière similaire à Citrix Receiver. Elle est complètement rétrocompatible avec l'infrastructure Citrix de votre entreprise. L'application Citrix Workspace offre toutes les fonctionnalités de Citrix Receiver, ainsi que de nouvelles fonctionnalités basées sur le déploiement Citrix de votre entreprise.

L'application Citrix Workspace repose sur la technologie Citrix Receiver et elle est entièrement rétrocompatible avec toutes les solutions Citrix.

Pour plus d'informations, visitez la page des questions fréquemment posées sur l'application Workspace.

Extensions Web de Citrix Workspace

April 25, 2024

Avec l'extension Web de Citrix Workspace, vous pouvez lancer vos applications d'espace de travail n'importe où sans fichier `.ica`, ce qui rend votre expérience plus sûre et plus fiable. L'ouverture de vos applications avec l'extension de navigateur permet de centraliser toutes vos applications et tous vos bureaux, de suivre facilement votre travail et de libérer votre bureau de tout encombrement. L'extension Web de Citrix Workspace permet également de bénéficier de la fonction App Protection contre les captures d'écran et de garantir la continuité des services.

Installation des extensions Web de Citrix Workspace

Pour installer l'extension Web de Citrix Workspace, procédez comme suit :

1. Accédez au magasin Web de votre navigateur préféré :
   - Chrome Web Store
   - Modules complémentaires pour Microsoft Edge
   - App Store pour Mac
2. Ajoutez et confirmez l'installation de l'extension Web de Citrix Workspace via le magasin d'applications de votre navigateur préféré.
3. Confirmez le message contextuel indiquant que vous souhaitez ajouter l'extension Web si nécessaire.
4. (Facultatif) Sélectionnez l'icône représentant une pièce de puzzle en haut à droite du navigateur pour épingler le navigateur afin d'y accéder facilement.
5. Sélectionnez **Ajouter une extension**.

6. Sélectionnez l'icône de punaise pour épingler l'extension.

L'extension Web de Citrix Workspace est maintenant installée.

Pour plus d'informations sur l'extension Web de Citrix Workspace, consultez le blog sur l'extension Web de Citrix Workspace.

Ouvrir des applications SaaS au sein de votre instance Citrix Workspace

Si l'extension Web de Citrix Workspace n'est pas encore activée sur votre instance de Workspace, procédez comme suit :

1. Sélectionnez le profil de votre compte dans la fenêtre Workspace.
2. Sélectionnez **Avancé** dans le menu du profil.
3. Sélectionnez **Utiliser le navigateur Web** dans la fenêtre **Préférences de lancement des applications et des postes de travail**.
4. Confirmez **Ouvrir Citrix Workspace Launcher** dans la fenêtre contextuelle.

Vos applications SaaS s'ouvrent désormais dans la fenêtre de votre application Citrix Workspace.

Tableau des fonctionnalités de l'application Citrix Workspace

L'application Citrix Workspace fournit une gamme de fonctionnalités selon les plates-formes ou les systèmes d'exploitation. Grâce à ce tableau des fonctionnalités, vous pouvez clairement comprendre la disponibilité des fonctionnalités sur différentes plates-formes.

L'extension Web de Citrix Workspace est accessible depuis n'importe quel ordinateur doté d'un navigateur Web compatible et d'une connexion Internet. Pour utiliser toutes les fonctionnalités de l'extension Web de Citrix Workspace, les types de navigateur suivants sont pris en charge :

Nom du navigateur	Version
Google Chrome	Dernière version
Microsoft Edge	Dernière version
Apple Safari	Dernière version

App Protection

May 31, 2024

App Protection est une fonctionnalité de l'application Citrix Workspace qui offre une sécurité renforcée lors de l'utilisation des ressources publiées Citrix Virtual Apps and Desktops. App Protection est prise en charge pour les déploiements locaux de Citrix Virtual Apps and Desktops et Citrix DaaS (anciennement Citrix Virtual Apps and Desktops Service) avec StoreFront et Workspace. Cela signifie qu'App Protection est prise en charge dans tous les environnements cloud, environnements sur site et environnements hybrides. App Protection est également pris en charge lorsque vous vous connectez à StoreFront ou à Workspace via ADC Gateway.

Deux stratégies offrent des fonctionnalités de protection contre les programmes d'enregistrement de frappe et de capture d'écran dans une session Citrix HDX. Les stratégies ainsi que l'application Citrix Workspace 2203.1 LTSR pour Windows, Citrix Workspace 2001 pour Mac ou Citrix Workspace 2108 pour Linux (versions minimales) peuvent aider à protéger les données contre les programmes d'enregistrement de frappe et de capture d'écran.

Lorsque vous activez la protection contre l'enregistrement de frappe :

- L'enregistreur de frappe voit s'afficher des combinaisons de frappes chiffrées.
- Cette fonction n'est active que lorsqu'une fenêtre protégée a le focus.

Lorsque la protection contre les programmes d'enregistrement de capture d'écran est activée :

- Sous Windows OS et macOS, lorsque vous capturez un écran, seul le contenu de la fenêtre protégée est vide. Cette fonctionnalité est active lorsqu'une fenêtre protégée n'est pas réduite. Sur le système d'exploitation Linux, l'intégralité de la capture est vide. Cette fonctionnalité est active, qu'une fenêtre protégée soit réduite ou non.
- Lorsque vous utilisez le bouton **Impression écran** du système d'exploitation Windows pour prendre des captures d'écran, les données ne sont pas copiées dans le presse-papiers. Pour prendre des captures d'écran à l'aide du bouton **Impression écran**, réduisez les applications protégées.

Vous pouvez configurer les stratégies via PowerShell et Web Studio. Pour de plus amples informations, consultez la section Configurer App Protection pour les applications et les bureaux virtuels.

Après avoir acheté cette fonctionnalité, assurez-vous d'activer la licence App Protection.

> **Clause d'exclusion de responsabilité**
>
> Les stratégies de protection des applications fonctionnent en filtrant l'accès aux fonctions requises du système d'exploitation sous-jacent (appels d'API spécifiques nécessaires pour capturer des écrans ou des frappes de clavier). Cela signifie que les stratégies App Protection peuvent fournir une protection même contre les outils de piratage personnalisés et spécifiques. Cependant, à mesure que les systèmes d'exploitation évoluent, de nouveaux programmes d'enregistrement de frappe et de capture d'écran peuvent émerger. Bien que nous continuions à les identifier et à les traiter, nous ne pouvons pas garantir une protection complète dans des config-

> urations et des déploiements spécifiques.
>
> Les stratégies Citrix App Protection fonctionnent efficacement avec les composants sous-jacents du système d'exploitation, y compris les fichiers ICA. Citrix peut ne pas être en mesure de fournir son assistance si une altération ou une modification intentionnelle des composants sous-jacents était détectée, afin de préserver l'intégrité des stratégies appliquées.

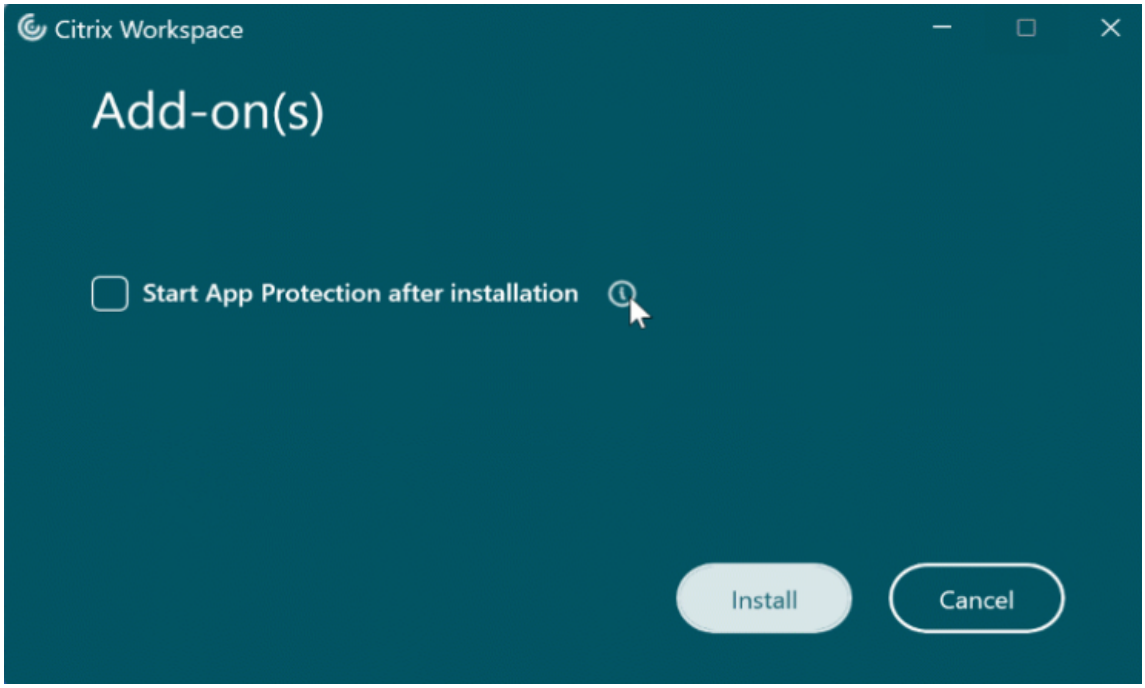
Vérifiez si App Protection est installé

Application Citrix Workspace pour Windows

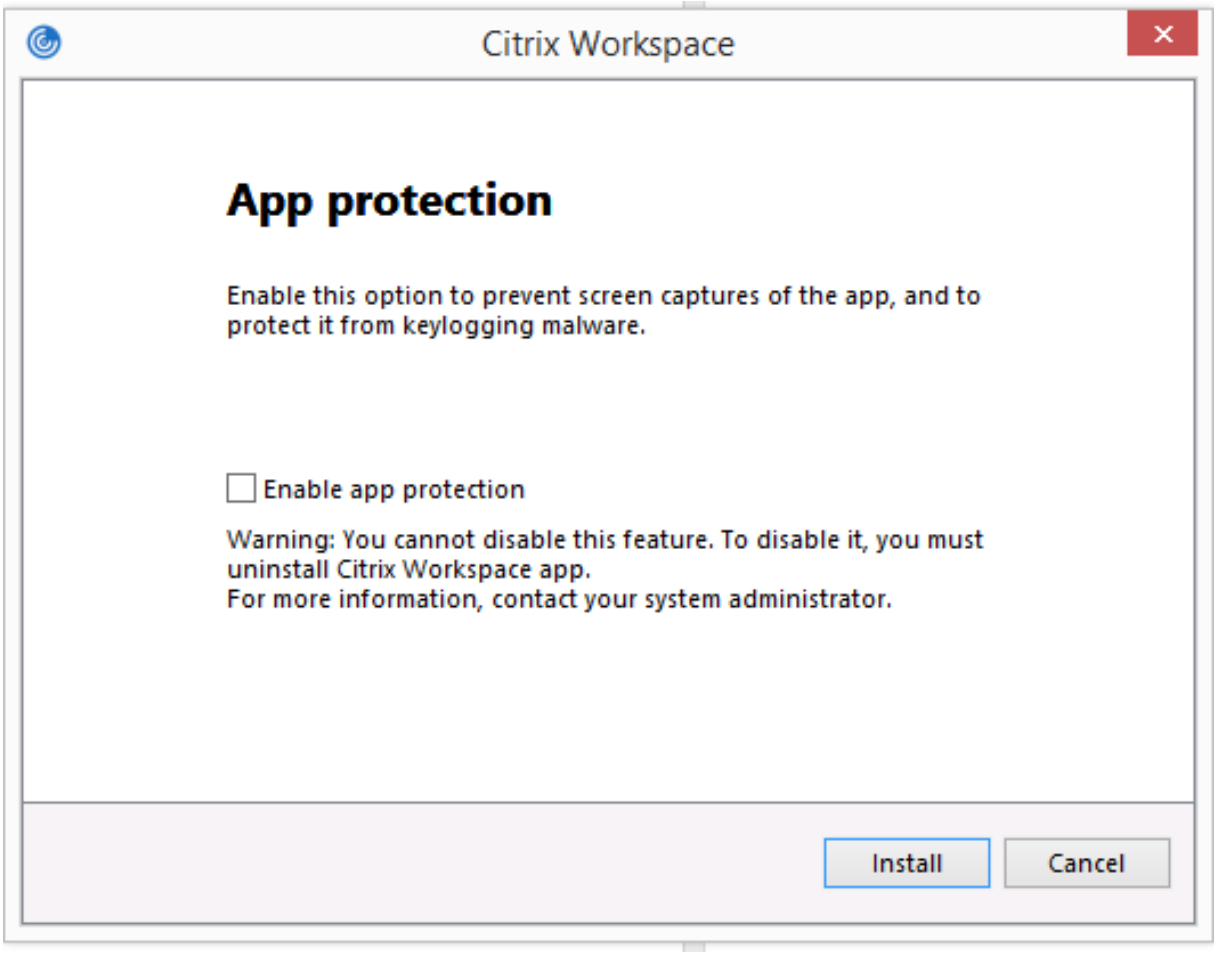
À partir de la version 2212 de l'application Citrix Workspace, App Protection est installée par défaut. Toutefois, le composant pourrait être actif ou inactif selon que l'utilisateur a sélectionné la case à cocher **Démarrer App Protection après l'installation** ou non.

- Pour les versions de l'application Citrix Workspace antérieures à la version 2311 :

- À partir de la version 2311 de l'application Citrix Workspace :



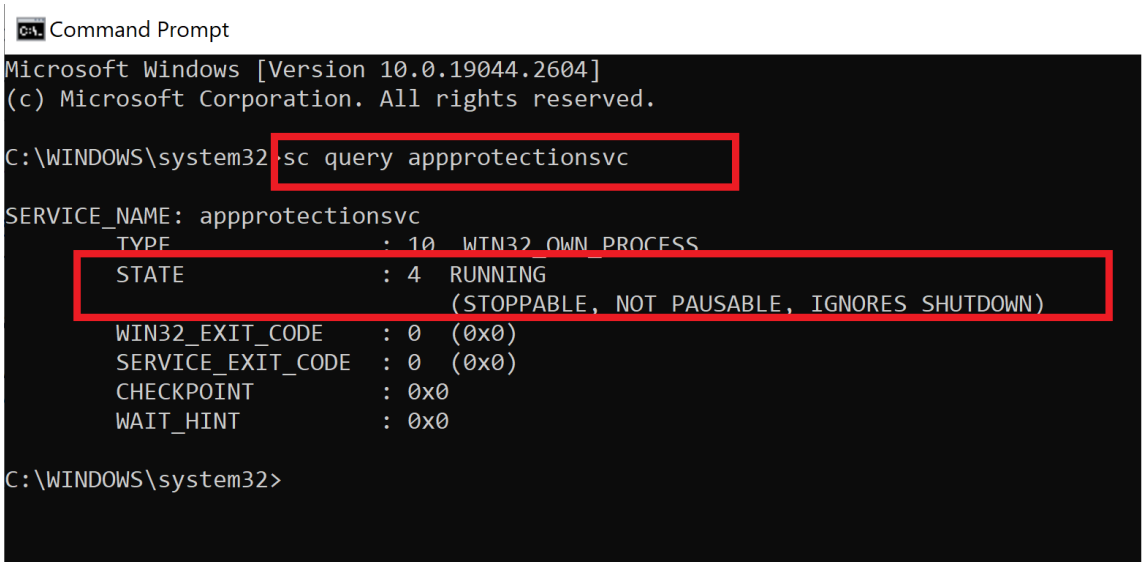
Pour les versions de l'application Citrix Workspace antérieures à la version 2212, App Protection est installé et activé uniquement si vous cochez la case **Activer App Protection** lors de l'installation de l'application Citrix Workspace.



App Protection peut être dans l'état **ARRÊTÉ** ou **EN COURS D'EXÉCUTION**.
Pour vérifier l'état du service, réalisez l'une des étapes suivantes :

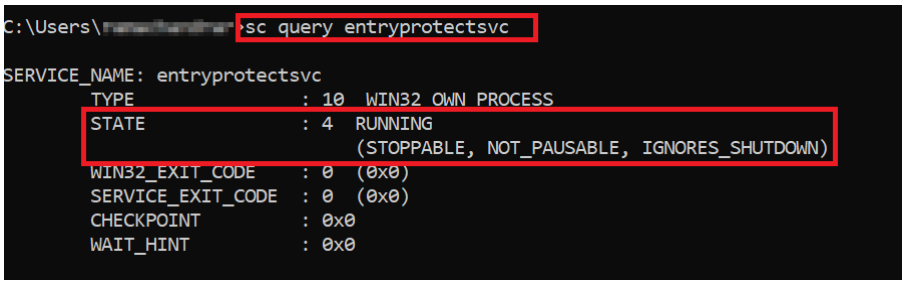
- Pour la version 2206 ou ultérieure de l'application Citrix Workspace, exécutez la commande suivante :

```
sc query appprotectionsvc
<!--NeedCopy-->
```

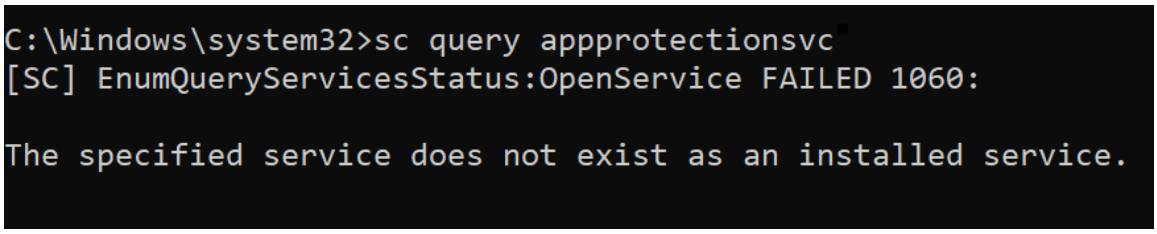



- Pour les versions de l'application Citrix Workspace antérieures à la version 2206, exécutez la commande suivante :

```
sc query entryprotectsvc
<!--NeedCopy-->
```



> **Remarque :**
>
> Pour les versions de l'application Citrix Workspace antérieures à la version 2212, si vous n'avez pas coché la case **Activer App Protection** lors de l'installation de l'application Citrix Workspace et exécuté la commande précédente pour vérifier son état, le message d'erreur suivant s'affiche :



Comportement d'App Protection dans différents environnements

Le comportement d'App Protection dépend de la manière dont vous accédez aux ressources configurées avec les stratégies d'App Protection. Ces ressources incluent Virtual Apps and Desktops, les applications Web internes et les applications SaaS. Vous pouvez accéder à ces ressources à l'aide d'un client d'application Citrix Workspace natif pris en charge ou un navigateur Web. Les performances d'App Protection varient selon les environnements :

- **Applications Citrix Receiver ou Citrix Workspace non prises en charge** : les ressources configurées avec les stratégies d'App Protection ne sont pas disponibles.
- **Versions de l'application Citrix Workspace prises en charge** : les ressources configurées avec les stratégies d'App Protection sont disponibles et se lancent correctement.
- **Lancement hybride à l'aide de l'URL du magasin Workspace** : les ressources configurées avec les stratégies d'App Protection sont toujours disponibles. Pour lancer correctement les ressources sur un navigateur Web à l'aide de l'URL du magasin Workspace, consultez la section App Protection pour le lancement hybride de Workspace.
- **Lancement hybride à l'aide de l'URL du magasin StoreFront** : les ressources configurées avec les stratégies d'App Protection ne sont pas disponibles si la personnalisation de StoreFront n'est pas déployée. Pour lancer correctement les ressources sur un navigateur Web à l'aide de l'URL du magasin StoreFront, consultez la section App Protection pour le lancement hybride de StoreFront.

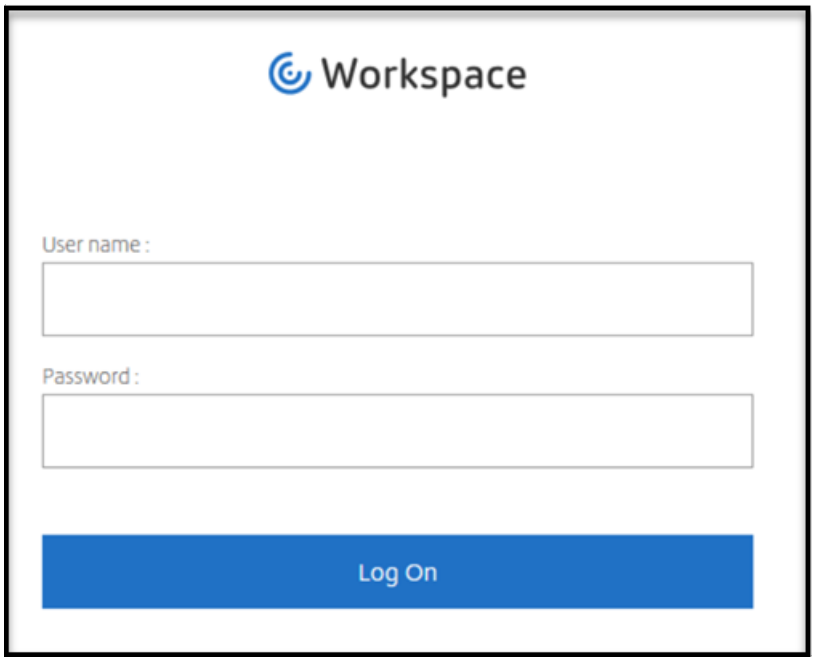
La protection est appliquée dans les conditions suivantes :

- **Prévention des captures d'écran** : pour les applications Citrix Workspace pour Windows et Mac, cette fonctionnalité est activée si une fenêtre protégée est visible à l'écran. Pour désactiver la protection, réduisez toutes les fenêtres protégées. Pour l'application Citrix Workspace pour Linux, elle est activée si une fenêtre protégée est active. Pour désactiver la protection, fermez toutes les fenêtres protégées.
- **Protection contre l'enregistrement de frappe** : activée si le focus est sur une fenêtre protégée. Pour désactiver la protection, déplacez le focus sur une autre fenêtre.

Éléments inclus dans la App Protection?

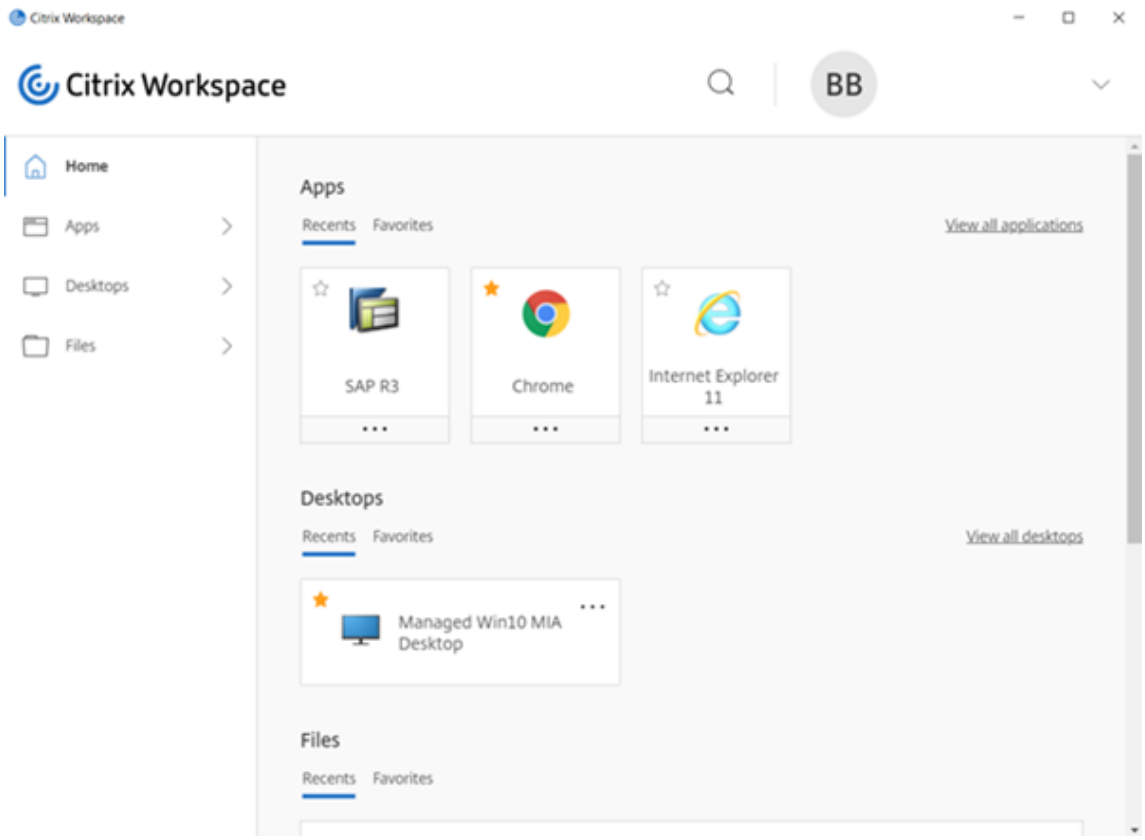
La App Protection protège les fenêtres Citrix suivantes :

- Fenêtres de connexion à Citrix

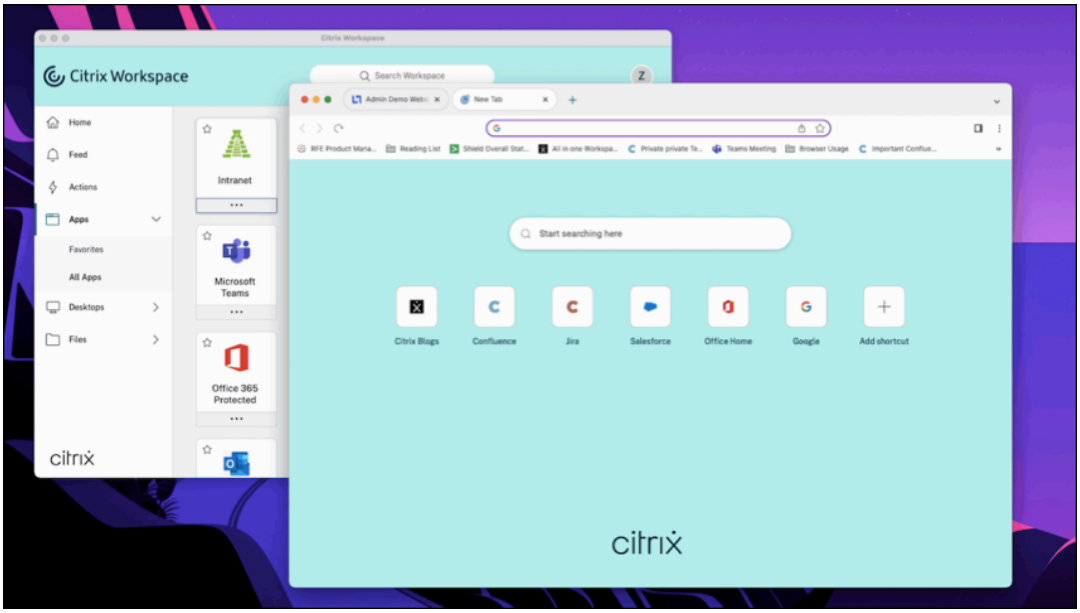


- Fenêtres de session HDX de l'application Citrix Workspace (exemple, bureau géré)

- Fenêtres du magasin en libre-service



- Applications Web et SaaS
  - Applications Citrix Workspace pour Windows et pour Mac : les applications Web et SaaS s'ouvrent dans Citrix Enterprise Browser. Si les applications sont configurées pour bénéficier des stratégies App Protection via Citrix Secure Private Access, App Protection s'applique par onglet.



  - Application Citrix Workspace pour Linux : Citrix Enterprise Browser n'est pas pris en charge.

Éléments non inclus dans la App Protection?

- Éléments suivants sous l'icône des applications Citrix Workspace dans la barre de navigation :
  - Centre de connexion
  - Tous les liens sous Préférences avancées
  - Personnaliser
  - Rechercher les mises à jour
  - Déconnexion
- Si vous choisissez de protéger un bureau virtuel en bloquant l'enregistrement de capture d'écran, les utilisateurs pourront toujours partager l'écran à partir des applications du bureau virtuel. Toutefois, pour les applications extérieures au bureau virtuel, les utilisateurs ne pourront pas prendre de captures d'écran ni enregistrer le bureau virtuel.

Limitations

Les limitations suivantes sont délibérées :

- Le lancement d'applications et de bureaux virtuels utilisant App Protection est bloqué lorsqu'ils sont accessibles dans le cadre de sessions RDP.
- Au cours de la session RDP, App Protection n'est pas pris en charge sur les applications Web et SaaS ouvertes à l'aide de Citrix Enterprise Browser.
- App Protection n'est pas pris en charge dans les scénarios à double saut et à sauts multiples.
- La protection des applications n'est pas prise en charge si vous utilisez une version non prise en charge de l'application Citrix Workspace ou de Citrix Receiver. Dans ce cas, les ressources sont masquées.
- Lorsque les fonctionnalités d'App Protection sont appliquées à des applications et à des bureaux virtuels, le partage d'écran sortant peut être affecté si l'optimisation est utilisée.
- L'application Citrix Workspace avec App Protection peut ne pas être compatible avec d'autres solutions de sécurité ou applications utilisant une technologie sous-jacente similaire.
- La App Protection n'est pas prise en charge lorsque vous lancez des ressources depuis Citrix Secure Browser ou avec Remote Browser Isolation.
- Dans l'application Citrix Workspace pour Linux, vous ne pouvez pas utiliser d'applications Snap lorsque la protection des applications est installée.

Protection contextuelle des applications

La protection contextuelle des applications offre la flexibilité d'appliquer les stratégies de protection des applications de manière conditionnelle à un sous-ensemble d'utilisateurs, en fonction des utilisateurs, de leur appareil et de la position du réseau. Pour plus d'informations, consultez les articles suivants :

- App Protection contextuelle pour StoreFront
- App Protection contextuelle pour Workspace

Protection des applications pour un lancement hybride

On parle de lancement hybride de Citrix Virtual Apps and Desktops lorsque vous vous connectez à l'application Citrix Workspace via le navigateur (Citrix Workspace pour le Web) et que vous utilisez les applications via l'application Citrix Workspace native. Le terme hybride désigne le résultat de l'utilisation combinée de l'application Citrix Workspace pour le Web et de l'application native Citrix Workspace pour connecter et utiliser les ressources. La protection des applications prend en charge le lancement hybride dans Workspace et StoreFront. Pour plus d'informations, consultez les articles suivants :

- App Protection pour le lancement hybride de Workspace
- App Protection pour le lancement hybride de StoreFront

Configuration système requise et compatibilité

April 29, 2024

Configuration système requise

Au préalable, assurez-vous d'avoir installé l'application Citrix Workspace à l'aide de droits d'administrateur.

Versions minimales des composants Citrix

- Application Citrix Workspace 2108 pour Linux
- Application Citrix Workspace 2203.1 LTSR pour Windows
- Application Citrix Workspace 2002 pour Windows
- Application Citrix Workspace 2305.1 pour Windows (Store)

- Application Citrix Workspace 2001 pour Mac
- StoreFront 1912 LTSR
- Delivery Controller 1912
- Licences Citrix valides. Pour plus d'informations, contactez votre représentant commercial Citrix ou votre partenaire Citrix.

> **Remarque :**
>
> Si les utilisateurs utilisent des appareils ou des versions de l'application Workspace qui ne prennent pas en charge App Protection, ils ne peuvent pas accéder aux ressources protégées. Les ressources protégées incluent Virtual Apps and Desktops et les applications Web et SaaS.

Licences

La section suivante explique les différents types de licences disponibles pour App Protection en fonction des produits, des plateformes et des cas d'utilisation.

VDI géré par le service informatique Pour toutes les éditions de VDI géré par le service informatique, la protection des applications est disponible sous forme de module complémentaire. Pour plus d'informations, consultez la section VDI géré par le service informatique.

Citrix DaaS pour Hyperscalers

- Azure
- Google
- AWS

Citrix DaaS Dans l'article Feature Matrix for Citrix DaaS, accédez à **DaaS cloud Services > Security and Monitoring > App Protection**.

Citrix Secure Private Access App Protection est disponible sous forme de pièce jointe autonome pour Citrix Secure Private Access. Pour plus d'informations, accédez à **Citrix cloud services > Citrix Secure Private Access** dans l'article Service descriptions for Citrix Services.

Abonnement Citrix Universal La protection des applications est incluse dans les services suivants :

- Citrix Universal Premium
- Citrix Universal Premium Plus

Elle est disponible en tant que module complémentaire avec les éditions suivantes :

- Citrix Universal Advanced
- Citrix Universal Advanced Plus

Pour en savoir plus, consultez cet article.

Plates-formes du système d'exploitation

L'exécution des stratégies App Protection est installée sur le point de terminaison *à partir duquel* vous vous connectez et non sur le VDA *auquel* vous vous connectez. Par conséquent, seule la version du système d'exploitation du point de terminaison a une importance. (App Protection peut se connecter aux VDA hébergés sur tous les systèmes d'exploitation pris en charge décrits dans Configuration requise pour Citrix Virtual Apps and Desktops.)

La fonctionnalité de protection des applications est prise en charge sur les points de terminaison exécutant les systèmes d'exploitation suivants :

- **Windows :**
  - Windows 11 (édition 64 bits)
  - Windows 10 (éditions 32 et 64 bits)

    > **Remarque :**
    >
    > App Protection n'est pas pris en charge sur les périphériques dotés de l'édition Arm64 du système d'exploitation Windows.

- **macOS :**
  - High Sierra (10.13) et versions ultérieures
- **Linux :**
  - Ubuntu 22.04 64 bits
  - RHEL 9 64 bits
  - Système d'exploitation ARM64 Raspberry Pi (basé sur Debian 11 (bullseye))

> **Remarque :**
>
> Pour App Protection, l'application Citrix Workspace pour Linux nécessite Gnome Display Manager avec les systèmes d'exploitation pris en charge.

Matrice de compatibilité

Matrice de compatibilité pour les produits basés sur Citrix Cloud

Les fonctionnalités App Protection compatibles avec les produits basés sur Citrix Cloud sont les suivantes :

Fonctionnalité	Citrix Cloud	Citrix Cloud Japan
Protection contre l'enregistrement de frappe et protection contre les captures d'écran pour les applications et bureaux virtuels	Oui	Oui
Protection contre l'enregistrement de frappe et protection contre les captures d'écran pour les applications Web ou SaaS	Oui	Non
Anti-DLL pour Windows	Oui	Oui via un objet de stratégie de groupe (GPO)
Liste d'autorisations anti-DLL	Oui	Oui via un GPO
Global App Configuration Service (GACS)	Oui	Non
Protection des écrans d'authentification et de Self-Service Plug-in pour Linux	Oui	Oui via AuthManConfig.xml
Protection des écrans d'authentification et de Self-Service Plug-in pour Mac	Oui, par le biais du GACS	Oui, par le biais du GACS
Protection des écrans d'authentification et de Self-Service Plug-in pour Windows	Oui	Oui via un GPO
Événements de capture d'écran CAS App Protection	Oui	Non
Protection contextuelle des applications	Oui	Oui, en fonction de l'utilisateur
Détection d'altération des stratégies	Oui	Oui

Fonctionnalité	Citrix Cloud	Citrix Cloud Japan
Vérification de la posture d'App Protection	Oui	Oui
Liste d'autorisations ou filtres d'applications locales - Windows	Oui	Oui via un GPO
App Protection locale – Windows	Oui	Oui via un GPO

Fonctionnalités de protection des applications

June 19, 2024

Cet article présente les fonctionnalités de protection des applications prises en charge par l'application Citrix Workspace pour Windows, l'application Citrix Workspace pour Linux et l'application Citrix Workspace pour Mac.

Protection contre l'enregistrement de frappe

Grâce au chiffrement, les fonctionnalités de protection contre l'enregistrement de frappe d'App Protection brouillent le texte que l'utilisateur saisit à la fois sur le clavier physique et à l'écran. La fonctionnalité de protection contre l'enregistrement de frappe chiffre le texte avant qu'un outil d'enregistrement de frappe ne puisse y accéder depuis le niveau du noyau ou du système d'exploitation. Un enregistreur de frappe installé sur le point de terminaison client lisant les données du système d'exploitation ou du pilote capture uniquement le texte haché au lieu des frappes que l'utilisateur effectue. Les stratégies App Protection sont actives non seulement pour les applications et les bureaux publiés, mais également pour les boîtes de dialogue d'authentification de Citrix Workspace. Votre Citrix Workspace est protégé dès que vos utilisateurs ouvrent la première boîte de dialogue d'authentification. La protection des applications brouille les frappes et renvoie du texte indéchiffrable aux enregistreurs de touches.

Les administrateurs peuvent choisir d'activer la protection contre l'enregistrement de frappe pour les types de ressources suivants :

- Applications et bureaux virtuels
- Applications Web et SaaS internes
- Écrans d'authentification
- Écrans Self-Service Plug-In (SSP)

Prévention de capture d'écran

La prévention de capture d'écran empêche une application de tenter de prendre une capture d'écran ou un enregistrement de l'écran dans le cadre d'une session d'application ou de bureau virtuel. Le logiciel de capture d'écran ne peut pas détecter le contenu dans la zone de capture. La zone sélectionnée par l'application est grisée ou l'application ne capture rien à la place de la section d'écran qu'elle visait. La fonction de prévention de capture d'écran s'applique à
Snip & Sketch, à l'outil Capture d'écran et à la fonction **Maj+Ctrl+Imprimer** sous Windows.

Un autre cas d'utilisation de la prévention de capture d'écran consiste à empêcher le partage de données sensibles dans le cadre d'une réunion virtuelle ou d'applications de conférence Web telles que GoToMeeting, Microsoft Teams ou Zoom. App Protection empêche tout partage involontaire en renvoyant un écran vide lors des conférences Web lorsque les applications sont protégées. Cette fonctionnalité garantit que les données sensibles ne sont pas divulguées accidentellement en dehors de l'organisation. Elle peut contribuer à la conformité dans les secteurs réglementés, car l'intention n'est pas prise en compte lors de la divulgation d'une violation de données.

Les administrateurs peuvent choisir d'activer la prévention de capture d'écran pour les types de ressources suivants :

- Applications et bureaux virtuels
- Applications Web et SaaS internes
- Écrans d'authentification
- Écrans Self-Service Plug-In (SSP)

> **Remarque :**
>
> Si vous avez lancé deux bureaux virtuels et que la fonctionnalité de prévention de capture d'écran est activée sur l'un des bureaux virtuels, mais pas sur l'autre, la fonctionnalité de prévention de capture d'écran s'applique aux deux bureaux virtuels. Vous ne pouvez pas prendre de capture d'écran de l'un ou l'autre des bureaux virtuels.
>
> Si vous avez réduit le bureau virtuel sur lequel la fonction anti-capture d'écran est activée, la fonction est toujours applicable sur l'autre bureau virtuel.

Détection et notification de capture d'écran

Pour l'application Citrix Workspace, vous pouvez afficher une notification lorsqu'une éventuelle tentative de capture d'écran est effectuée sur des ressources protégées. Pour plus d'informations sur les ressources protégées par App Protection, consultez la section [Éléments inclus dans App Protection].(/en-us/citrix-workspace-app/app-protection.html#what-does-app-protection-protect)

La notification apparaît lorsqu'il y a une :

- tentative de capture d'écran ou d'enregistrement de vidéo à l'aide d'un outil de capture d'écran
- tentative de capture d'écran à l'aide de la touche Impression écran

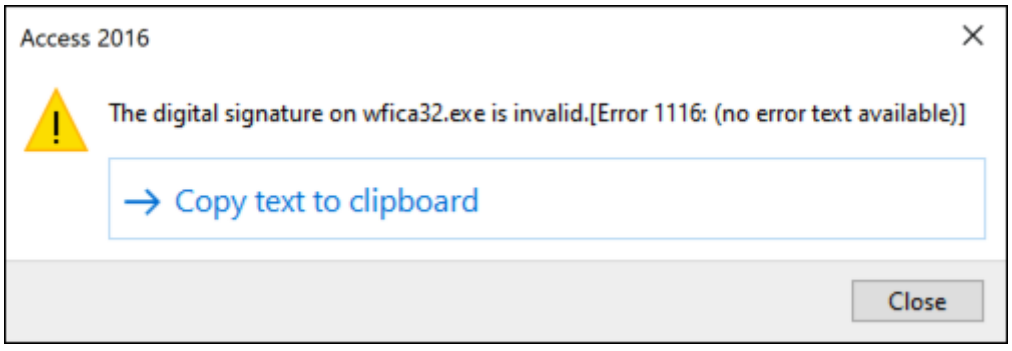
> **Remarque :**
>
> - La notification n'apparaît qu'une seule fois par instance en cours d'exécution de l'outil de capture d'écran. La notification apparaît à nouveau si vous relancez l'outil et que vous essayez de capturer l'écran.
> - Dans l'application Citrix Workspace pour Windows 2212 et versions ultérieures, les fenêtres de connexion et de Self-Service (Store) ne sont pas protégées par défaut.

Protection contre les injections de DLL

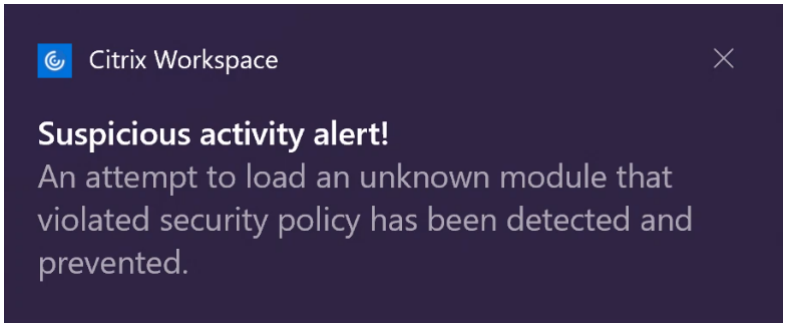
La protection contre les injections de DLL est une amélioration de la sécurité qui permet de protéger l'application Citrix Workspace contre certaines bibliothèques DLL non autorisées ou certains modules non fiables. Si de tels modules non fiables sont injectés, l'application Citrix Workspace détecte ces interventions et arrête le chargement des modules. En outre, si une DLL malveillante ou non fiable est détectée avant le lancement de la session, la protection des applications bloque le lancement de la session et affiche un message d'erreur. La fermeture du message d'erreur entraîne la fermeture de la session d'application et de bureau virtuel.

Cette fonctionnalité s'applique à tous les bureaux et applications virtuels protégés ainsi qu'à la fenêtre d'authentification de l'application Citrix Workspace (déploiement sur site/StoreFront).

Cette amélioration permet de quitter la session immédiatement lorsque certaines DLL non fiables ou malveillantes existent sur le composant protégé.



Cette amélioration affiche une notification lorsqu'une DLL non fiable ou malveillante est bloquée. La fermeture du message entraîne la fermeture de la session d'application et de bureau virtuel.



Clause d'exclusion de responsabilité : cette fonctionnalité opère en filtrant l'accès aux fonctions requises du système d'exploitation sous-jacent (appels d'API spécifiques requis pour charger les DLL). Cela signifie qu'elle peut fournir une protection même contre certains outils de piratage personnalisés et spécifiques. Cependant, à mesure que les systèmes d'exploitation évoluent, de nouvelles méthodes de chargement des DLL peuvent apparaître. Bien que nous continuions à les identifier et à les traiter, nous ne pouvons pas garantir une protection complète dans des configurations et des déploiements spécifiques.

Cette fonctionnalité prend en charge l'application Citrix Workspace pour Windows version 2206 et versions ultérieures.

> **Remarque :**
>
> Auparavant, les fonctionnalités anti-capture d'écran et de protection contre l'enregistrement de frappe étaient appliquées par défaut pour l'authentification Citrix et les écrans de l'application Citrix Workspace. Toutefois, à partir de la version 2212, ces fonctionnalités sont désactivées par défaut et doivent être configurées à l'aide de l'objet de stratégie de groupe. Pour plus d'informations sur la configuration de l'objet de stratégie de groupe, consultez la section Amélioration de la configuration d'App Protection.

Compatibilité avec l'optimisation HDX pour Microsoft Teams

Microsoft Teams optimisé prend en charge le partage d'écran lorsque l'application Citrix Workspace est activée avec App Protection uniquement en mode Desktop Viewer. Lorsque vous cliquez sur **Partager du contenu** dans Microsoft Teams, le sélecteur d'écran propose les options suivantes :

- Option **Fenêtre** permettant de partager n'importe quelle application ouverte. Elle ne s'affiche qu'avec la version 2109 du VDA ou une version ultérieure.
- Option **Bureau** permettant de partager les contenus sur votre bureau VDA : cette option n'est affichée qu'avec les versions suivantes de l'application Citrix Workspace :
  - Application Citrix Workspace pour Linux version 2311 ou ultérieure
  - Application Citrix Workspace pour Mac version 2308 ou ultérieure
  - Application Citrix Workspace pour Windows version 2309 ou ultérieure

Remarque :

Pour l'application Citrix Workspace pour Linux, l'option de partage de bureau est désactivée par défaut. Pour l'activer, ajoutez le paramètre `UseGbufferScreenSharing` dans le fichier *config.json* comme suit :

```
mkdir -p /var/.config/citrix/hdx_rtc_engine
vim /var/.config/citrix/hdx_rtc_engine/config.json
{

      "UseGbufferScreenSharing":1
 }

<!--NeedCopy-->
```

La version optimisée de Microsoft Teams activée avec App Protection prend également en charge la disposition des moniteurs virtuels Citrix, ce qui vous permet de partager chaque moniteur virtuel de manière individuelle.

Limitation :

- La version optimisée de Microsoft Teams activée avec App Protection ne prend pas en charge le partage d'écran sur les bureaux publiés activés avec Local App Access (LAA).
- Le contenu rendu par le client, tel que le contenu du navigateur utilisant le BCR, ne peut être capturé ou partagé. Si vous essayez de faire une capture d'écran, celle-ci s'affiche sous forme d'écran noir.

Remarque :

Avec l'application Citrix Workspace pour Linux et Mac, cette fonctionnalité est en version Technical Preview.

App Protection locale (version préliminaire)

La protection des applications offre une sécurité renforcée pour protéger les clients contre les enregistreurs de frappe et les captures d'écran accidentelles et malveillantes sur les terminaux. Actuellement, les fonctionnalités de protection des applications ne sont proposées que pour les ressources de Workspace. Grâce à cette fonctionnalité, les fonctionnalités de protection des applications sont étendues aux applications locales sur les terminaux. À partir de l'application Citrix Workspace 2210 pour Windows, la protection des applications peut être appliquée aux applications locales sur les appareils Windows.

Inscrivez-vous à la version préliminaire de cette fonctionnalité en utilisant le formulaire Podio.

Détection d'altération des stratégies

La fonction de détection d'altération des stratégies empêche l'utilisateur d'accéder à la session d'application ou de bureau virtuel si les stratégies de prévention de capture d'écran et de protection contre l'enregistrement de frappe d'App Protection sont altérées. Si une altération des stratégies est détectée, la session d'application ou de bureau virtuel est interrompue.

> **Remarque :**
>
> La fonctionnalité de détection d'altération des stratégies sera activée par défaut dans une prochaine version.

Pour configurer la détection d'altération des stratégies, consultez Configurer la détection d'altération des stratégies.

Vérification de l'état

Pour détecter et bloquer le lancement d'applications et de bureaux virtuels dotés de stratégies App Protection à partir de versions de l'application Citrix Workspace qui ne prennent pas en charge la fonctionnalité de détection d'altération des stratégies, activez le paramètre Vérification de l'état d'App Protection.

> **Remarque :**
>
> Si la vérification de l'état est activée et que vous utilisez la version de l'application Citrix Workspace qui ne prend pas en charge la vérification de l'état, les sessions dotées de stratégies d'App Protection sont interrompues.

Pour configurer la vérification de l'état, consultez Configurer la vérification de l'état.

> **Limitation :**
>
> La vérification de l'état cesse de fonctionner par intermittence lorsque vous utilisez des VDA Windows Workstation hébergés sur Microsoft Azure avec un VDA 2308. Cette limitation est résolue dans les versions 2311 et ultérieures du VDA.

App Protection avec le scénario double saut (DoubleHop)

Les fonctionnalités de protection des applications ne sont pas prises en charge dans un scénario double saut (DoubleHop) Le double saut (ou « DoubleHop ») désigne une session Citrix Virtual Apps ou Virtual Desktops exécutée dans le cadre d'une session Citrix Virtual Desktops. Vous avez été autorisé à lancer des applications et des bureaux virtuels dotés de stratégies App Protection dans un scénario DoubleHop, mais les fonctionnalités d'App Protection n'ont pas été appliquées.

À partir de la version 2309 de l'application Citrix Workspace pour Windows, une stratégie de groupe Windows est introduite et vous permet de bloquer le lancement d'applications et de bureaux virtuels dotés de stratégies App Protection dans un scénario DoubleHop. Pour en savoir plus sur l'activation du paramètre **Bloquer le lancement de DoubleHop**, consultez la section Activer le paramètre Bloquer le lancement de DoubleHop.

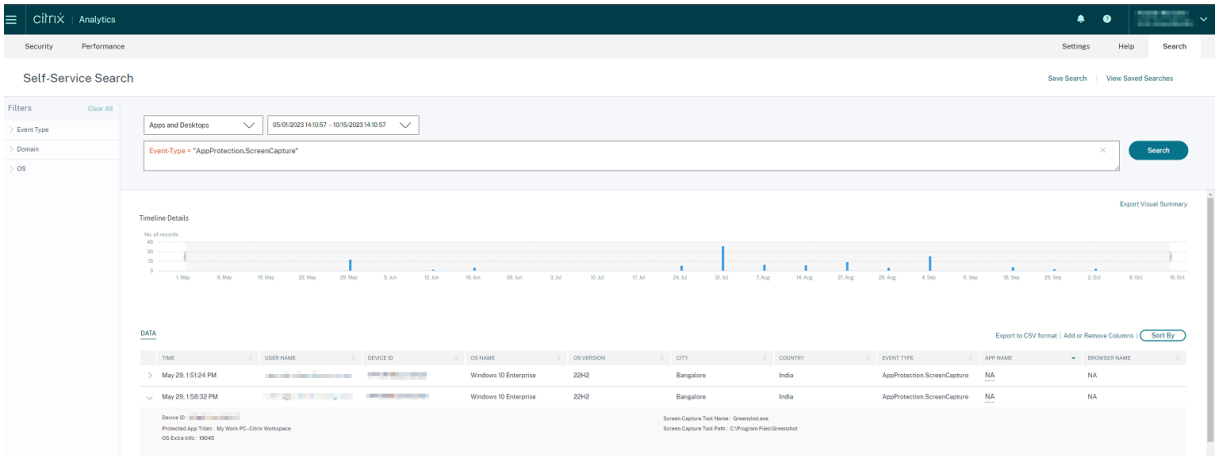
Citrix Analytics Service pour App Protection

Lorsque vous utilisez Citrix Virtual Apps and Desktops, des événements utilisateur correspondant à leurs activités et actions sont générés. Citrix Analytics for Security dispose d'une fonctionnalité nommée **Recherche en libre-service** qui enregistre ces événements utilisateur et vous fournit des informations à leur sujet. La fonctionnalité de **Recherche en libre-service** vous permet de rechercher, de filtrer et de consulter ces événements utilisateur afin de comprendre lequel est effectué et de prendre des mesures en fonction de sa gravité. Pour en savoir plus sur la **Recherche en libre-service**, voir Recherche en libre-service.

La fonctionnalité **Recherche en libre-service pour applications et bureaux** comporte le type d'événement `AppProtection.ScreenCapture`, qui vous permet de déterminer si des tentatives ont été faites pour prendre des captures d'écran des applications et bureaux virtuels dotés de stratégies App Protection. Pour en savoir plus sur la façon de rechercher un événement utilisateur, voir Spécifier une recherche pour filtrer les événements.

Ce service propose les informations suivantes :

- ID de l'appareil
- Titres d'applications protégés
- Informations supplémentaires sur le système d'exploitation
- Nom de l'outil de capture d'écran
- Chemin d'accès de l'outil de capture d'écran



Liste verte des captures d'écran

Si l'application Citrix Workspace, Citrix Virtual Apps and Desktops ou les applications SaaS sont activés avec la stratégie de prévention des captures d'écran App Protection, vous ne pouvez pas capturer leurs écrans à l'aide d'un outil de capture d'écran.

Toutefois, à partir de la version 2402 de l'application Citrix Workspace pour Windows, la fonctionnalité Liste verte des captures d'écran vous permet d'ajouter une application à la liste verte de captures d'écran. Cette fonctionnalité vous permet d'utiliser l'application inscrite sur la liste verte et de capturer l'écran de la ressource activée avec la stratégie de prévention des captures d'écran App Protection. Pour ajouter une application à la liste verte de capture d'écran, consultez Configuration de la liste verte de capture d'écran.

> **Important :**
>
> Il n'est pas recommandé d'exécuter une application sur liste verte sur votre appareil pendant une période prolongée, car cela réduit le niveau de sécurité. Vous pouvez utiliser les applications sur liste verte pour partager temporairement votre écran lors de scénarios tels que la résolution de problèmes. Il est recommandé de respecter les conditions suivantes :
>
> - Exécutez l'application sur liste verte pendant une courte période en activant la fonction anti-capture d'écran App Protection sur la ressource.
> - Une fois la tâche requise terminée, fermez immédiatement l'application sur liste verte.
> - Pour plus de sécurité lors du partage d'un écran tout en utilisant la ressource avec la fonction anti-capture d'écran App Protection activée, ajoutez un filigrane.

Liste d'exclusion des processus

Lorsque vous lancez un processus ou une application sur votre appareil, des DLL App Protection sont injectées dans chaque processus si l'App Protection est activée. Parfois, cela peut empêcher le processus ou l'application de fonctionner en raison de problèmes de compatibilité avec la DLL.

À partir de la version 2402 de l'application Citrix Workspace pour Windows, vous pouvez ajouter n'importe quel processus à la liste d'exclusion des processus afin d'éviter l'injection de la DLL App Protection dans ce processus particulier et de résoudre les problèmes de compatibilité causés par la présence de DLL App Protection. Pour configurer la liste d'exclusion des processus, consultez Configuration de la liste d'exclusion des processus.

> **Important :**
>
> l'exclusion de processus n'est pas recommandée, car cela réduit la posture de sécurité. Vous pouvez l'utiliser pour débloquer temporairement l'utilisation de l'application et créer un ticket d'assistance pour une étude plus approfondie.

Liste d'exclusion des pilotes de filtre USB

Parfois, lorsque vous utilisez des claviers externes spécialisés tels que des claviers de gaming avec l'application Citrix Workspace, le pilote de filtre USB App Protection peut entraîner des problèmes de compatibilité et vous empêcher d'utiliser le clavier.

À partir de la version 2402 de l'application Citrix Workspace pour Windows, la fonctionnalité Liste d'exclusion des pilotes de filtre USB vous permet d'exclure tout périphérique USB présentant des problèmes de compatibilité avec l'application Citrix Workspace à l'aide de l'ID fournisseur et de l'ID produit de l'appareil. Pour ajouter un périphérique à la liste d'exclusion des pilotes de filtre USB, consultez Configuration de la liste d'exclusion des pilotes de filtre USB.

> **Remarque :**
>
> l'exclusion définitive de périphériques n'est pas recommandée. Utilisez cette fonctionnalité pour empêcher temporairement l'utilisateur d'utiliser le périphérique et créez un ticket d'assistance afin d'étudier le problème de compatibilité de manière plus approfondie.

Configurer la protection des applications

April 10, 2024

La protection des applications renforce la sécurité lorsque vous utilisez l'application Citrix Workspace. Cette fonctionnalité limite la capacité des clients à être compromis par des logiciels malveillants d'enregistrement de touches et de capture d'écran. La protection des applications empêche l'exfiltration d'informations confidentielles telles que les informations d'identification de l'utilisateur et les informations sensibles affichées à l'écran. Cette fonctionnalité empêche les utilisateurs et les attaquants de prendre des captures d'écran et d'utiliser des enregistreurs de frappe pour récupérer et exploiter des informations sensibles.

Cet article explique comment configurer la protection des applications sur l'application Citrix Workspace sur différentes plateformes.

La protection des applications est disponible sur l'application Citrix Workspace pour les plateformes suivantes :

- Application Citrix Workspace pour Windows
- Application Citrix Workspace pour Linux
- Application Citrix Workspace pour Mac

> **Clause d'exclusion de responsabilité**
>
> Les stratégies App Protection filtrent l'accès aux fonctions requises du système d'exploitation sous-jacent. Les appels d'API spécifiques sont nécessaires pour capturer des écrans ou des frappes de clavier. Les stratégies App Protection fournissent une protection même contre les outils de piratage personnalisés et spécifiques. Cependant, à mesure que les systèmes d'exploitation évoluent, de nouveaux programmes d'enregistrement de frappe et de capture d'écran peuvent émerger. Bien que nous continuions à les identifier et à les traiter, nous ne pouvons pas garantir une protection complète dans des configurations et des déploiements spécifiques.

Application Citrix Workspace pour Windows

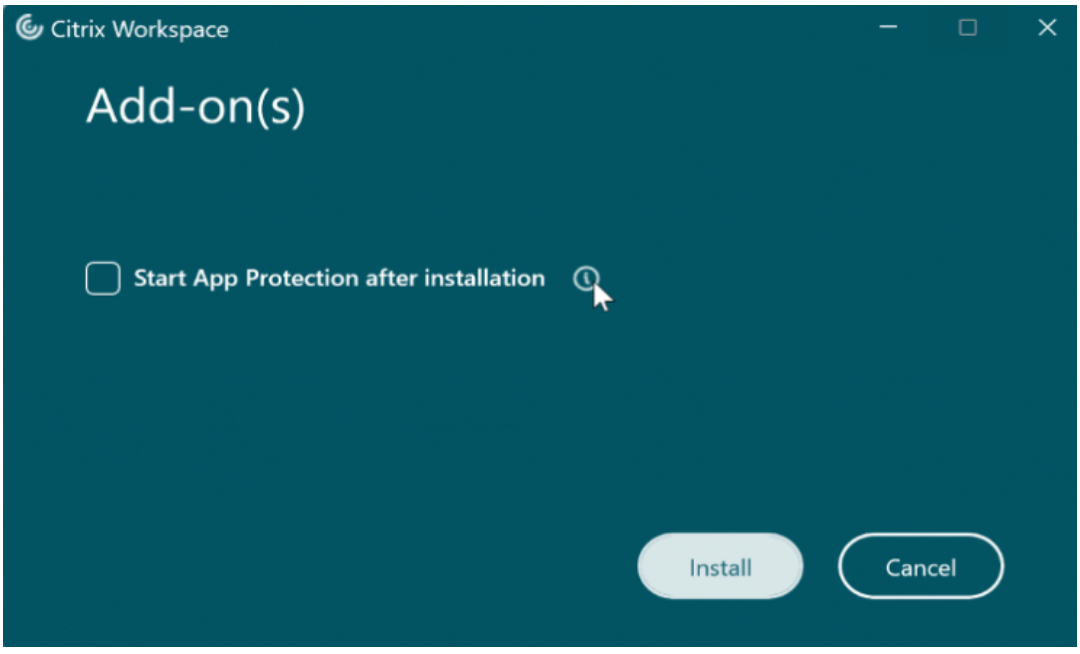
Pré-requis

- Citrix Virtual Apps and Desktops 1912 LTSR ou versions ultérieures.
- StoreFront version 1912 LTSR ou Workspace.
- Application Citrix Workspace version 2203.1 LTSR ou versions ultérieures.
- Une licence Protection des applications valide
- À partir de la version 2212 de l'application Citrix Workspace, le composant App Protection est installé par défaut lors de l'installation de l'application Citrix Workspace.

  La case à cocher **Activer App Protection** qui apparaît lors de l'installation est remplacée par **Démarrer App Protection après l'installation**.

  - Pour les versions de l'application Citrix Workspace antérieures à la version 2311 :

– À partir de la version 2311 de l'application Citrix Workspace :



Lorsque vous cochez cette case, la fonctionnalité App Protection démarre immédiatement après l'installation.

> **Remarque :**
>
> Si vous ne cochez pas cette case, la fonctionnalité App Protection démarre automatiquement dès le premier démarrage d'une ressource ou d'un composant protégé pour les clients ayant droit à la protection des applications.

Configurer

Configurez les fonctionnalités App Protection suivantes pour l'application Citrix Workspace pour Windows :

- **Protection contre l'enregistrement de frappe et prévention des captures d'écran :**
  - Pour Virtual Apps and Desktops, consultez la section Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications et les bureaux virtuels.
  - Pour les applications Web et SaaS, consultez la section Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications Web et SaaS.
  - Pour l'authentification et Self-Service Plug-in :
    - Si vous utilisez l'interface utilisateur Global App Configuration Service, consultez la section Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour l'authentification et Self-Service Plug-in à l'aide de l'interface utilisateur Global App Configuration Service
    - Si vous utilisez un objet de stratégie de groupe, consultez la section Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour l'authentification et Self-Service Plug-in à l'aide d'un objet de stratégie de groupe
    - Si vous utilisez l'API, consultez la section Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour l'authentification et Self-Service Plug-in à l'aide de l'API GACS
- Pour configurer la protection contre les injections de DLL, consultez l'article Configurer la protection contre les injections de DLL.
- Pour configurer la détection d'altération des stratégies App Protection, consultez l'article Configurer la détection d'altération des stratégies de protection des applications.
- Pour configurer la vérification de l'état de la fonctionnalité App Protection, consultez l'article Configurer la vérification de l'état d'App Protection.
- Pour activer le paramètre Bloquer le lancement de DoubleHop, consultez la section Bloquer le lancement de DoubleHop.

Limitations

- Cette fonctionnalité est prise en charge uniquement sur les systèmes d'exploitation de bureau tels que Windows 11 et Windows 10.
- À partir de la version 2006.1, l'application Citrix Workspace n'est plus prise en charge sous Windows 7. La protection des applications ne fonctionne donc pas sous Windows 7. Pour plus d'informations, consultez Fin de prise en charge.
- Cette fonctionnalité n'est pas prise en charge par le protocole RDP (Remote Desktop Protocol).

Interface de ligne de commande

Vous pouvez démarrer le composant Protection des applications à l'aide du paramètre de ligne de commande /`startappprotection`. Cependant, l'ancien commutateur /`includeappprotection` est obsolète.

Le tableau suivant fournit des informations sur les écrans protégés en fonction du déploiement :

Déploiement d'App Protection	Écrans protégés	Écrans non protégés
Inclus dans l'application Citrix Workspace	Boîte de dialogue Self-Service Plug-in et Authentication Manager/Informations d'identification utilisateur	Centre de connexion, Appareils, messages d'erreur liés à l'application Citrix Workspace, Reconnexion automatique des clients, Ajouter un compte
Configuré sur le Controller	Écran de session ICA (applications et bureaux)	Centre de connexion, Appareils, messages d'erreur liés à l'application Citrix Workspace, Reconnexion automatique des clients, Ajouter un compte

Lorsque vous prenez une capture d'écran, seule la fenêtre protégée est occultée. Vous pouvez prendre une capture d'écran de la zone à l'extérieur de la fenêtre protégée. Toutefois, si vous utilisez la touche **Impr écran** pour réaliser une capture d'écran sur une machine Windows 10, vous devez réduire la fenêtre protégée.

Auparavant, les fonctionnalités anti-capture d'écran et de protection contre l'enregistrement de frappe étaient appliquées par défaut pour l'authentification Citrix et les écrans de l'application Citrix Workspace. Toutefois, à partir de la version 2212, ces fonctionnalités sont désactivées par défaut et doivent être configurées à l'aide de l'objet de stratégie de groupe.

> **Remarque :**
>
> Cette stratégie d'objet de stratégie de groupe ne s'applique pas aux sessions ICA et SaaS. Les sessions ICA et SaaS continuent d'être contrôlées à l'aide du Delivery Controller et de Citrix Secure Private Access.

Amélioration d'App Protection :

À compter de l'application Citrix Workspace pour Windows 2305 et versions ultérieures, la protection contre l'enregistrement de frappe est activée sur les écrans d'authentification et du Self-Service Plug-in si l'un des critères suivants est rempli :

- Vous avez activé la App Protection à l'aide de l'une des méthodes suivantes :
  - En sélectionnant la case **Démarrer la App Protection** lors de l'installation.
  - En démarrant le composant App Protection à l'aide du paramètre de ligne de commande **/startappprotection**.
- Si vous n'avez pas sélectionné la case **Démarrer App Protection** ou si vous n'avez pas utilisé le paramètre de ligne de commande **/startappprotection** lors de l'installation, la protection contre l'enregistrement de frappe est activée après le lancement de la première ressource protégée.

> **Remarque :**
>
> Les paramètres Global App Configuration Service et des objets de stratégie de groupe remplacent le comportement précédent. Par exemple, si vous avez désactivé la stratégie GACS ou GPO pour ces écrans, la protection contre l'enregistrement de frappe n'est pas activée sur les écrans d'authentification et du SSP.

Application Citrix Workspace pour Linux

Depuis la version 2108, la fonction App Protection est entièrement fonctionnelle. Cette fonctionnalité prend en charge Virtual Apps and Desktops et elle est activée par défaut. Toutefois, vous devez configurer la fonctionnalité Protection des applications dans le fichier `AuthManConfig.xml` pour l'activer dans les interfaces Authentication Manager et Self-Service Plug-in.

Conditions préalables

La fonctionnalité App Protection fonctionne mieux avec les systèmes d'exploitation suivants, ainsi qu'avec Gnome Display Manager :

- Ubuntu 22.04, Ubuntu 20.04 et Ubuntu 18.04 64 bits

- Debian 10 et Debian 9 64 bits
- CentOS 7 64 bits
- RHEL 7 64 bits
- Système d'exploitation Raspberry Pi 32 bits ARMHF (basé sur Debian 10 (Buster))
- Système d'exploitation ARM64 Raspberry Pi (basé sur Debian 11 (bullseye))

> **Remarque :**
>
> Si vous utilisez l'application Citrix Workspace antérieure à la version 2204, la fonctionnalité App Protection ne prend pas en charge les systèmes d'exploitation utilisant la version `glibc` 2.34 ou ultérieure.
>
> Si vous installez l'application Citrix Workspace avec la fonctionnalité App Protection activée sur le système d'exploitation utilisant la bibliothèque `glibc` 2.34 ou une version ultérieure, le démarrage du système d'exploitation peut échouer lors du redémarrage du système. Pour activer la récupération après l'échec de démarrage du système d'exploitation, effectuez l'une des opérations suivantes :
>
> - Réinstallez le système d'exploitation.
> - Accédez au mode Récupération du système d'exploitation et désinstallez l'application Citrix Workspace à l'aide du terminal.
> - Démarrez via le système d'exploitation actif et supprimez le fichier `rm -rf /etc/ld.so.preload` du système d'exploitation existant.

Installer le composant Protection des applications

1. Lorsque vous installez l'application Citrix Workspace à l'aide du package tarball, le message suivant s'affiche : **Voulez-vous installer le composant Protection des applications ? Avertissement : vous ne pouvez pas désactiver cette fonctionnalité. Pour désactiver cette fonctionnalité, vous devez désinstaller l'application Citrix Workspace. Pour plus d'informations, contactez votre administrateur système. [default $INSTALLER_N]:**
2. Entrez **Y** pour installer le composant App Protection. La protection des applications n'est pas installée par défaut.
3. Redémarrez votre ordinateur pour que les modifications soient prises en compte. La protection des applications fonctionne comme prévu uniquement après le redémarrage de votre machine.

Installation du composant Protection des applications sur les packages RPM À partir de la version 2104, le composant App Protection est pris en charge sur la version RPM de l'application Citrix Workspace.

Pour installer le composant App Protection, procédez comme suit :

1. Installez l'application Citrix Workspace.
2. Installez le package App Protection `ctxappprotection<version>.rpm` à partir du programme d'installation de l'application Citrix Workspace.
3. Redémarrez le système pour que les modifications soient prises en compte.

Installation du composant Protection des applications sur les packages Debian À partir de la version 2101, le composant App Protection est pris en charge sur la version Debian de l'application Citrix Workspace.

Pour installer le composant Protection des applications, exécutez la commande suivante à partir du terminal avant d'installer l'application Citrix Workspace :

```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select yes"

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

sudo apt install -f ./icaclient_<version>._amd64.deb
<!--NeedCopy-->
```

À compter de la version 2106, l'application Citrix Workspace introduit une option qui permet de configurer séparément les fonctionnalités de protection contre les programmes d'enregistrement de frappe et de capture d'écran pour les interfaces Authentication Manager et Self-Service Plug-in.

Configurer

Configurez les fonctionnalités App Protection suivantes pour l'application Citrix Workspace pour Linux :

- Pour configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour l'écran d'authentification, consultez la section Configurer à l'aide du fichier AuthManConfig.xml pour le gestionnaire d'authentification.
- Pour configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour Self-Service Plug-in, consultez la section Configurer à l'aide du fichier AuthManConfig.xml pour l'interface de Self-Service Plug-in.
- Pour configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications et les bureaux virtuels, consultez la section Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications et les bureaux virtuels.
- Pour configurer la détection d'altération des stratégies App Protection, consultez l'article Configurer la détection d'altération des stratégies de protection des applications.

- Pour configurer la vérification de l'état de la fonctionnalité App Protection, consultez l'article Configurer la vérification de l'état d'App Protection.

Application Citrix Workspace pour Mac

Configurez les fonctionnalités App Protection suivantes pour l'application Citrix Workspace pour Mac :

- Pour configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour l'authentification et Self-Service Plug-in à l'aide de l'interface utilisateur du service Global App Configuration, consultez la section Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour l'authentification et Self-Service Plug-in à l'aide de l'interface utilisateur du service Global App Configuration.
- Pour configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour l'authentification et Self-Service Plug-in à l'aide de l'API, consultez la section Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour l'authentification et Self-Service Plug-in à l'aide de l'API GACS.
- Pour configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications et les bureaux virtuels, consultez la section Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications et les bureaux virtuels.
- Pour configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications Web et SaaS, consultez la section Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications Web et SaaS.
- Pour configurer la détection d'altération des stratégies App Protection, consultez l'article Configurer la détection d'altération des stratégies de protection des applications.
- Pour configurer la vérification de l'état de la fonctionnalité App Protection, consultez l'article Configurer la vérification de l'état d'App Protection.

Conseil

Les stratégies de protection des applications sont principalement axées sur l'amélioration de la sécurité et de la protection d'un point de terminaison. Passez en revue toutes les autres recommandations et stratégies de sécurité pour votre environnement. Vous pouvez utiliser un modèle de stratégie **Sécurité et contrôle** pour une configuration recommandée dans des environnements à faible tolérance au risque. Pour plus d'informations, veuillez consulter la section Modèles de stratégie.

Configuration de la protection contre l'enregistrement de frappe et de la prévention des captures d'écran

April 10, 2024

Vous pouvez configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les écrans suivants :

- Authentification et Self-Service Plug-in
- Virtual Apps and Desktops
- Applications Web et SaaS

Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour l'authentification et Self-Service Plug-in

Vous pouvez configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour l'authentification et pour Self-Service Plug-in à l'aide des méthodes suivantes :

Méthode de configuration	Application Citrix Workspace pour Linux	Application Citrix Workspace pour Mac	Application Citrix Workspace pour Windows
Utilisation de l'objet de stratégie de groupe	Non	Non	Oui
Utilisation de Global App Configuration Service	Non	Oui	Oui
Utilisation du fichier AuthManConfig.xml	Oui	Non	Non

Utilisation de l'objet de stratégie de groupe

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant `gpedit.msc`.
2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace**.
3. Selon que vous configurez App Protection pour Authentication Manager ou Self-Service Plug-in, procédez de l'une des manières suivantes :

- **Authentication Manager**

  Pour configurer les fonctionnalités de protection contre les programmes d'enregistrement de frappe et de capture d'écran pour le gestionnaire d'authentification, sélectionnez la stratégie **Authentification utilisateur** > **Gérer App Protection**.

- **Interface de Self-Service Plug-in**

  Pour configurer les fonctionnalités de protection contre les programmes d'enregistrement de frappe et de capture d'écran pour l'interface du Self-Service Plug-in, sélectionnez **Self Service** > **Gérer la protection des applications**.

4. Sélectionnez l'une ou les deux options suivantes :

   - **Protection contre l'enregistrement de frappe** : empêche les keyloggers de capturer les frappes
   - **Protection contre la capture d'écran** : empêche les utilisateurs de prendre des captures d'écran et de partager leur écran.

5. Cliquez sur **Appliquer** et **OK**.

Comportement attendu :

Le comportement attendu dépend de la façon dont les utilisateurs accèdent au magasin StoreFront qui contient des ressources protégées.

Utilisation de l'interface utilisateur de Global App Configuration Service

À compter de la version 2302 ou 2301 de l'application Citrix Workspace pour Windows, l'application Citrix Workspace vous permet de configurer App Protection pour les écrans d'authentification et Self-Service Plug-In à l'aide du service GACS (Global App Configuration Service).

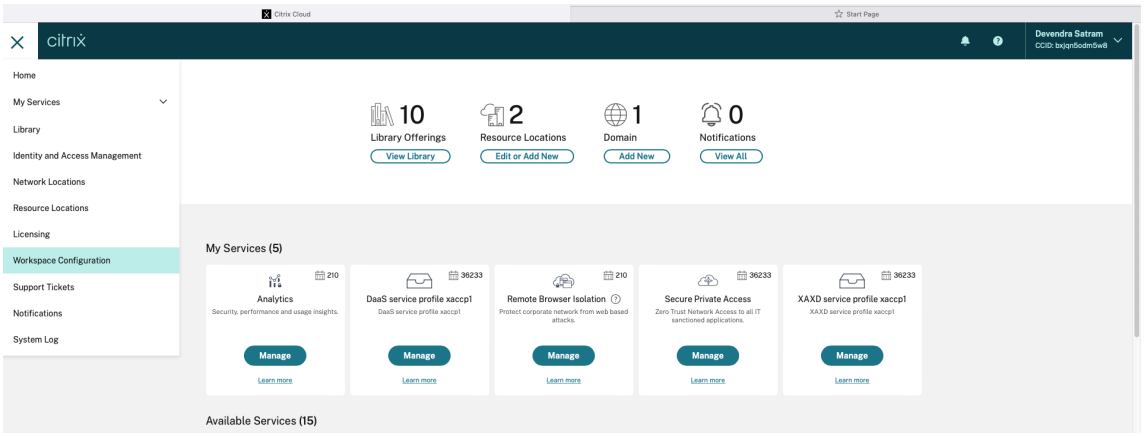
Si vous activez les fonctionnalités de protection contre l'enregistrement de frappe et de prévention des captures d'écran à l'aide du service GACS, elles s'appliquent à la fois aux écrans d'authentification et de plug-in en libre-service.

> **Remarque :**
>
> - La configuration de la protection contre l'enregistrement de frappe et de la prévention des captures d'écran pour l'authentification et Self-Service Plug-In à l'aide du service GACS s'applique aux applications Citrix Workspace pour Windows et Citrix Workspace pour Mac. Elle ne s'applique pas à l'application Citrix Workspace pour Linux.
> - Les configurations GACS ne s'appliquent pas aux applications et bureaux virtuels, ni aux applications Web et SaaS. Ces ressources continuent d'être contrôlées à l'aide du Delivery Controller et de Citrix Secure Private Access.
> - À compter de la version 2311 de l'application Citrix Workspace pour Mac, vous pouvez

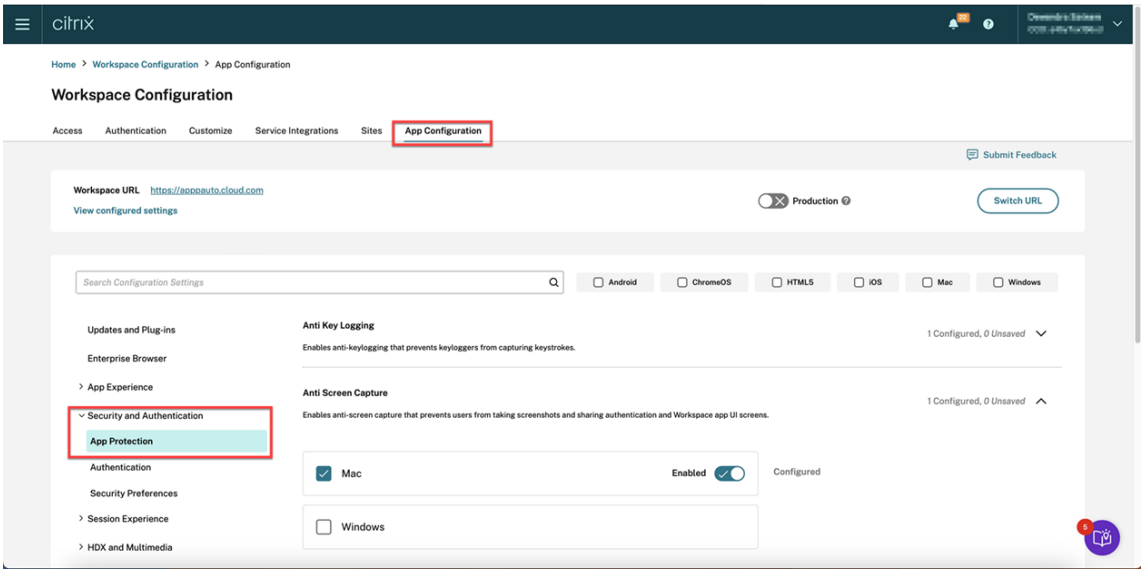
> configurer App Protection pour l'authentification et Self-Service Plug-in à l'aide de l'interface utilisateur GACS (Global App Configuration Service) pour les magasins cloud et locaux. Toutefois, si vous utilisez une version de l'application Citrix Workspace pour Mac antérieure à la version 2311, vous ne pouvez la configurer que pour les magasins cloud.

Les administrateurs peuvent configurer la App Protection à l'aide de l'interface utilisateur de configuration de Workspace :

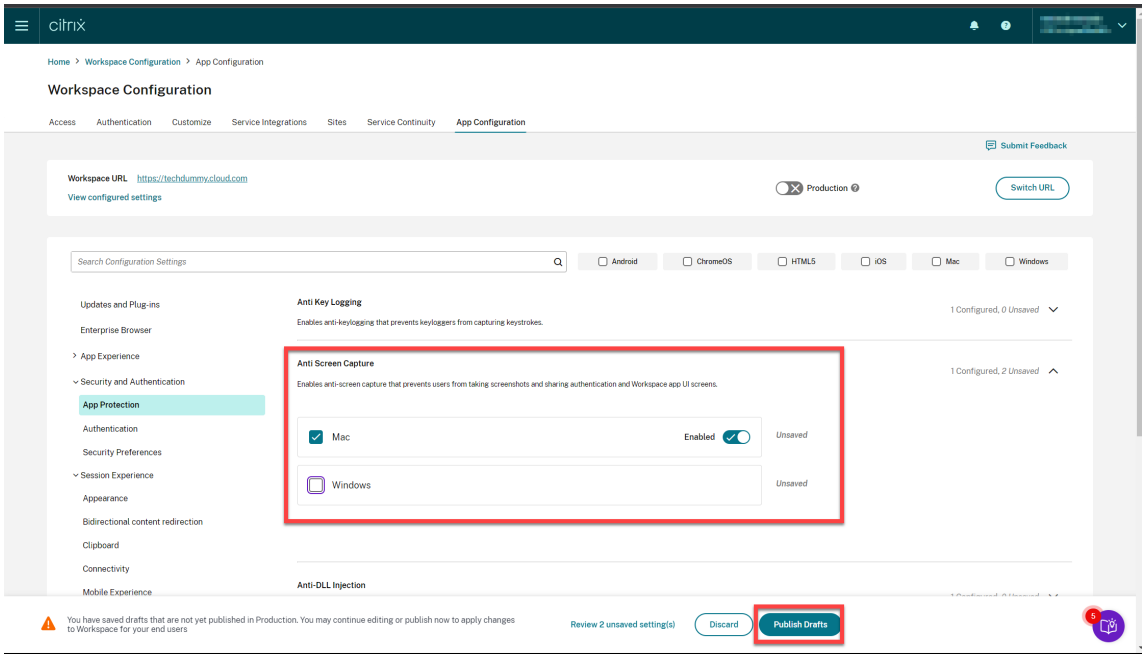
1. Connectez-vous à votre compte Citrix Cloud et sélectionnez **Configuration de l'espace de travail**.



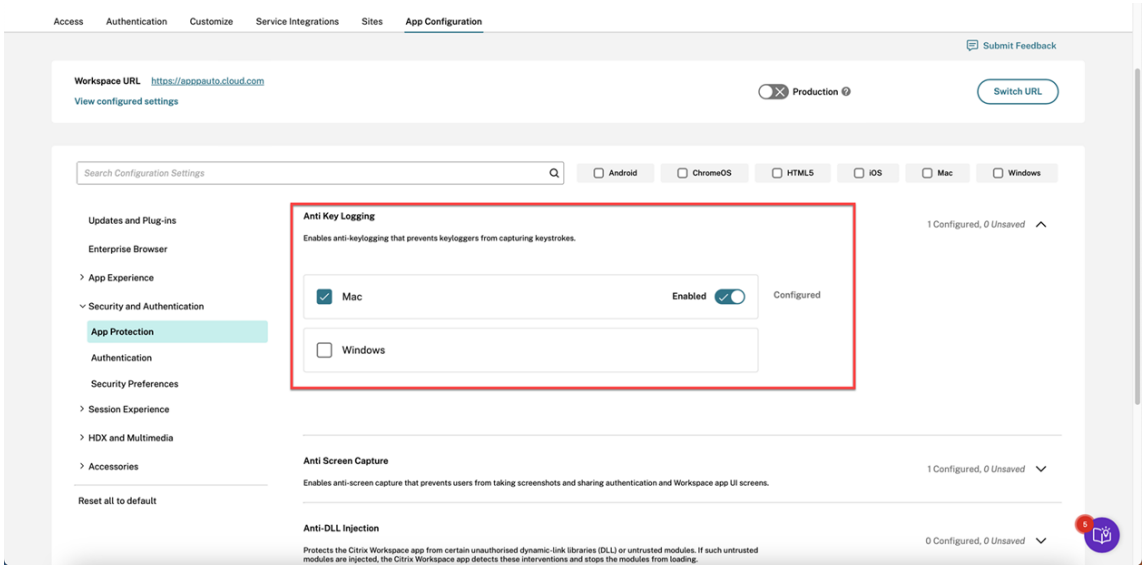
2. Sélectionnez **Configuration de l'application** > **Sécurité et authentification** > **App Protection**.



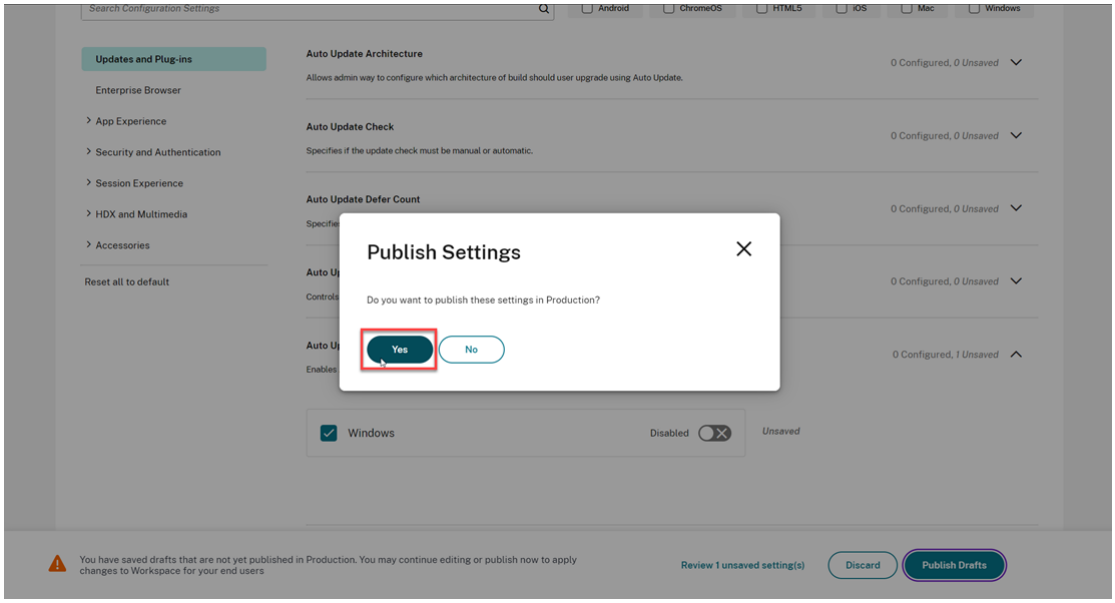
3. Cliquez sur **Prévention des captures d'écran**, puis sélectionnez le système d'exploitation approprié (Windows ou Mac).
4. Cliquez sur le bouton **Activé**, puis sur **Publier les brouillons**.



5. Cliquez sur **Protection contre l'enregistremen de frappe**, puis sélectionnez le système d'exploitation approprié (Windows ou Mac).
6. Cliquez sur le bouton **Activé**, puis sur **Publier les brouillons**.



7. Dans la boîte de dialogue **Paramètres de publication**, cliquez sur **Oui**.



Utilisation de l'API Global App Configuration Service

Les administrateurs peuvent utiliser l'API pour configurer ces fonctionnalités de App Protection. Les paramètres sont les suivants :

- **Paramètre permettant d'activer ou de désactiver la protection contre la capture d'écran :**

  "name": "enable anti screen capture for auth and ssp"
  "value": "true"ou "false"

- **Paramètre permettant d'activer ou de désactiver la protection contre l'enregistrement de frappe :**

  "name": "enable anti key-logging for auth and ssp"
  "value": "true"ou "false"

Exemple : le fichier JSON suivant illustre comment activer les fonctionnalités de prévention des captures d'écran et de protection contre l'enregistrement de frappe pour l'application Citrix Workspace pour Windows dans GACS :

```
{

        "category": "App Protection",

        "userOverride": true,

        "assignedTo": [

          "AllUsersNoAuthentication"
```



```
11
12            ],
13
14            "settings": [
15
16              {
17
18
19                "name": "enable anti screen capture for auth and ssp",
20
21                "value": true
22
23               }
24  ,
25
26              {
27
28
29                "name": "enable anti key-logging for auth and ssp",
30
31                "value": true
32
33               }
34
35
36            ] }
```

Utilisation du fichier AuthManConfig.xml pour Authentication Manager

Accédez au fichier `$ICAROOT/config/AuthManConfig.xml` et modifiez-le comme suit :

```
1 /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
     authmananti -A 1
2     <key>AuthManAntiScreenCaptureEnabled</key>
3     <value>true</value>
4     <key>AuthManAntiKeyLoggingEnabled</key>
5     <value>true </value>
6
7 <!--NeedCopy-->
```

Utilisation du fichier AuthManConfig.xml pour l'interface de Self-Service Plug-in

Accédez au fichier `$ICAROOT/config/AuthManConfig.xml` et modifiez-le comme suit :

```
1 /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
     protection -A 4
2 <!-- Selfservice App Protection configuration -->
3     <Selfservice>
4       <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
```



```
        <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
    </Selfservice>

<!--NeedCopy-->
```

Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications et les bureaux virtuels

Deux stratégies offrent des fonctionnalités de protection contre l'enregistrement de frappe et de prévention des captures d'écran dans une session. Vous pouvez configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications et les bureaux virtuels comme suit :

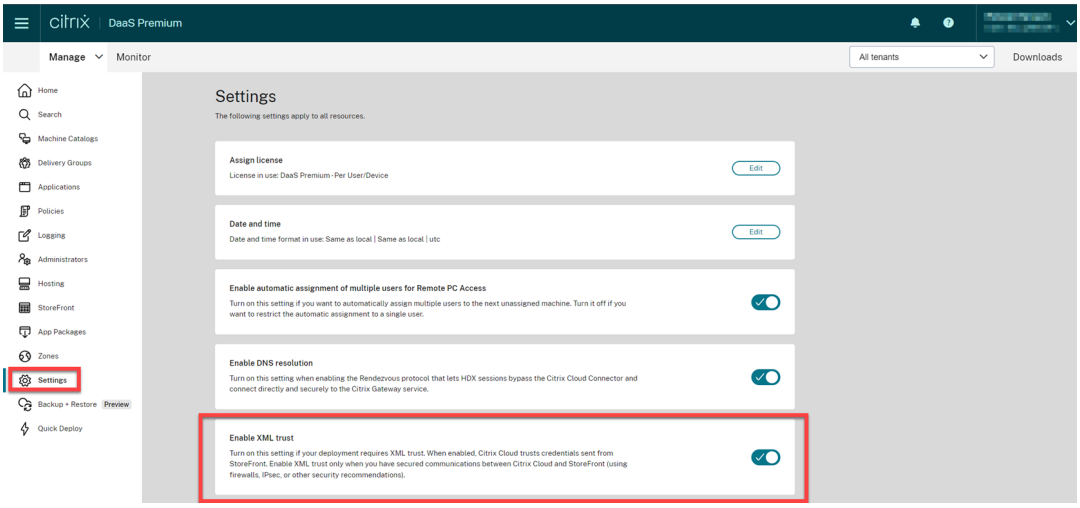
> **Remarque :**
>
> À compter de la version 2103, Citrix DaaS prend en charge la App Protection avec StoreFront et Workspace.

Utilisation de Web Studio

Pour configurer la protection contre l'enregistrement de frappe et la capture d'écran pour Citrix Virtual Apps or Desktops via Web Studio, procédez comme suit :

1. App Protection nécessite une approbation XML. Pour activer l'approbation XML, procédez comme suit :

    a) Connectez-vous à votre compte Citrix DaaS et cliquez sur **Gérer** > **Paramètres** > **Activer l'approbation XML**.

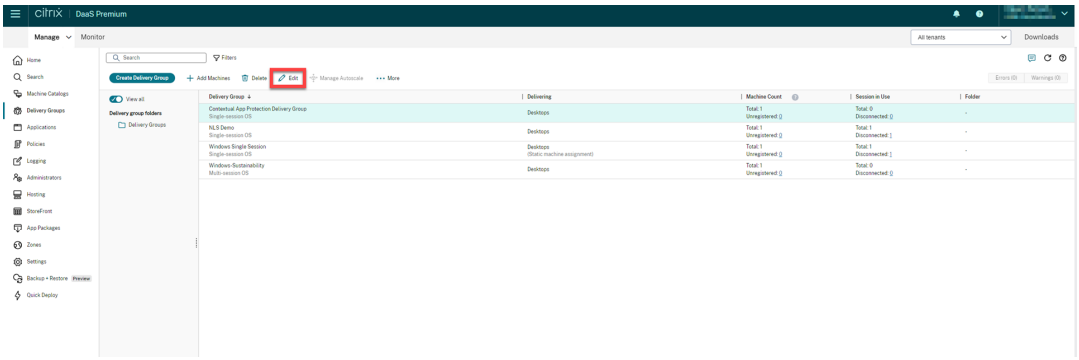


    b) Activez le bouton **Activer l'approbation XML**.

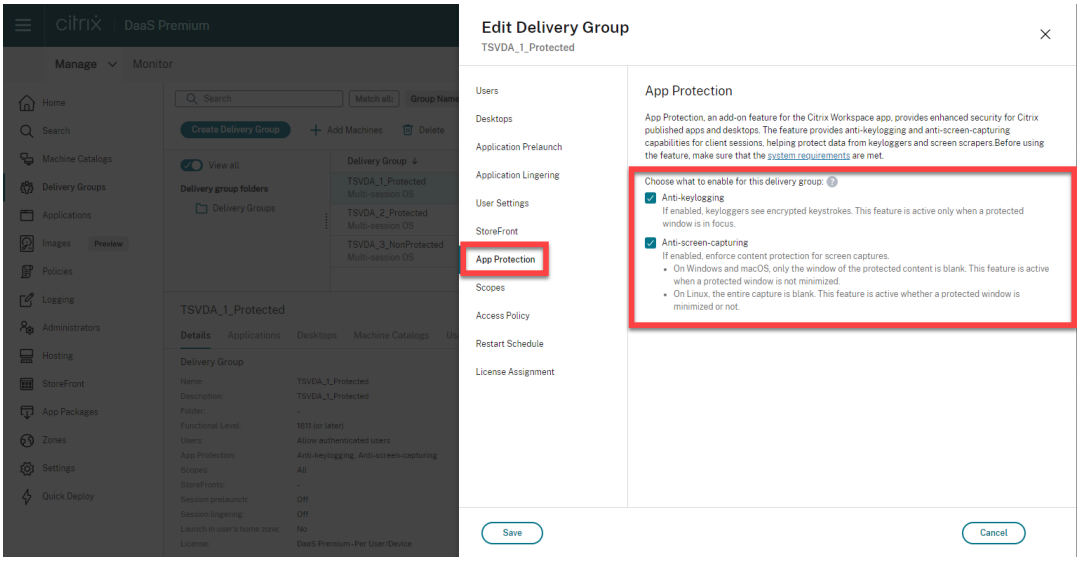
2. Pour choisir une méthode d'App Protection pour un groupe de mise à disposition, procédez comme suit :

   a) Dans Citrix DaaS, cliquez sur **Gérer** > **Groupes de mise à disposition**.

   b) Sélectionnez un groupe de mise à disposition, puis cliquez sur **Modifier** dans la barre d'actions.



   c) Cliquez sur **App Protection**, puis cochez les cases **Protection contre l'enregistrement de frappe** et **Protection contre la capture d'écran**.



   d) Cliquez sur **Enregistrer**.

Utilisation de PowerShell

> **Remarque :**
>
> Dans un environnement Citrix DaaS, utilisez les applets de commande dans le Kit de développement logiciel distant SDK Citrix Virtual Apps and Desktops Remote PowerShell sur n'importe

> quelle machine (à l'exception des machines Citrix Cloud Connector) pour émettre les commandes de cette section.

Activez les propriétés suivantes pour le groupe de mise à disposition doté d'App Protection à l'aide du SDK Citrix Virtual Apps and Desktops sur n'importe quelle machine Delivery Controller ou sur une machine avec un composant Studio autonome sur laquelle les composants logiciels enfichables FMA PowerShell sont installés.

- `AppProtectionKeyLoggingRequired : True`
- `AppProtectionScreenCaptureRequired : True`

Vous pouvez activer chacune de ces stratégies individuellement par groupe de mise à disposition. Par exemple, vous pouvez configurer la protection contre l'enregistrement de frappe uniquement pour le groupe de mise à disposition DG1, et la protection contre l'enregistrement de capture d'écran uniquement pour le groupe de mise à disposition DG2. Vous pouvez activer les deux stratégies pour le groupe de mise à disposition DG3.

Exemple :

Pour activer les deux stratégies pour un groupe de mise à disposition nommé **DG3**, exécutez la commande suivante sur n'importe quel composant Delivery Controller du site :

```
Set-BrokerDesktopGroup -Name DG3 -AppProtectionKeyLoggingRequired
$true -AppProtectionScreenCaptureRequired $true
```

Pour valider les paramètres, exécutez cette applet de commande :

```
Get-BrokerDesktopGroup -Property Name, AppProtectionKeyLoggingRequired
, AppProtectionScreenCaptureRequired | Format-Table -AutoSize
```

Activez également l'approbation XML :

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

Assurez-vous de sécuriser le réseau entre StoreFront et le broker. Pour plus d'informations, consultez les articles CTX236929 et Sécurisation du service XML XenApp et XenDesktop du centre de connaissances.

Configurer la protection contre l'enregistrement de frappe et la prévention des captures d'écran pour les applications Web et SaaS

Les applications Web et SaaS s'ouvrent dans les applications Citrix Enterprise Browser pour Citrix Workspace pour Windows et Citrix Workspace pour Mac. Si les applications sont configurées pour bénéficier des stratégies App Protection via Citrix Secure Private Access, App Protection est appliqué par onglet.

Configurez App Protection pour les applications Web et SaaS à l'aide des méthodes suivantes :

- Pour configurer App Protection pour les applications Web et SaaS pour Workspace, consultez l'article Citrix Secure Private Access pour Citrix Workspace.
- Pour configurer App Protection pour les applications Web et SaaS pour StoreFront, consultez l'article Prise en charge de Citrix Secure Private Access pour StoreFront.

Configurer la protection contre les injections de DLL

March 11, 2024

Par défaut, la fonctionnalité de protection contre les injections de DLL est désactivée. Vous pouvez l'activer à l'aide des méthodes suivantes :

- Objet de stratégie de groupe (GPO)
- Global App Configuration Service (GACS)

Configurer à l'aide d'un objet de stratégie de groupe

Les stratégies suivantes sont ajoutées pour configurer la protection contre les injections de DLL :

- Protection contre les injections de DLL
- Liste verte des modules de protection contre l'injection de DLL

Utilisation de la stratégie de protection contre les injections de DLL

Utilisez cette stratégie pour activer ou désactiver la protection contre les injections de DLL. Si cette stratégie n'est pas configurée, la protection contre les injections de DLL est désactivée. Les valeurs possibles sont les suivantes :

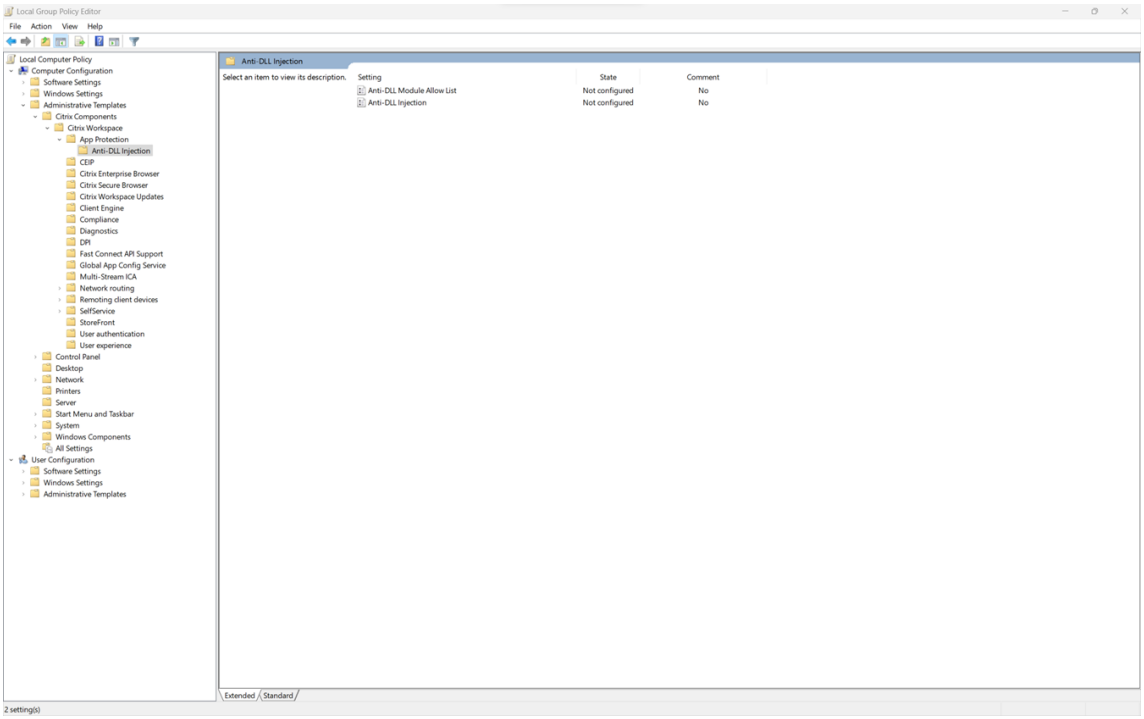
- **Activé** –La protection contre les injections de DLL est activée pour Citrix Authentication Manager, l'interface utilisateur de l'application Citrix Workspace et pour Citrix Virtual Apps and Desktops. Les administrateurs peuvent sélectionner les composants requis pour activer la protection contre les injections de DLL.
- **Désactivé** –La protection contre les injections de DLL est désactivée pour Citrix Authentication Manager, l'interface utilisateur de l'application Citrix Workspace et pour Citrix Virtual Apps and Desktops.

Pour activer la stratégie de protection contre les injections de DLL, procédez comme suit :

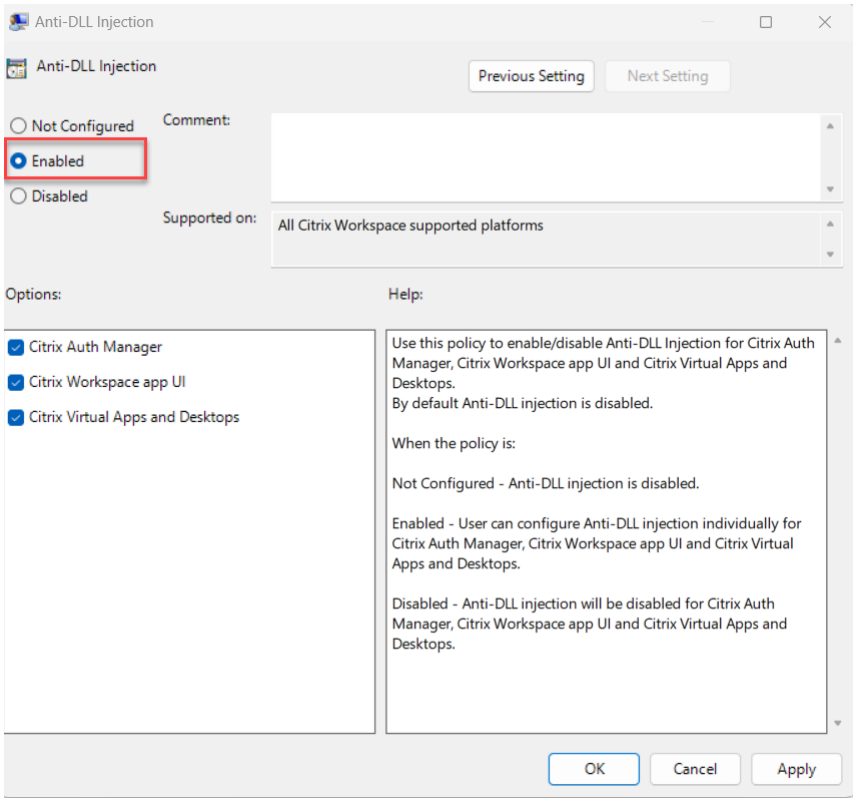
1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant la commande suivante :


```
gpedit.msc
```

2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **App Protection** > **Protection contre les injections de DLL**.



3. Cliquez sur la stratégie **Protection contre les injections de DLL** et sélectionnez **Activé**. Tous les composants sont sélectionnés. Vous pouvez toutefois modifier la sélection des composants dans la section Options.



4. Cliquez sur **OK**.

Utilisation de la stratégie de liste verte des modules de protection contre les injections de DLL

En tant qu'administrateur, vous pouvez utiliser cette stratégie pour exclure toute DLL de la protection contre les injections de DLL. Citrix vous recommande de n'utiliser cette stratégie que pour gérer tout scénario exceptionnel. Lorsque cette stratégie n'est pas configurée, aucune DLL ne fait partie de la liste d'autorisation. Toutes les DLL sont incluses dans la fonction de protection contre les injections de DLL. Les valeurs possibles sont les suivantes :

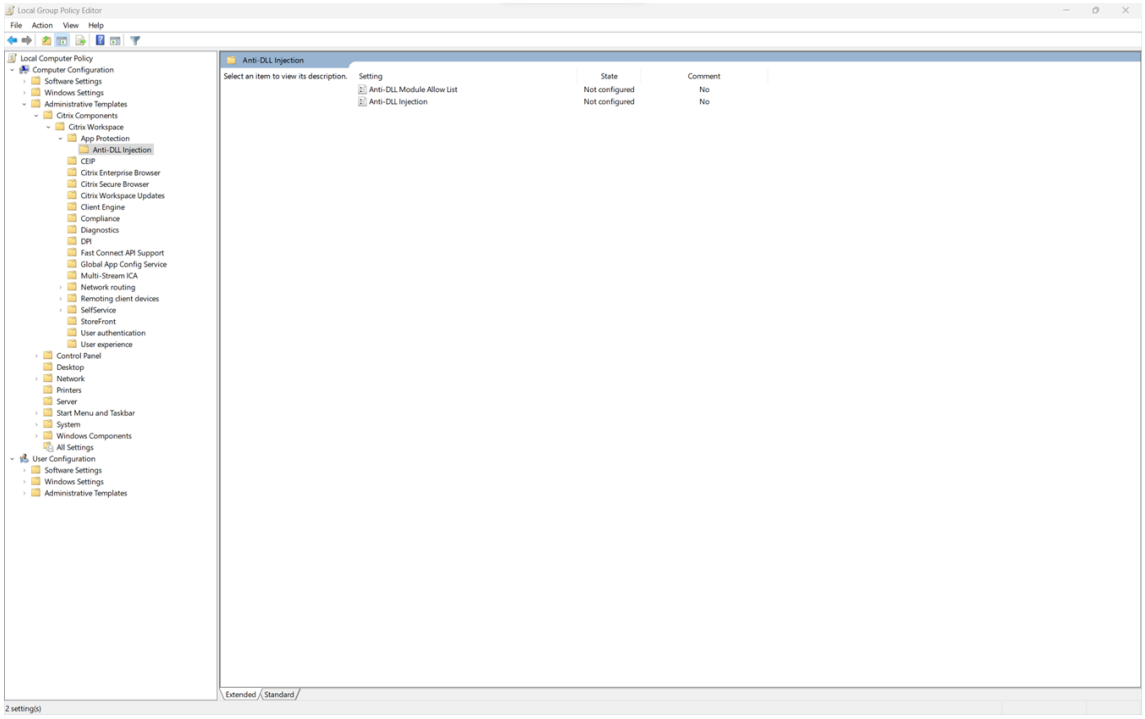
- **Activé** - Exclut toutes les DLL ajoutées à la liste verte de la protection contre les injections de DLL.
- **Désactivé** - Efface les DLL ajoutées à la liste verte.

Pour activer la stratégie de liste verte du module de protection contre les injections de DLL, procédez comme suit :

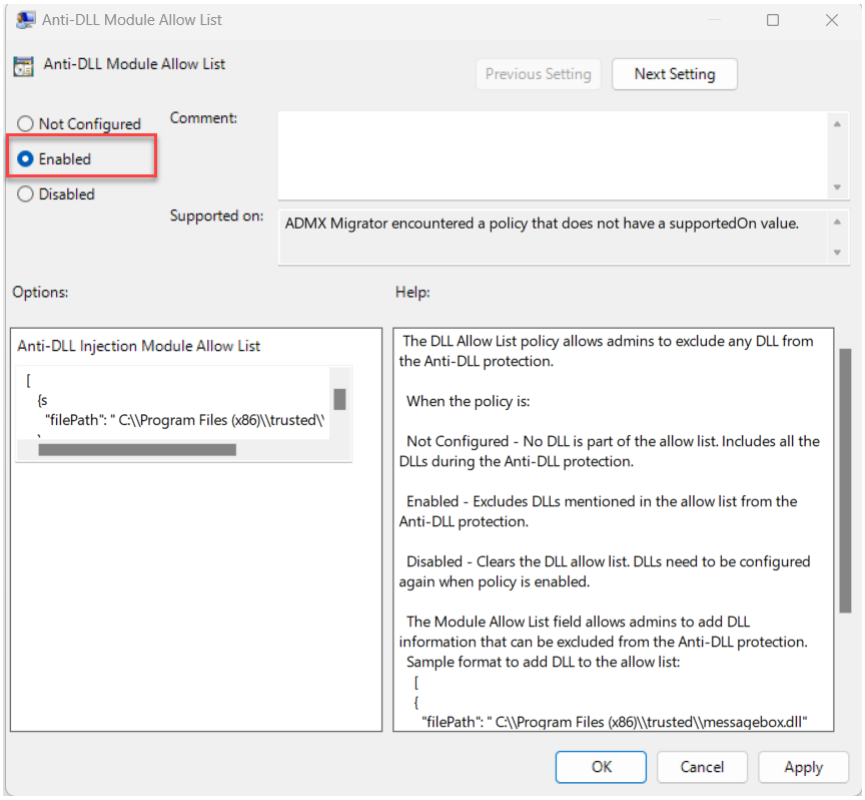
1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant la commande suivante :

   ```
   gpedit.msc
   ```

2. Sous le nœud **Configuration ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **App Protection** > **Liste des modules d'injection de DLL autorisés**.



3. Cliquez sur la stratégie **Liste verte des modules de protection contre les injections de DLL** et sélectionnez **Activé**.



4. Ajoutez la liste des modules que vous souhaitez exclure de la protection contre les injections de DLL dans le champ **Liste des modules d'injection de DLL autorisés**.

Exemple de format pour ajouter une DLL à la liste d'autorisation :

```
[
    {

        "filePath":"C:\Program Files (x86)\trusted\messagebox.dll"
     }
 ,
    {

        "filePath":"%PROGRAMFILES%\trusted\logging.dll"
     }

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

5. Cliquez sur **OK**.

Configurer à l'aide de Global App Configuration Service

Les administrateurs peuvent configurer la protection contre les injections de DLL à l'aide du service GACS. Les paramètres sont les suivants :

- Protection contre les injections de DLL : permet d'ajouter les modules requis pour activer la fonction de protection contre les injections de DLL.
- Liste des modules d'injection de DLL autorisés : permet d'ajouter les DLL requises que vous souhaitez exclure de la protection contre les injections de DLL

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

Le fichier suivant est un exemple de fichier JSON permettant d'activer la **protection contre les injections de DLL** et la **liste verte des modules de protection contre les injections de DLL** pour l'application Citrix Workspace exécutée sous Windows dans GACS :

```
{

  "serviceURL": {

    "url": "https://tuleshtest.cloudburrito.com:443"
   }
 ,
  "settings": {

    "appSettings": {

      "windows": [
        {

          "category": "App Protection",
          "userOverride": false,
```



```
            "assignedTo": [
              "AllUsersNoAuthentication"
            ],
            "assignmentPriority": 0,
            "settings": [
              {

                "name": "anti dll injection",
                "value": [
                  "Citrix Auth Manager",
                  "Citrix Virtual Apps And Desktops",
                  "Citrix Workspace app UI"
                ]
               }
  ,
              {

                "name": "anti dll module allow list",
                "value": [
                  {

                    "filePath": "C:\Program Files (x86)\Citrix\ICA Client
                       \wfica32.exe"
                   }
  ,
                  {

                    "filePath": "C:\Program Files (x86)\Citrix\ICA Client
                       \AuthManager\AuthManSvr.exe"
                   }

                ]
               }

           ]
          }

       ]
     }
  ,
     "name": "name",
     "description": "desc",
     "useForAppConfig": true
    }

  }

<!--NeedCopy-->
```


Configurer la détection d'altération des stratégies

March 11, 2024

Logiciels requis

Pour configurer la fonctionnalité de détection d'altération des stratégies, assurez-vous que vous disposez des éléments suivants :

- Pour les déploiements dans le cloud : Cloud Desktop Delivery Controller version 115 ou version ultérieure
- Pour les déploiements sur site : Citrix Virtual Apps and Desktops version 2308 ou ultérieure
- Windows Virtual Delivery Agent, version 2308 ou ultérieure
- Pour Windows : application Citrix Workspace pour Windows version 2309 ou ultérieure
- Pour Mac : application Citrix Workspace pour Mac version 2308 ou ultérieure
- Pour Linux : application Citrix Workspace pour Linux version 2308 ou ultérieure

Pour activer la détection d'altération des stratégies, l'administrateur doit démarrer le **service de protection des applications Citrix** sur les VDA TS/WS qui hébergent les applications et les bureaux virtuels configurés avec App Protection.

Effectuez l'une des étapes suivantes pour activer la détection d'altération des stratégies :

- Utilisation de l'invite de commande :

  1. Dans la partie la plus à gauche de la barre des tâches, cliquez sur l'icône **Rechercher** . Entrez **cmd**, puis cliquez sur **Exécuter en tant qu'administrateur**. L'écran d'**invite de commande** apparaît.
  2. Exécutez les commandes suivantes :

     ```
     sc config ctxappprotectionsvc start=auto
     sc start ctxappprotectionsvc

     <!--NeedCopy-->
     ```

- Utilisation de l'interface utilisateur :

  1. Dans la partie la plus à gauche de la barre des tâches, cliquez sur l'icône **Rechercher** . Entrez **services.msc** et appuyez sur **Entrée**. L'écran **Services** apparaît.
  2. Sélectionnez **Service de protection des applications Citrix**, puis cliquez sur **Démarrer**.
  3. Cliquez avec le bouton droit sur **Service Citrix App Protection**, puis sélectionnez **Propriétés**.

4. Sélectionnez **Général** > **Type de démarrage** > **Automatique**, puis cliquez sur **OK** pour vous assurer que le service démarre automatiquement au démarrage du système.

La fonction de détection d'altération des stratégies est correctement activée.

Pour détecter et bloquer les versions antérieures de l'application Citrix Workspace qui ne prennent pas en charge la détection d'altération des stratégies, configurez le paramètre Vérification de l'état d'App Protection. Pour plus d'informations sur ce paramètre, consultez Vérification de l'état d'App Protection.

Configurer la vérification de la posture d'App Protection

March 11, 2024

Pour activer la vérification de l'état de App Protection, configurez la nouvelle stratégie du VDA Citrix associé à cette fonctionnalité.

Logiciels requis

Assurez-vous que vous disposez des éléments suivants :

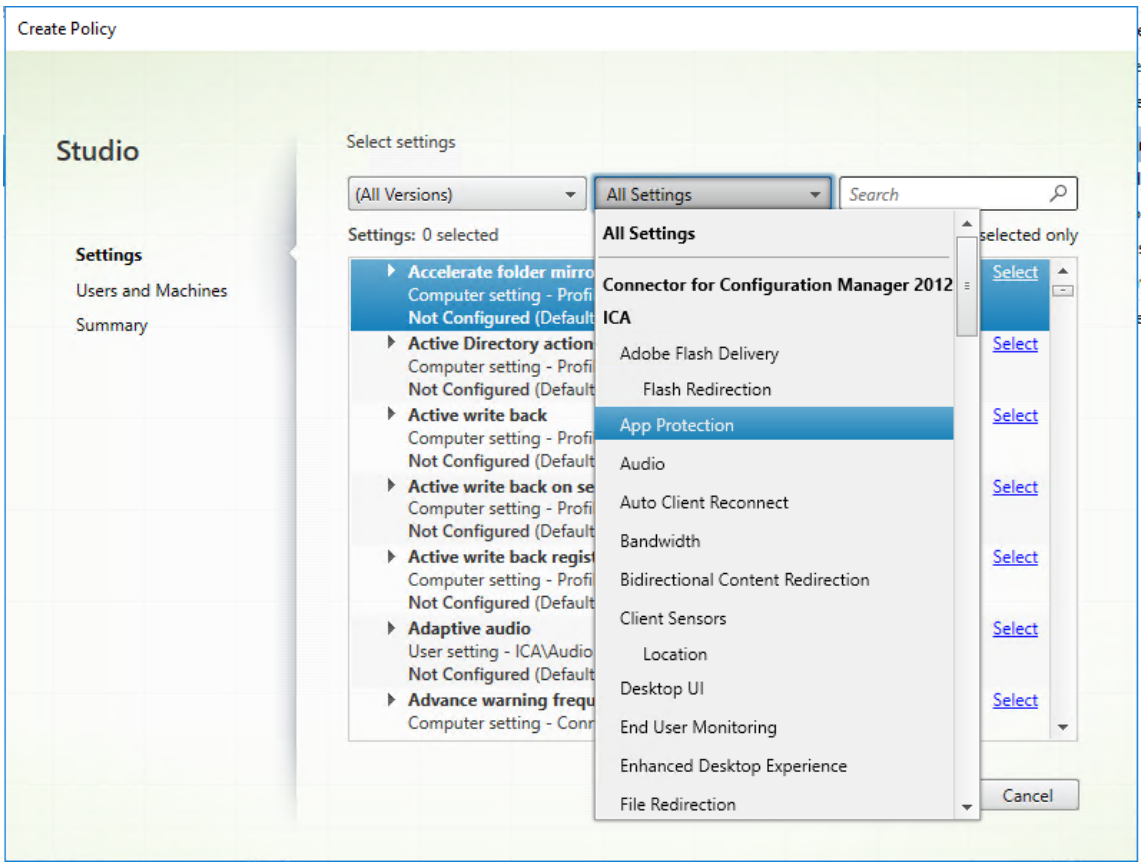
- Pour les déploiements dans le cloud : Cloud Desktop Delivery Controller version 115 ou version ultérieure
- Pour les déploiements sur site : Citrix Virtual Apps and Desktops version 2308 ou ultérieure
- Windows Virtual Delivery Agent, version 2308 ou ultérieure
- Pour Windows : application Citrix Workspace pour Windows version 2309 ou ultérieure
- Pour Mac : application Citrix Workspace pour Mac version 2308 ou ultérieure
- Pour Linux : application Citrix Workspace pour Linux version 2308 ou ultérieure

Configurez la nouvelle stratégie du VDA Citrix pour la fonctionnalité de vérification de l'état comme suit :

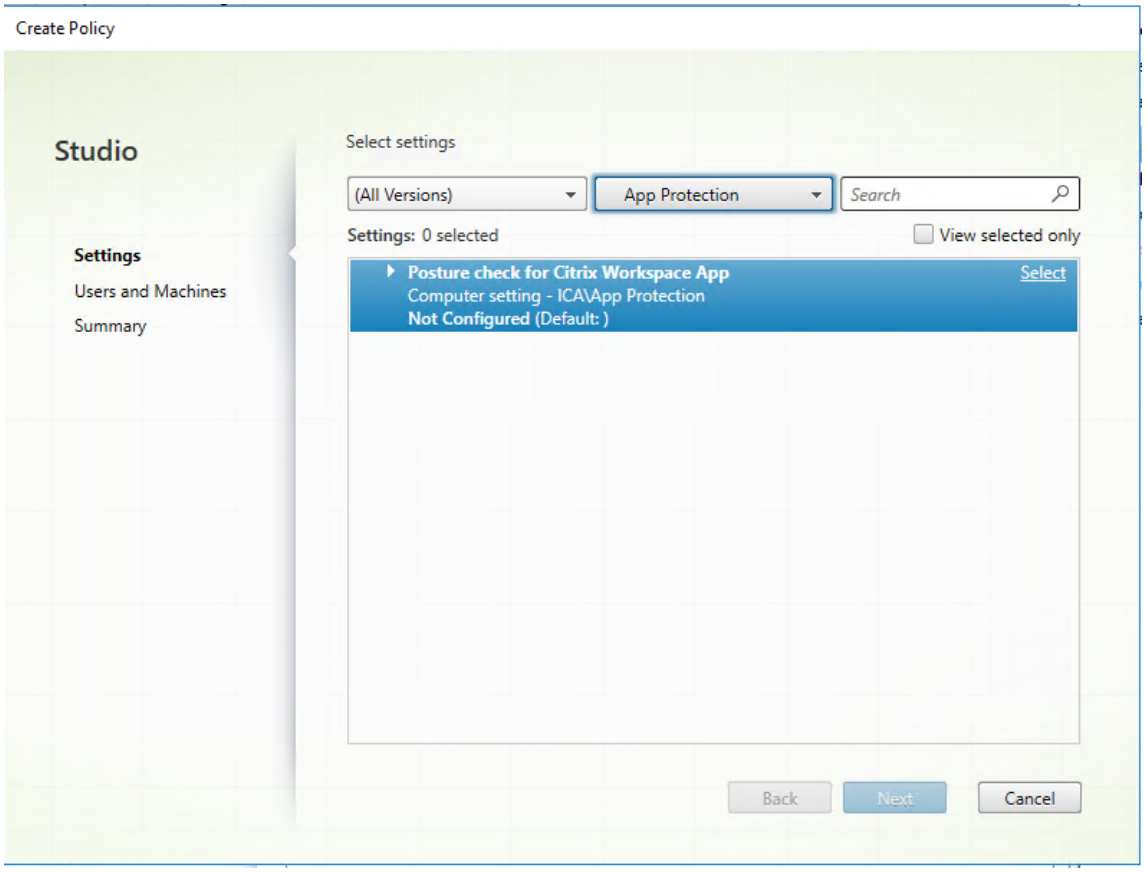
> **Remarque :**
>
> Cette nouvelle stratégie du VDA Citrix peut être déployée à la fois à l'aide de Citrix Studio et de Web Studio. La procédure suivante s'effectue via Citrix Studio ; vous pouvez également utiliser la même procédure pour Web Studio.

1. Ouvrez l'application Citrix Studio sur Desktop Delivery Controller (DDC) pour les déploiements sur site ou Web Studio pour les déploiements dans le cloud, puis sélectionnez **Stratégies**.
2. Sous **Actions**, sélectionnez **Stratégies** > **Créer une stratégie**.

3. Cliquez sur le menu déroulant **Tous les paramètres**, puis sélectionnez **App Protection** sous **ICA**.



4. Sélectionnez **Vérification de l'état de l'application Citrix Workspace**, puis cliquez sur **Sélectionner**.

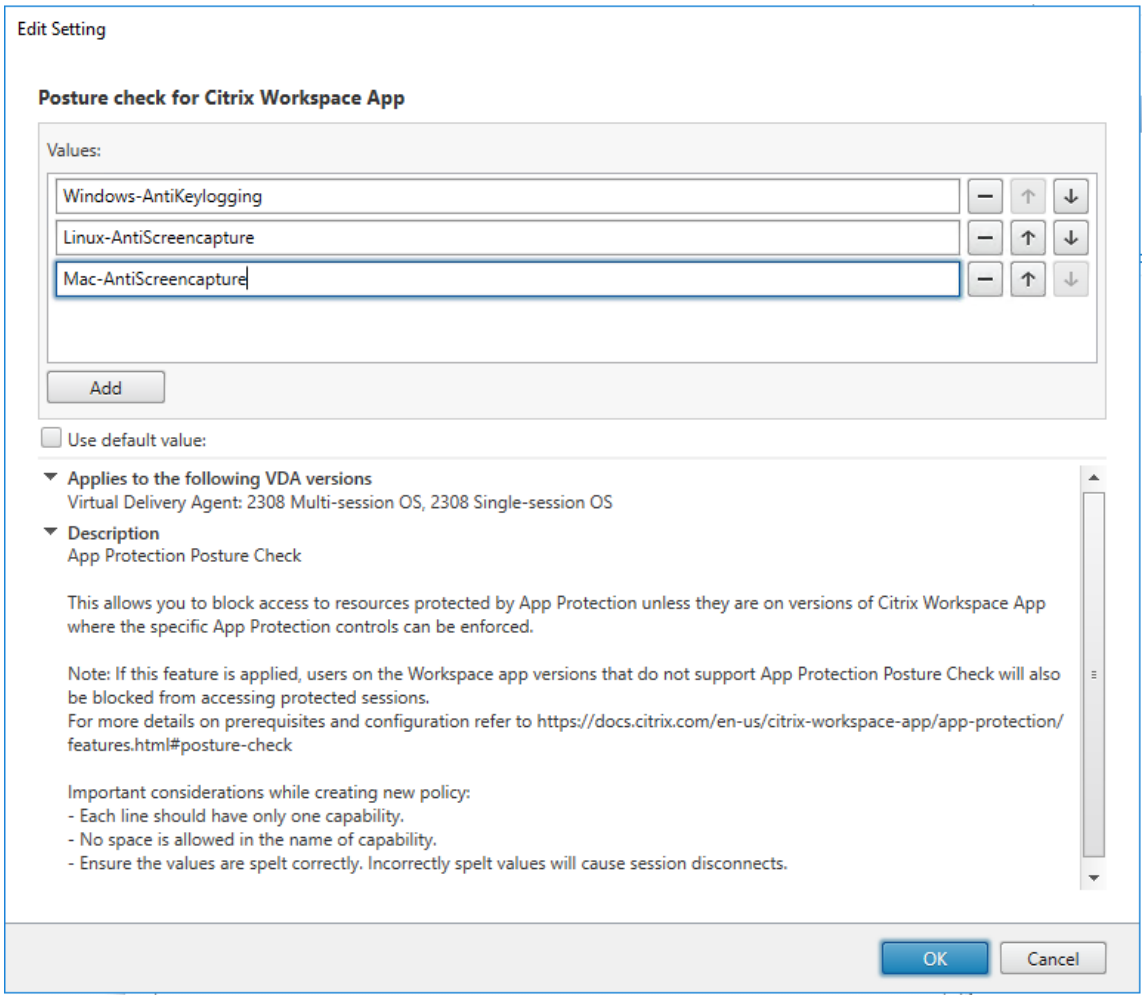


La fenêtre **Modifier le paramètre** s'affiche.

5. Décochez la case **Utiliser la valeur par défaut**.
6. Cliquez sur **Ajouter** et entrez les valeurs appropriées parmi les suivantes :

   - Windows-AntiScreencapture
   - Windows-AntiKeylogging
   - Linux-AntiScreencapture
   - Linux-AntiKeylogging
   - Mac-AntiScreencapture
   - Mac-AntiKeylogging

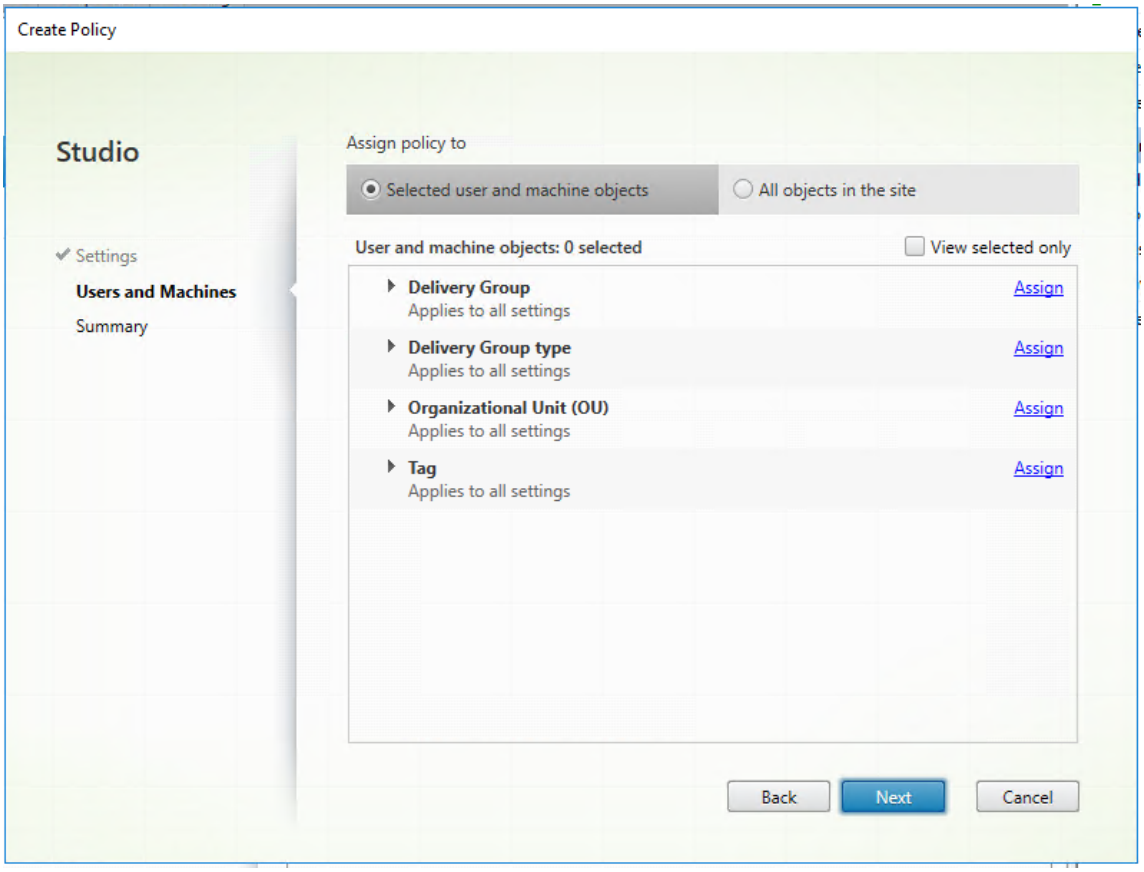
   Par exemple, si vous avez ajouté « Windows-AntiScreencapture » et « Windows-AntiKeylogging », l'application Citrix Workspace pour Windows qui prend en charge la vérification de l'état et possède ces fonctionnalités est autorisée à se connecter au VDA.



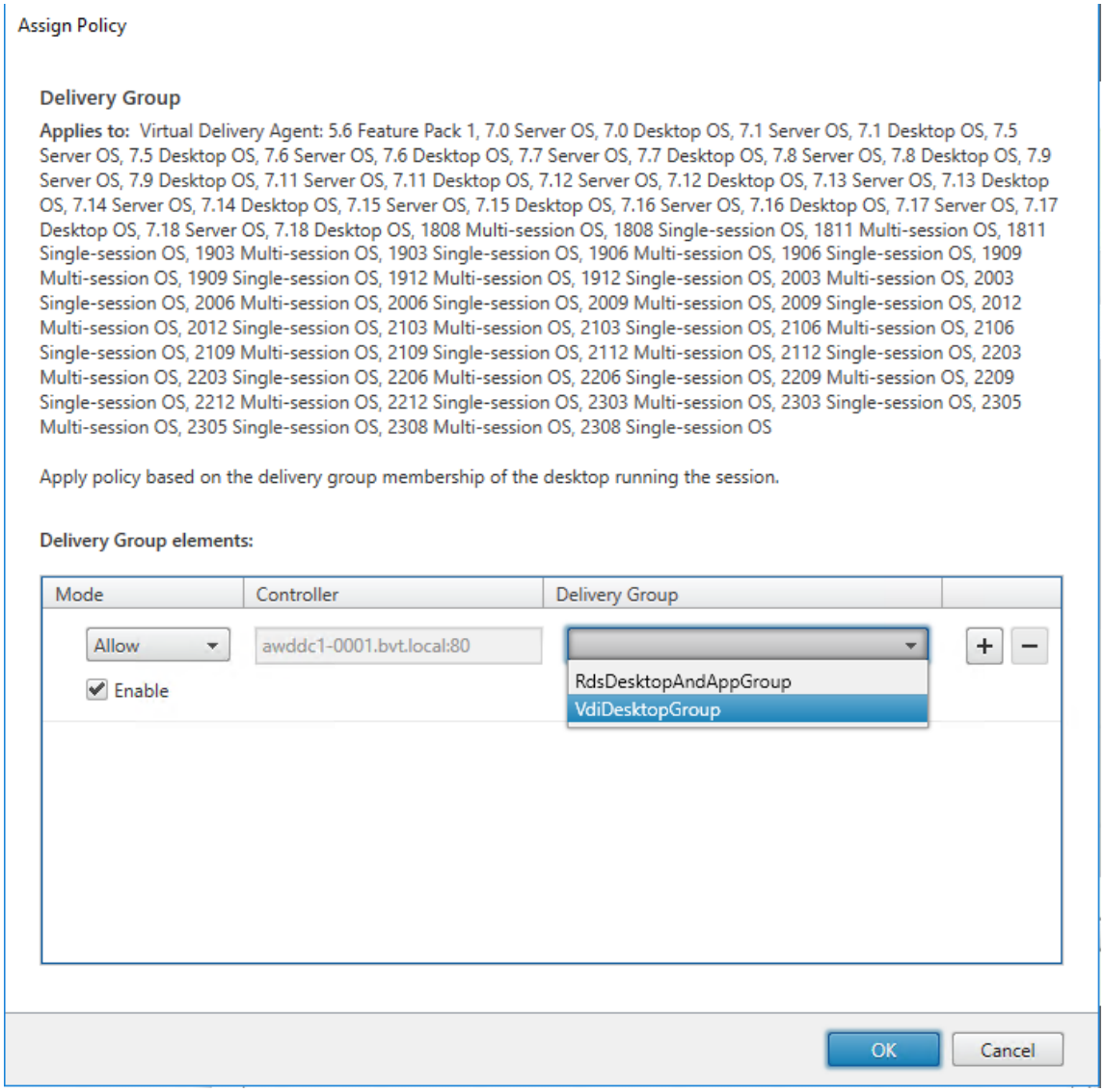
Remarque :

- Chaque entrée ne doit comporter qu'une seule fonctionnalité.
- Aucun espace n'est autorisé dans le nom de la fonctionnalité.
- Assurez-vous que les valeurs sont correctement orthographiées. Les valeurs mal orthographiées entraînent la fin de la session.
- Les valeurs qui ne comportent pas le préfixe Windows-, Linux- ou Mac- sont ignorées.

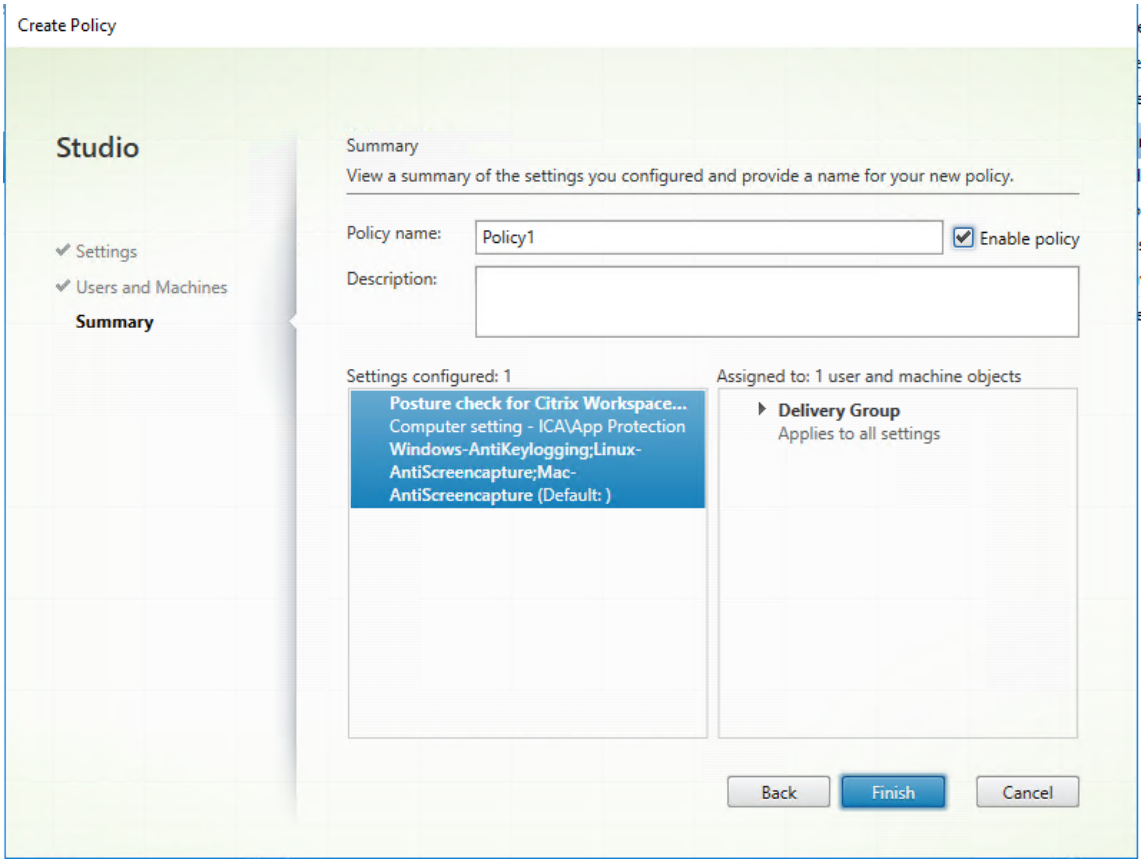
7. Une fois toutes les valeurs requises ajoutées, cliquez sur **OK**.
8. Cliquez sur **Suivant**.
9. Sélectionnez **Attribuer la stratégie à** > **Objets d'utilisateur et de machine sélectionnés**.



10. Sélectionnez les groupes de mise à disposition requis dans lesquels cette stratégie doit être déployée, puis cliquez sur **OK**.



11. Cliquez sur **Suivant**.
12. Entrez le nom de la stratégie dans le champ **Nom de la stratégie**, puis cochez la case **Activer la stratégie**.

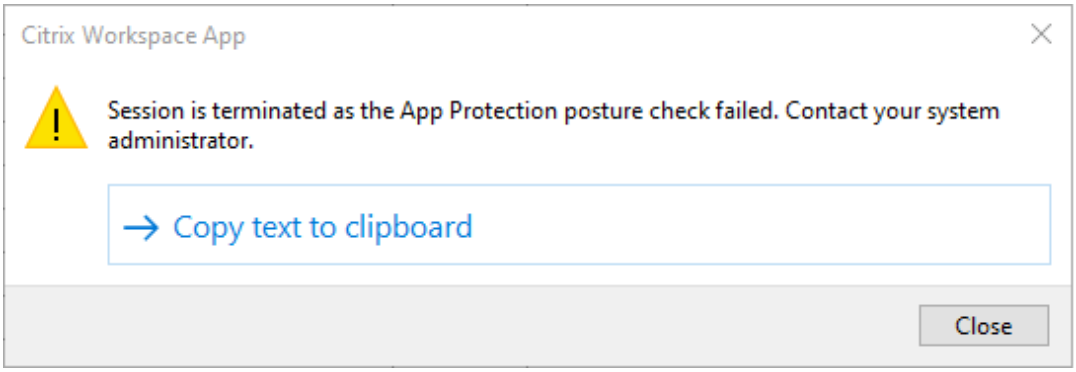


13. Cliquez sur **Terminer**.

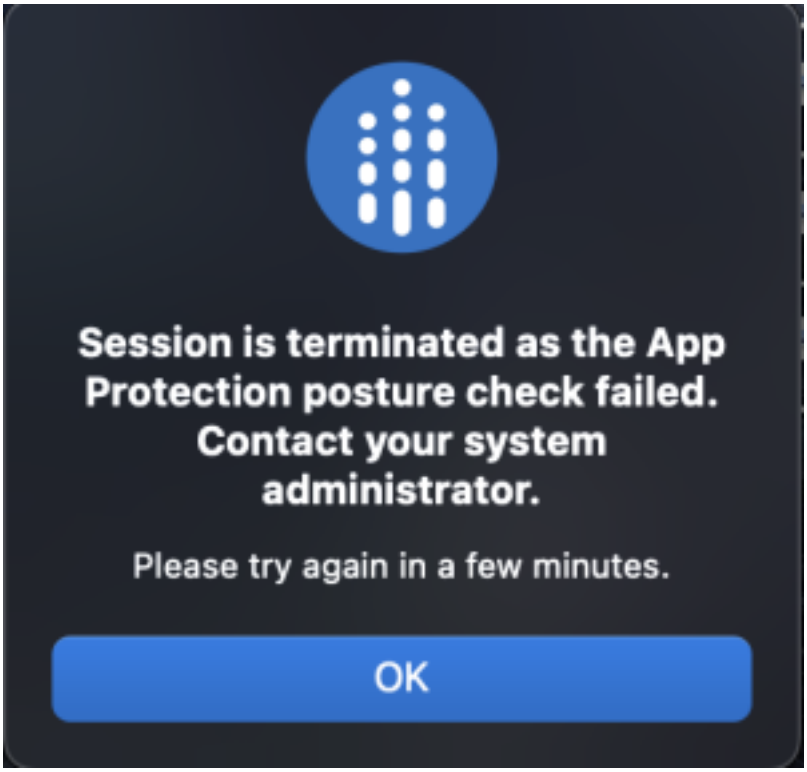
Une stratégie de vérification de l'état est désormais créée.

Comportement attendu en cas d'échec de la vérification de l'état d'App Protection

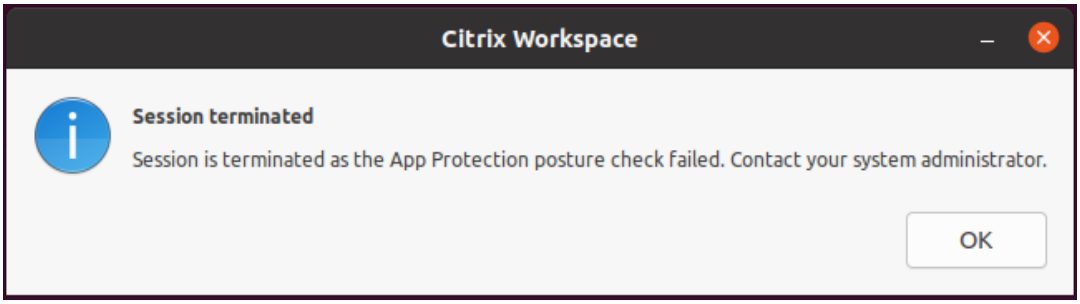
- Si la stratégie du VDA Citrix de vérification de l'état est activée et que vous utilisez une version de l'application Citrix Workspace qui ne prend pas en charge la fonctionnalité de vérification de l'état, la session est interrompue sans afficher de message d'erreur.
- Si vous utilisez une version de l'application Citrix Workspace qui prend en charge la fonctionnalité de vérification de l'état, la session se termine en affichant respectivement les messages d'erreur suivants :
  - Windows :



- Mac



- Linux



Bloquer le lancement de DoubleHop

March 11, 2024

Pour bloquer le lancement de DoubleHop, assurez-vous que vous exécutez l'application Citrix Workspace pour Windows 2309 ou version ultérieure lors du premier saut.

Déployez les configurations suivantes sur tous les VDA lors du premier saut :

1. Mettez à jour les dernières stratégies GPO. Pour en savoir plus, consultez la section Mettre à jour les dernières stratégies GPO.
2. Lancez l'**éditeur de stratégie de groupe**, puis accédez à **Configuration de l'ordinateur** > **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **App Protection** > **Bloquer le lancement de DoubleHop**.
3. Sélectionnez **Activé** et cliquez sur **OK**.

   Le paramètre **Bloquer le lancement de DoubleHop** est activé et vous êtes bloqué si vous essayez d'effectuer un lancement DoubleHop.

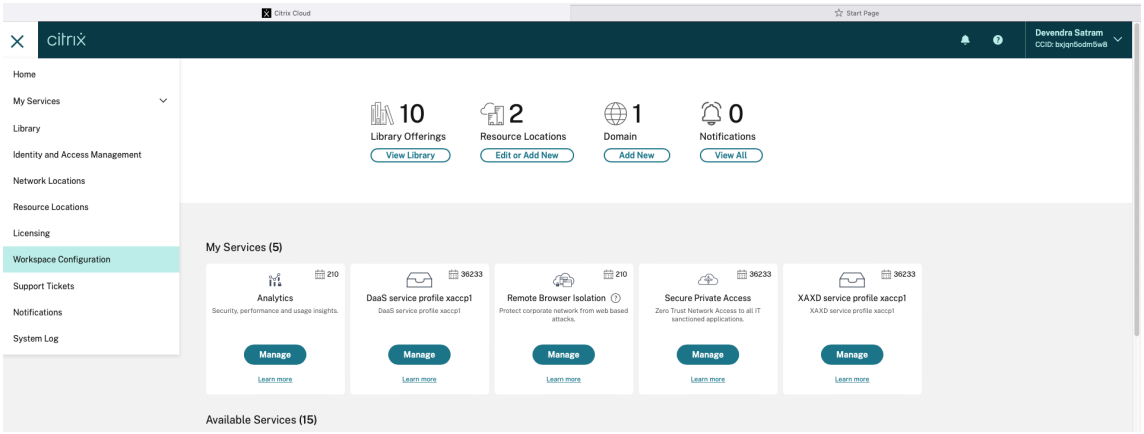
> **Remarque :**
>
> Le système d'exploitation Windows Server ne prend pas en charge App Protection. Les instances de Virtual Apps and Desktops activées avec App Protection ne s'affichent pas si vous utilisez un système d'exploitation Windows Server lors du premier saut.

Configuration de la liste verte de capture d'écran

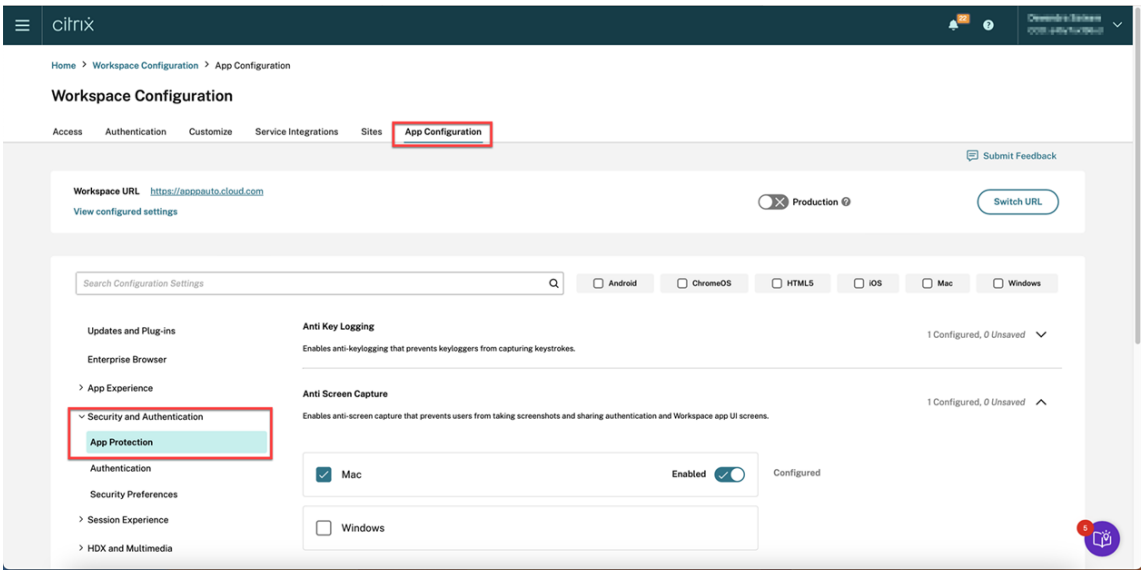
April 25, 2024

Pour ajouter une application à la liste verte des captures d'écran, procédez comme suit :

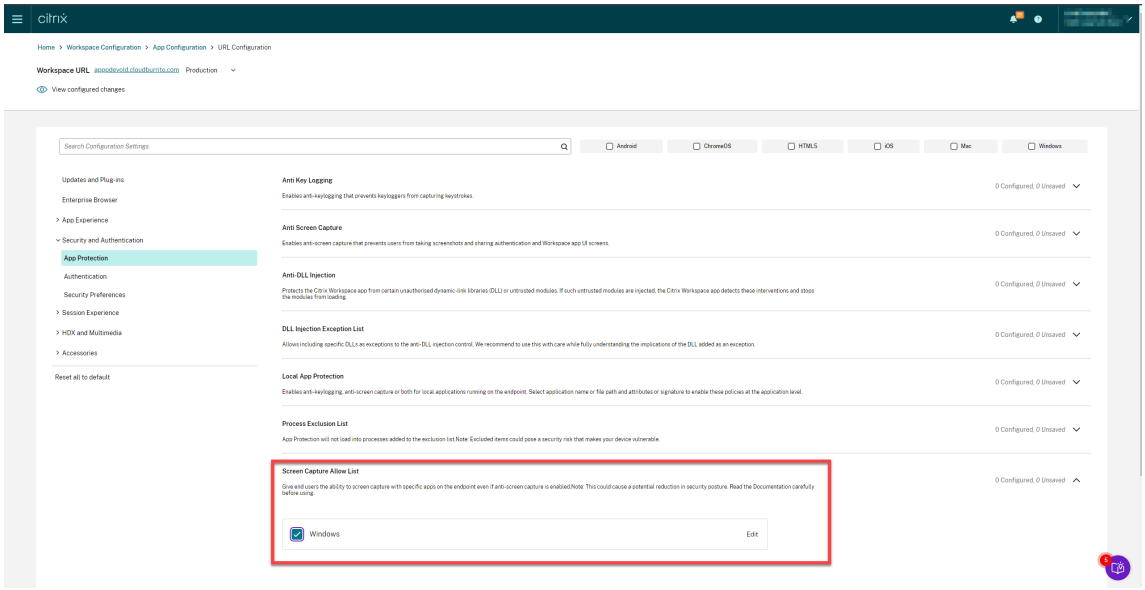
1. Connectez-vous à votre compte Citrix Cloud et sélectionnez **Configuration de l'espace de travail**.



2. Sélectionnez **Configuration de l'application** > **Sécurité et authentification** > **Configurer** > **App Protection**.



3. Cliquez sur **Liste verte des captures d'écran** et cochez la case **Windows**.



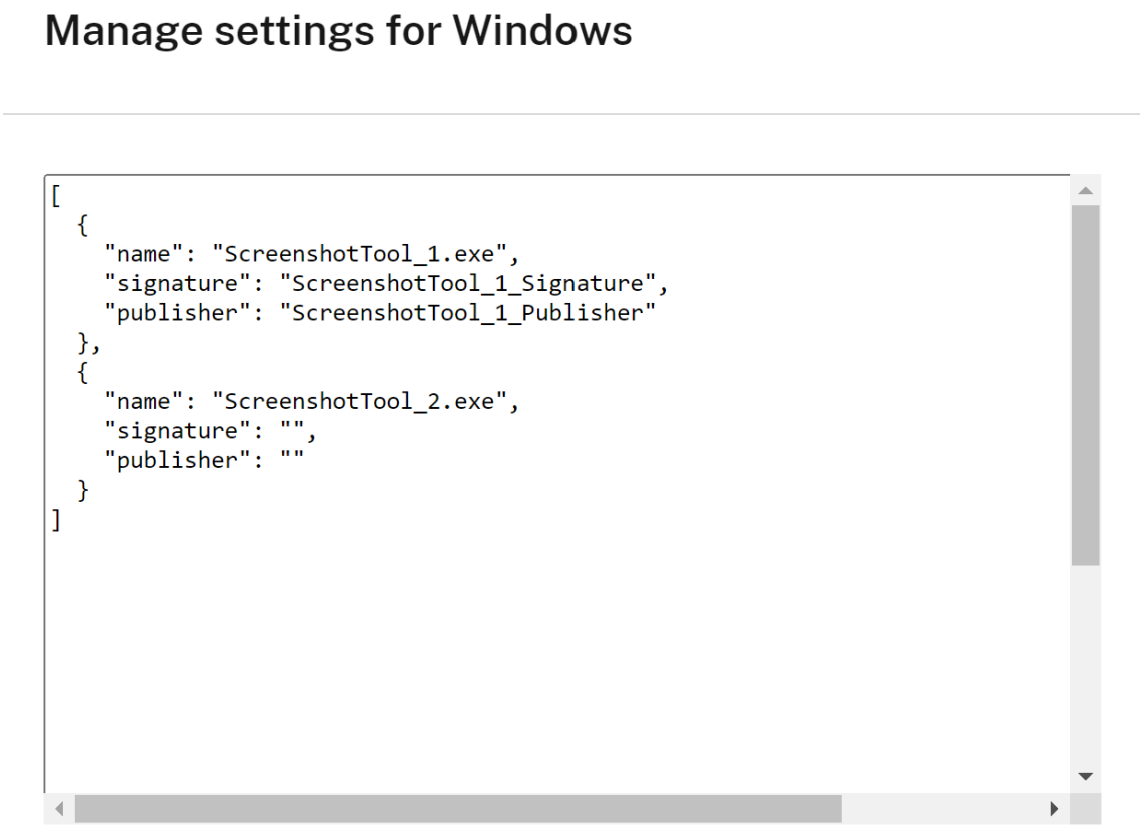
4. Cliquez sur l'option **Modifier**.

   L'écran **Gestion des paramètres Windows** s'affiche.

5. Ajoutez les informations relatives à l'application que vous souhaitez ajouter à la liste verte des captures d'écran.

   Par exemple,

```
[
 {

 "name": "ScreenshotTool_1.exe",
 "signature": "ScreenshotTool_1 Signature",
 "publisher": "ScreenshotTool_1 Publisher"
  }
 ,
 {

  "name": "Screenshottool_2.exe",
  "signature": "",
  "publisher": ""
  }

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

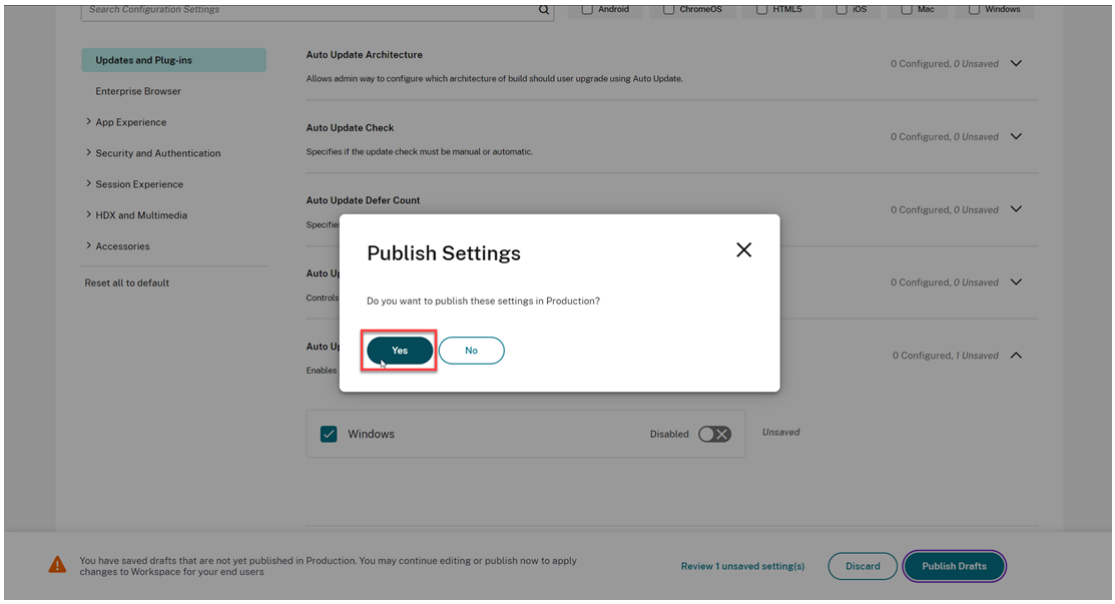
Remarque :

- Le champ `name` doit obligatoirement être rempli. Cependant, les champs `publisher` et `signature` ne sont pas obligatoires. Nous vous recommandons toutefois de spécifier les valeurs `publisher` et `signature` appropriées pour vous assurer que seule l'application figurant sur la liste verte peut prendre des captures d'écran.
- Si vous ne spécifiez pas les valeurs `publisher` et `signature`, une application malveillante du même nom peut prendre des captures d'écran.
- Vous pouvez également ajouter plusieurs applications à la liste verte de capture d'écran en spécifiant plusieurs entrées dans ce bloc.

Pour obtenir les informations `publisher` et `signature`, consultez Obtenir les informations `publisher` et `signature`.

6. Cliquez sur **Enregistrer le brouillon**, puis sur **Publier les brouillons**.

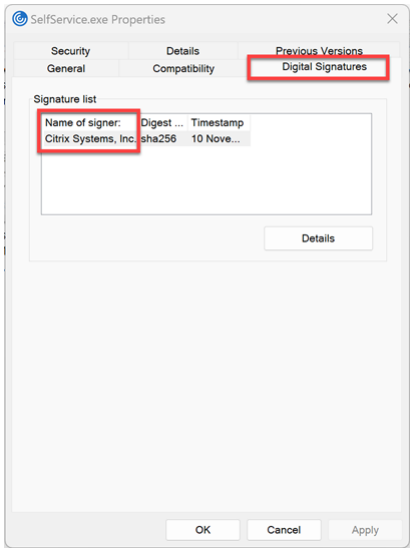
7. Dans la boîte de dialogue **Paramètres de publication**, cliquez sur **Oui**.



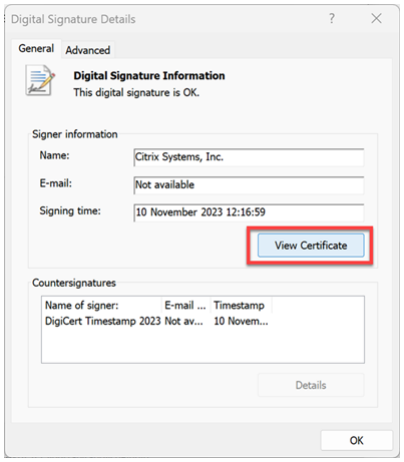
Obtention des informations `publisher` et `signature`

Pour obtenir les informations `publisher` et `signature`, procédez comme suit :

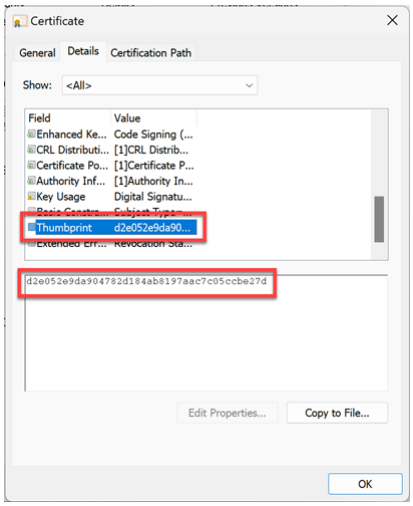
1. Ouvrez l'emplacement du fichier où se trouve le fichier `.exe` correspondant de l'application.
2. Cliquez avec le bouton droit de la souris sur le fichier `.exe`, puis sur **Propriétés**. Une fenêtre contextuelle des propriétés s'affiche.
3. Cliquez sur **Signatures numériques**. Le **nom du signataire** est la valeur `publisher`.



4. Cliquez sur la première entrée du champ **Nom du signataire**, puis cliquez sur **Détails** > **Afficher certificat**.



5. Cliquez sur **Détails** > **Empreinte numérique**. Le contenu qui apparaît dans la zone de texte est la `signature`.

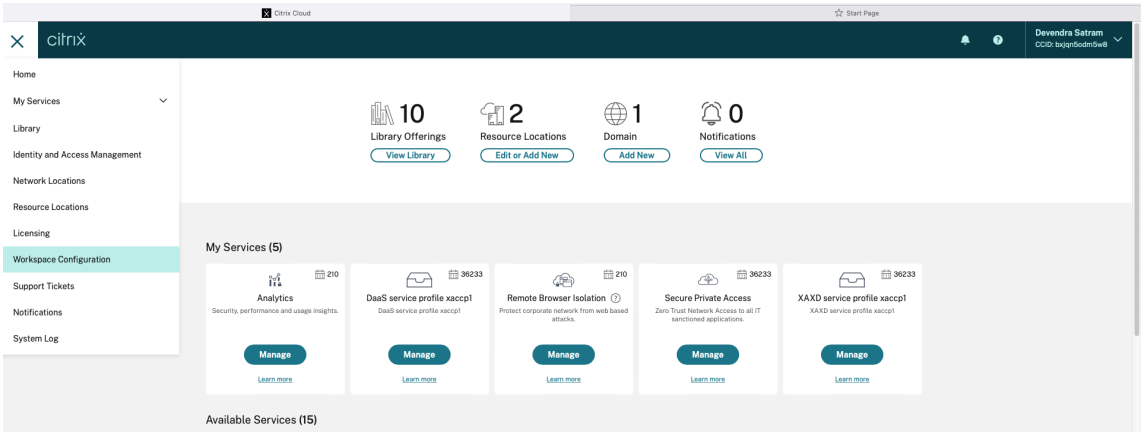


Configuration de la liste d'exclusion des processus

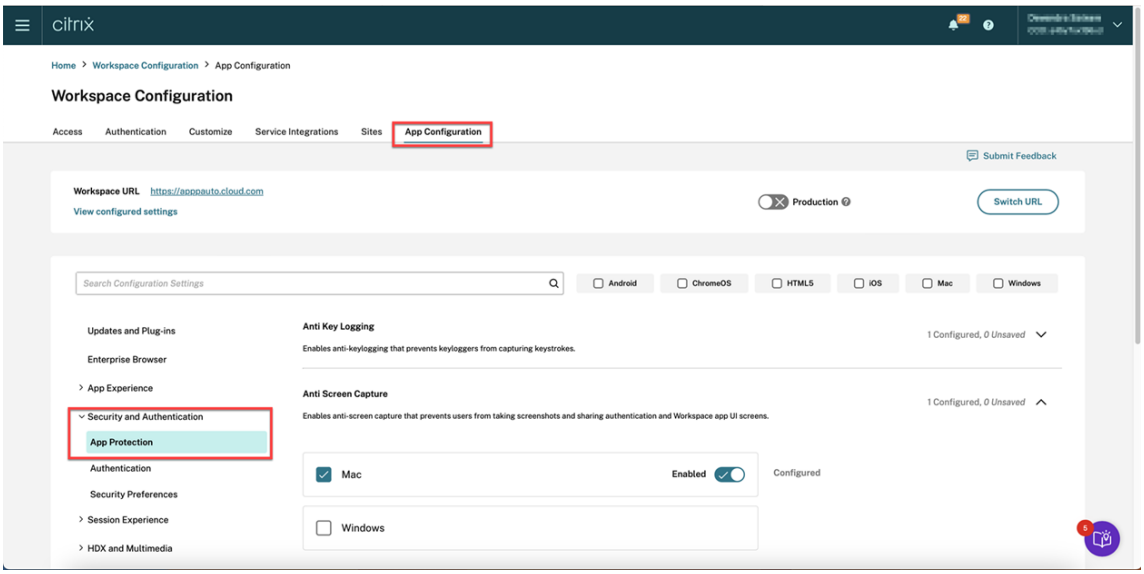
April 29, 2024

Pour ajouter un processus à la liste d'exclusion des processus, procédez comme suit :

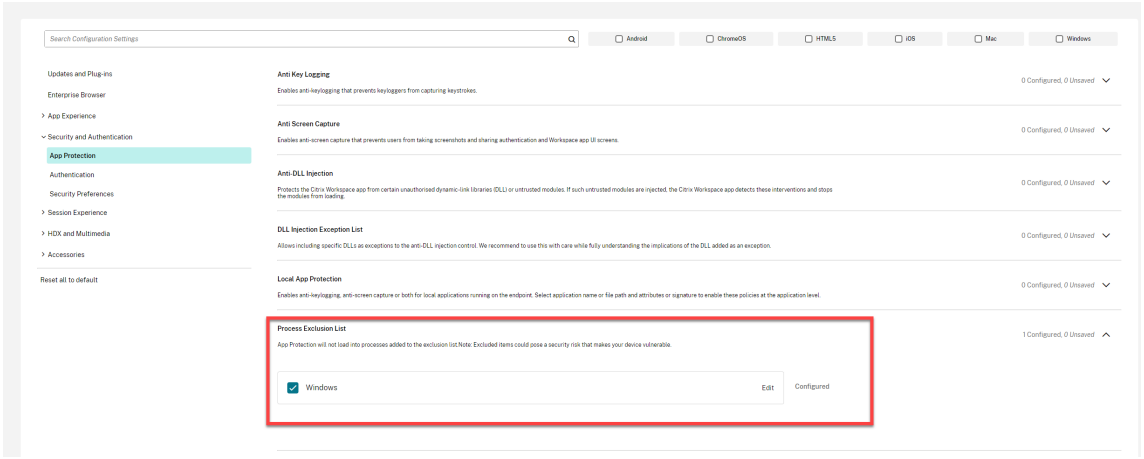
1. Connectez-vous à votre compte Citrix Cloud et sélectionnez **Configuration de l'espace de travail**.



2. Sélectionnez **Configuration de l'application** > **Sécurité et authentification** > **Configurer** > **App Protection**.



3. Cliquez sur **Liste d'exclusion des processus**, puis cochez la case **Windows**.



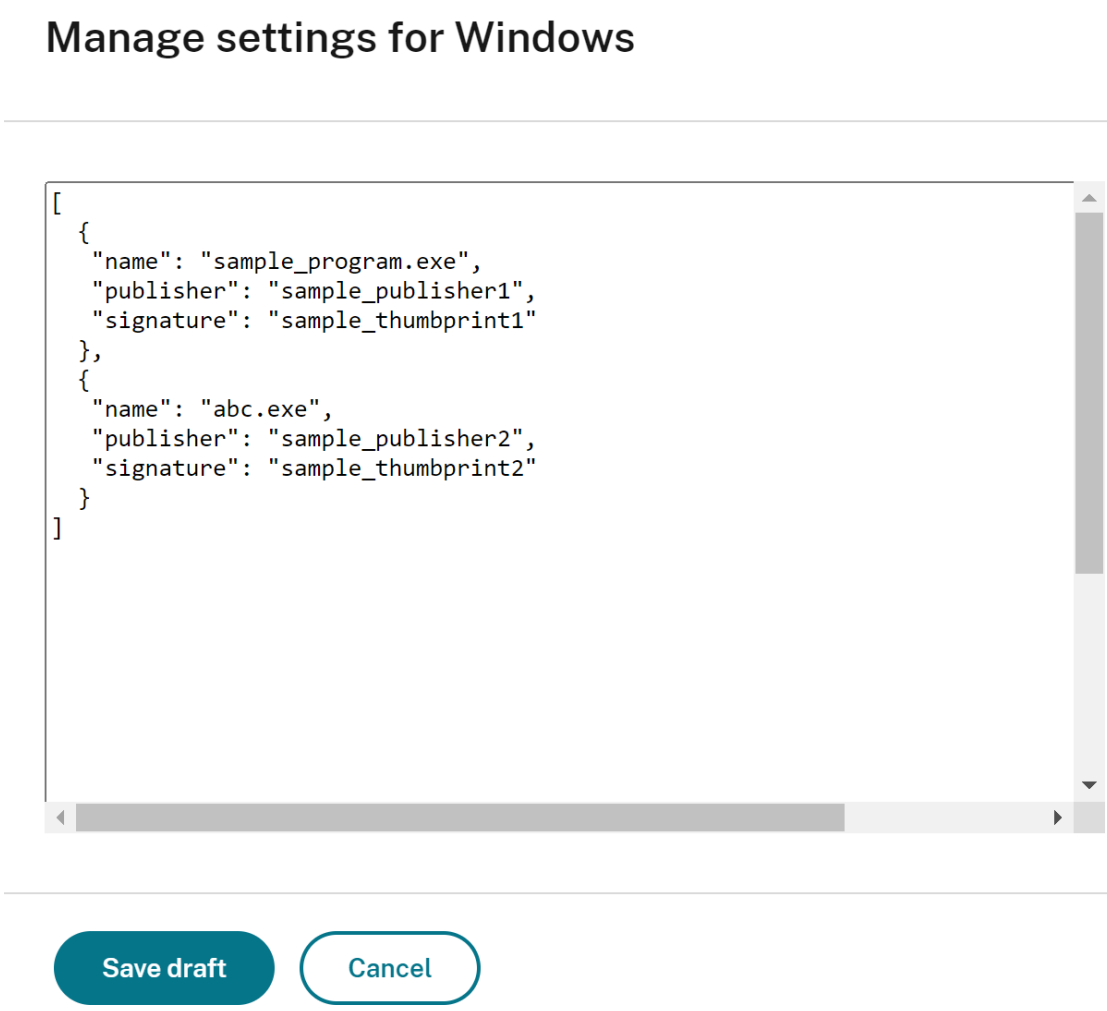
4. Cliquez sur l'option **Modifier**.

L'écran **Gestion des paramètres Windows** s'affiche.

5. Ajoutez les informations relatives au processus que vous souhaitez ajouter à la liste d'exclusion des processus.

   Par exemple,

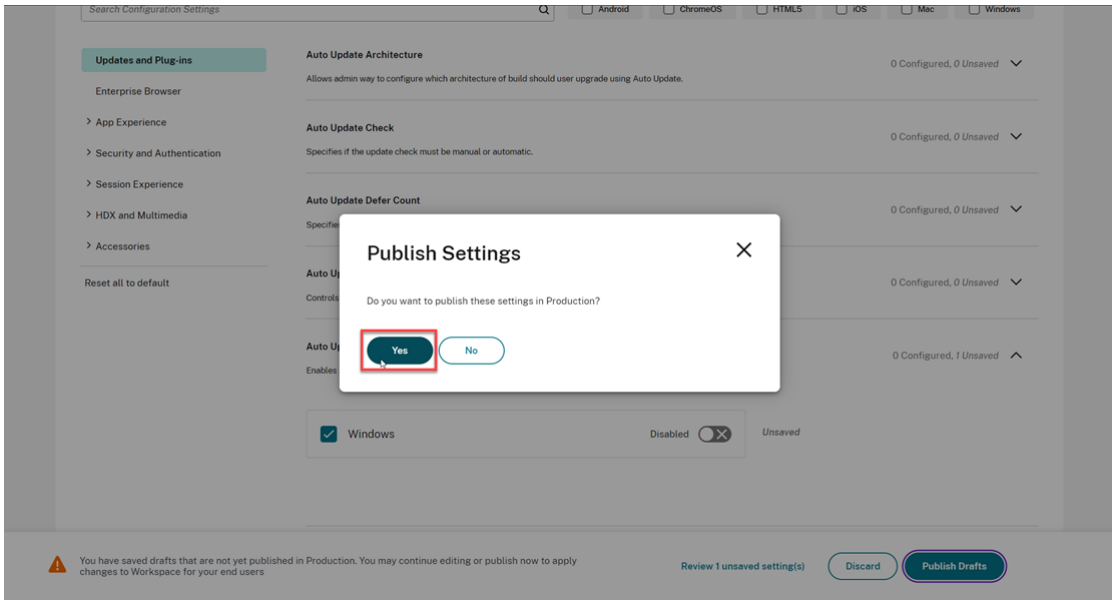
```
[
 {

  "name": "sample_program.exe",
  "publisher": "sample_publisher1",
  "signature": "sample_thumbprint1"
  }

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



> **Remarque :**
>
> - Le champ `name` doit obligatoirement être rempli. Cependant, les champs `publisher` et `signature` ne sont pas obligatoires. Nous vous recommandons toutefois de spécifier les valeurs `publisher` et `signature` pour vous assurer d'ajouter le processus correct à la liste.
> - Vous pouvez également ajouter plusieurs processus à la liste d'exclusion des processus en spécifiant plusieurs entrées dans ce bloc.

Pour obtenir les informations `publisher` et `signature`, consultez Obtenir les informations `publisher` et `signature`.

6. Cliquez sur **Enregistrer le brouillon**, puis sur **Publier les brouillons**.
7. Dans la boîte de dialogue **Paramètres de publication**, cliquez sur **Oui**.



8. Redémarrez l'application Citrix Workspace.

Configuration de la liste d'exclusion des pilotes de filtre USB

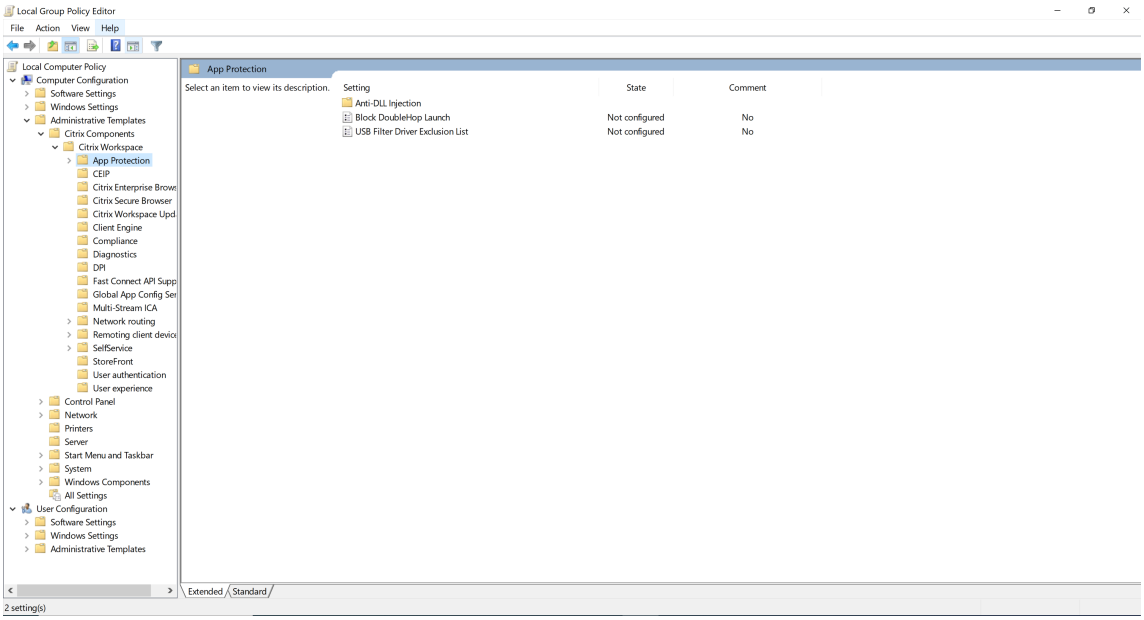
April 29, 2024

Vous pouvez ajouter un périphérique USB à la liste d'exclusion des pilotes de filtre USB en utilisant l'une des méthodes suivantes :

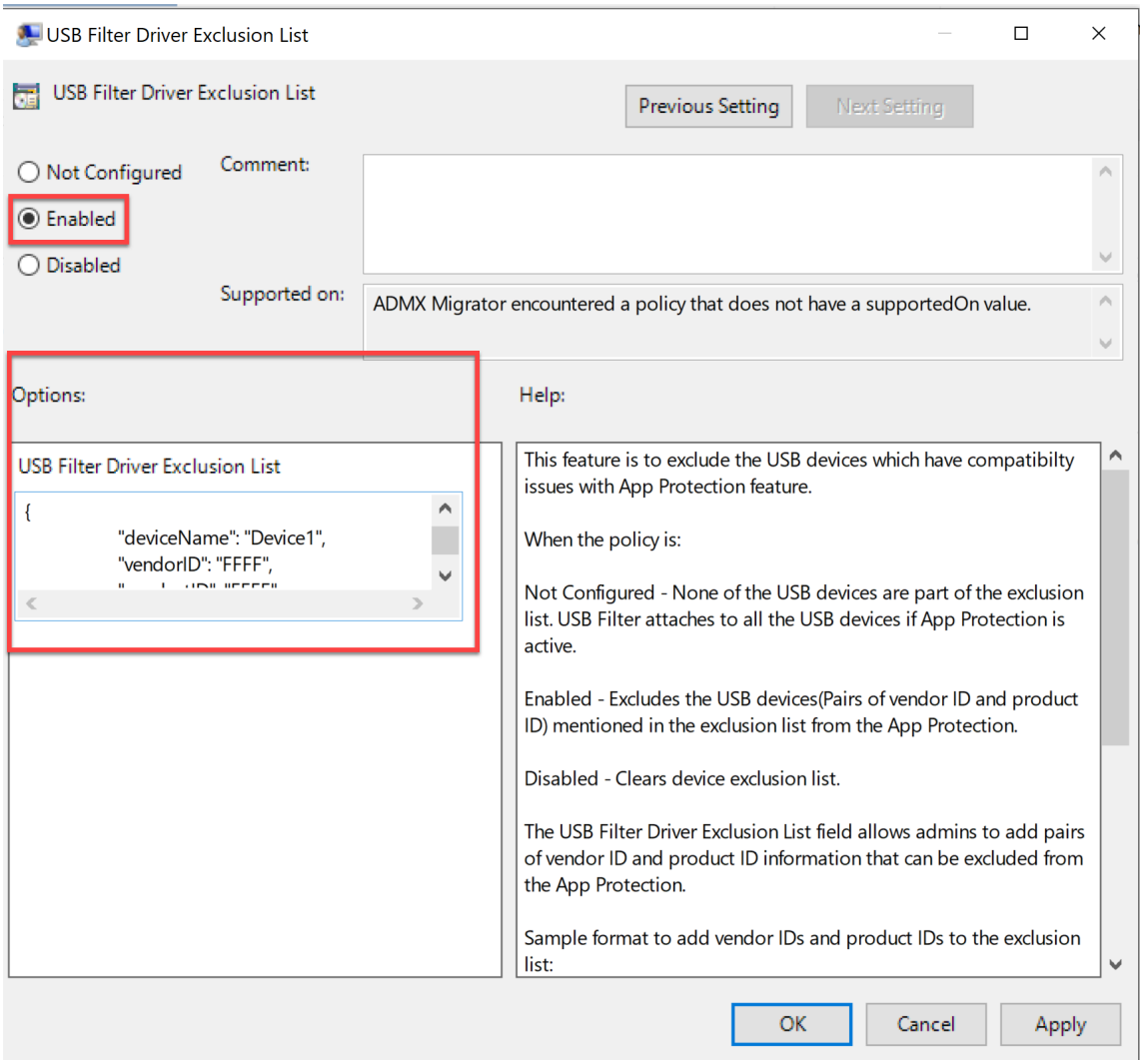
- Utilisation de l'objet de stratégie de groupe
- Utilisation de l'interface utilisateur de Global App Configuration Service

Utilisation de l'objet de stratégie de groupe

1. Ouvrez le modèle d'administration d'objet de stratégie de groupe de l'application Citrix Workspace en exécutant `gpedit.msc`. Pour plus d'informations, consultez la section Objet de stratégie de groupe.
2. Sous le nœud **Configuration de l'ordinateur**, accédez à **Modèles d'administration** > **Composants Citrix** > **Citrix Workspace** > **App Protection** > **Liste d'exclusion des pilotes de filtre USB**.



3. Sélectionnez **Activé** et entrez l'**ID fournisseur** et l'**ID produit** du périphérique USB que vous souhaitez exclure dans la zone de texte **Options**.



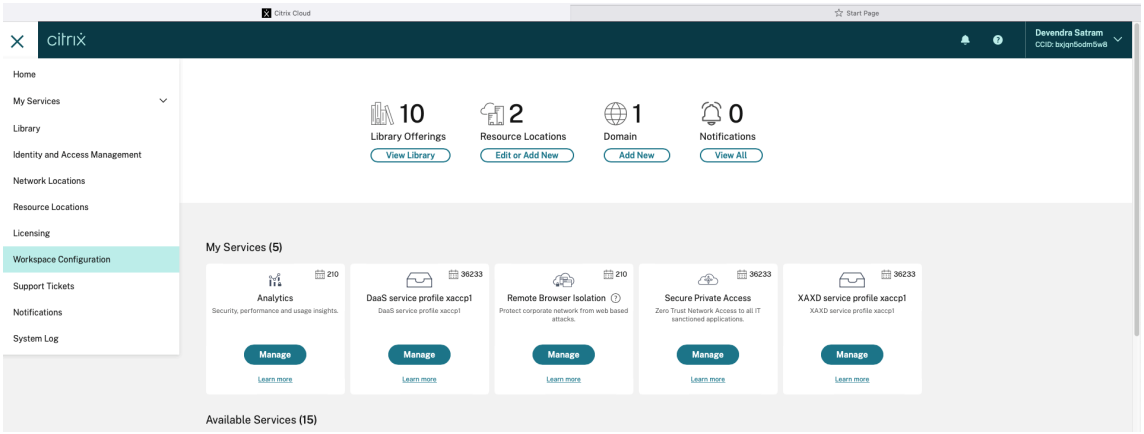
> **Remarque :**
>
> - Les champs `productID` et `vendorID` doivent être obligatoirement remplis. Cependant, le champ `deviceName` n'est pas obligatoire.
> - Vous pouvez également ajouter plusieurs périphériques USB à la liste d'exclusion en spécifiant plusieurs entrées dans ce bloc.

Pour obtenir les informations `productID` et `vendorID`, consultez Obtention des informations `productID` et `vendorID`.

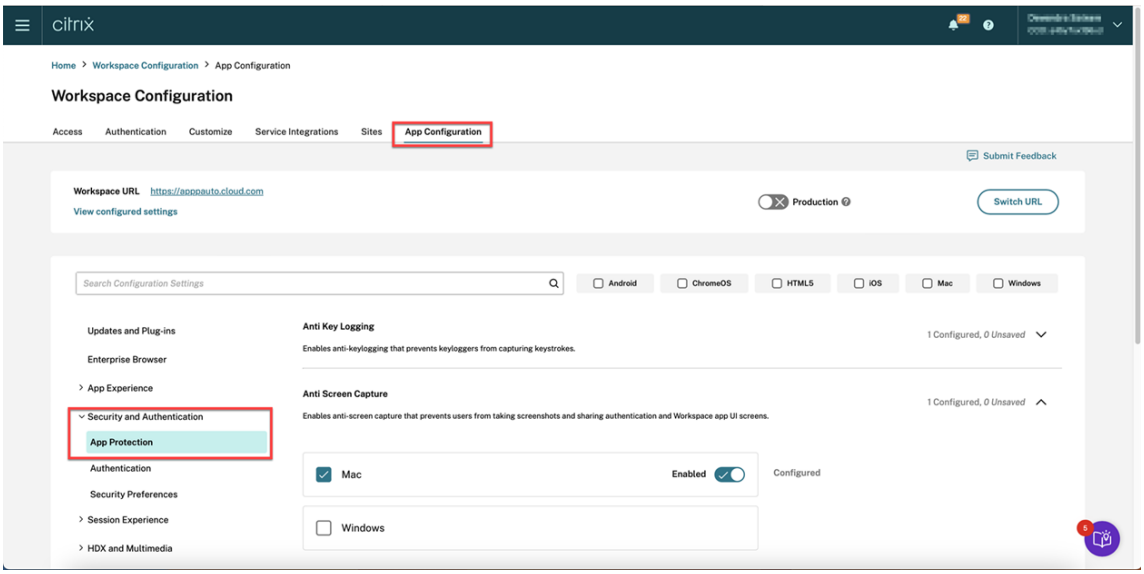
4. Cliquez sur **OK**.

Utilisation de l'interface utilisateur de Global App Configuration Service

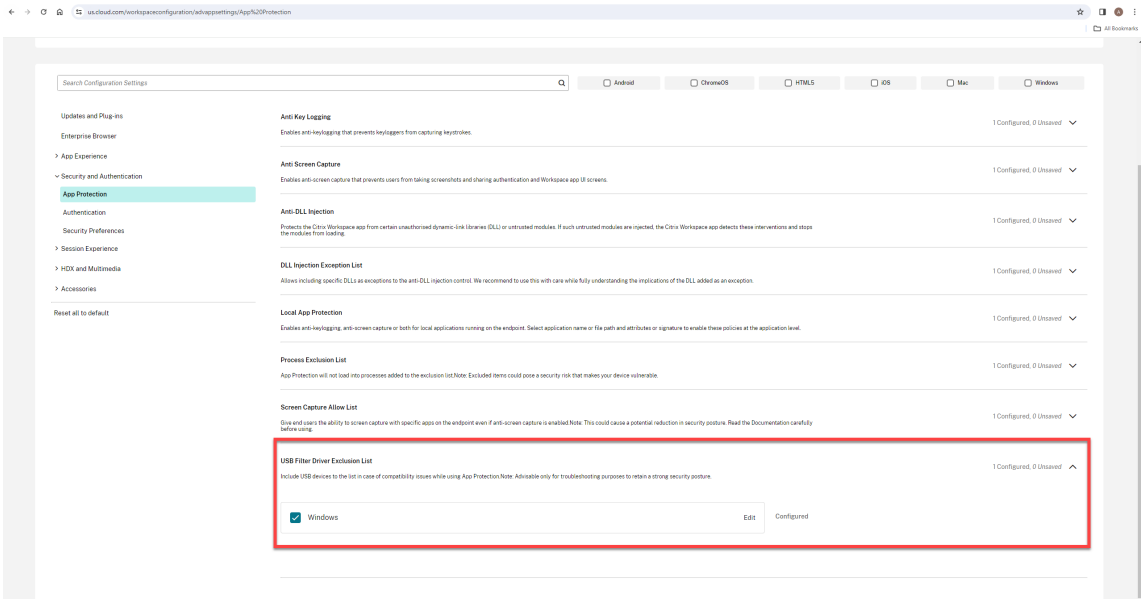
1. Connectez-vous à votre compte Citrix Cloud et sélectionnez **Configuration de l'espace de travail**.



2. Sélectionnez **Configuration de l'application** > **Sécurité et authentification** > **Configurer** > **App Protection**.



3. Cliquez sur **Liste d'exclusion des pilotes de filtre USB**, puis cochez la case **Windows**.



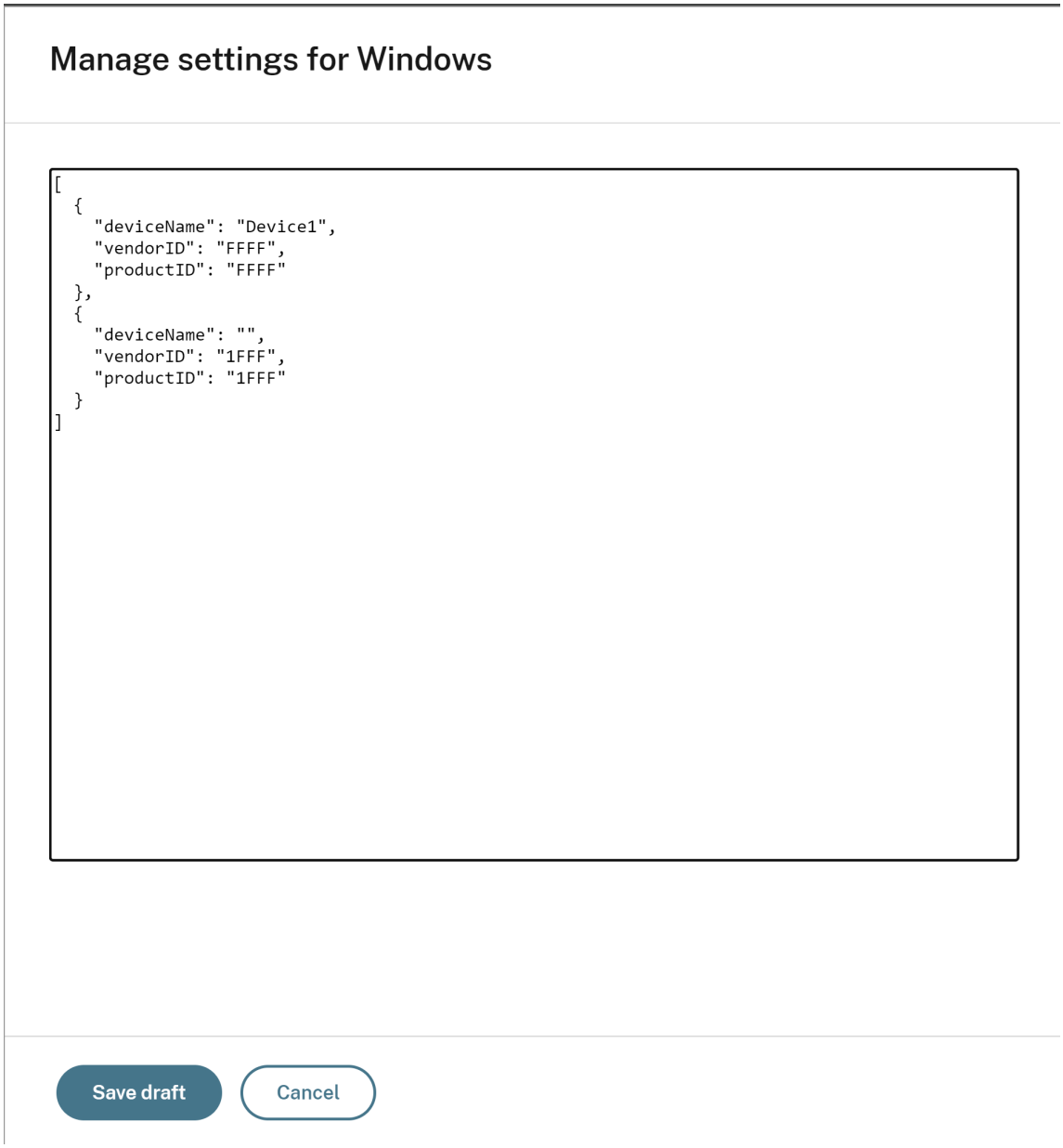
4. Cliquez sur l'option **Modifier**.

   L'écran **Gestion des paramètres Windows** s'affiche.

5. Ajoutez les informations relatives au processus ou à l'application que vous souhaitez ajouter à la liste d'exclusion des pilotes de filtre USB.

   Par exemple,

```
[
 {

  "deviceName": "Device1",
  "vendorID": "FFFF",
  "productID": "FFFF"
  }

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

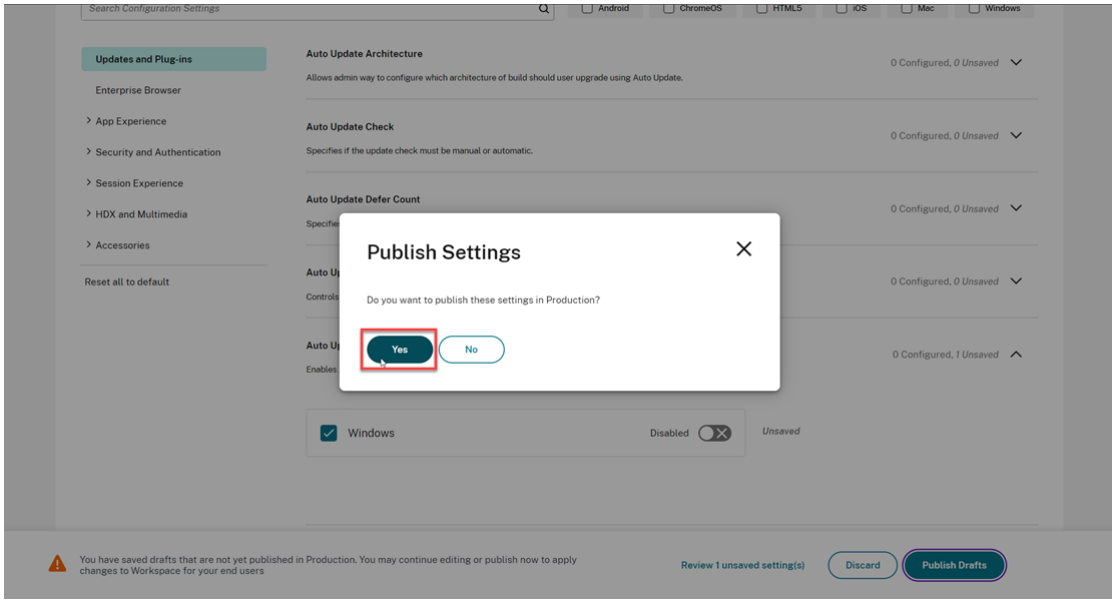



Remarque :

- Les champs `productID` et `vendorID` doivent être obligatoirement remplis. Cependant, le champ `deviceName` n'est pas obligatoire.
- Vous pouvez également ajouter plusieurs périphériques USB à la liste d'exclusion en spécifiant plusieurs entrées dans ce bloc.

Pour obtenir les informations `productID` et `vendorID`, consultez Obtention des informations `productID` et `vendorID`.

6. Cliquez sur **Enregistrer le brouillon**, puis sur **Publier les brouillons**.
7. Dans la boîte de dialogue **Paramètres de publication**, cliquez sur **Oui**.

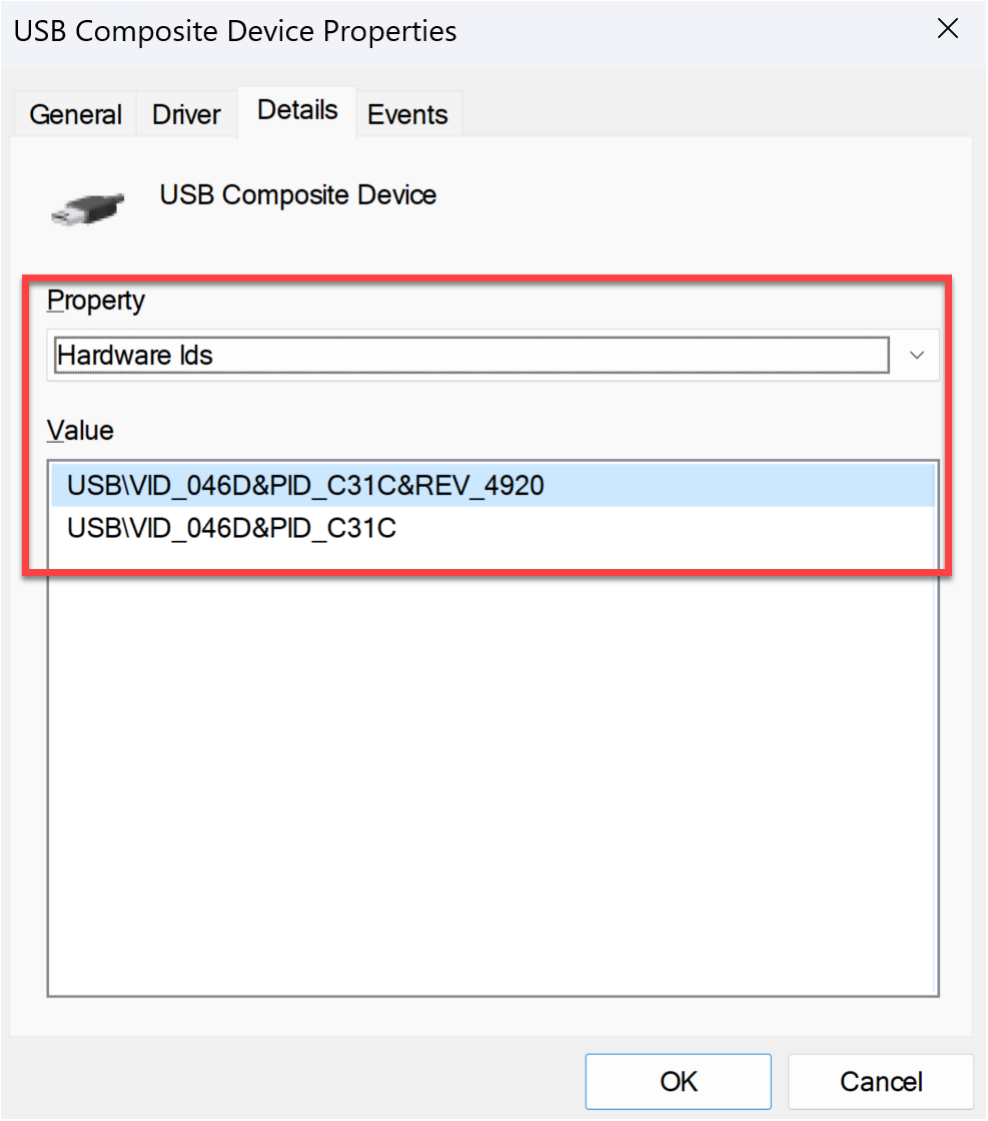


8. Redémarrez l'application Citrix Workspace.

Obtention des informations `productID` et `vendorID`

Pour obtenir les informations `productID` et `vendorID`, procédez comme suit :

1. Ouvrez le **Gestionnaire de périphériques** et recherchez le périphérique que vous souhaitez ajouter à la liste d'exclusion.
2. Cliquez avec le bouton droit de la souris sur le nom du périphérique, puis cliquez sur **Propriétés**. Une fenêtre contextuelle des propriétés s'affiche.
3. Cliquez sur **Détails**, puis sélectionnez l'option **Identifiants matériels** dans la liste **Propriétés**.
4. Dans le champ **Valeur**, la valeur avec le préfixe `VID_` est l'ID `vendorID` et la valeur avec le préfixe `PID_` est l'ID `productID`.



Dépannage

March 11, 2024

Cet article explique comment résoudre les problèmes liés à la App Protection sur différentes plates-formes pour l'application Citrix Workspace.

Pour les scénarios de dépannage, consultez les rubriques suivantes :

- Scénarios de dépannage génériques
- Détection d'altération des stratégies
- Vérification de la posture d'App Protection

Application Citrix Workspace pour Windows

1. Collectez les journaux comme décrit dans la section Collecte de journaux.
2. Appuyez sur **Win+R** pour ouvrir la boîte Exécuter, puis tapez `cmd` > Sélectionnez **Entrée**.
3. Exécutez les commandes suivantes :

    - Si vous utilisez une version de l'application Citrix Workspace pour Windows antérieure à 2311, exécutez les commandes suivantes :

        - `sc query appprotectionsvc`
        - `sc query entryprotectdrv`
        - `sc query epinject6`
        - `sc query epusbfilter`

    - Si vous utilisez la version 2311 de l'application Citrix Workspace pour Windows ou une version ultérieure, exécutez les commandes suivantes :

        - `sc query appprotectionsvc`
        - `sc query ctxapdriver`
        - `sc query ctxapinject`
        - `sc query ctxapusbfilter`

Obtenez les résultats ainsi que les traces collectées à l'aide de l'outil de collecte de journaux.

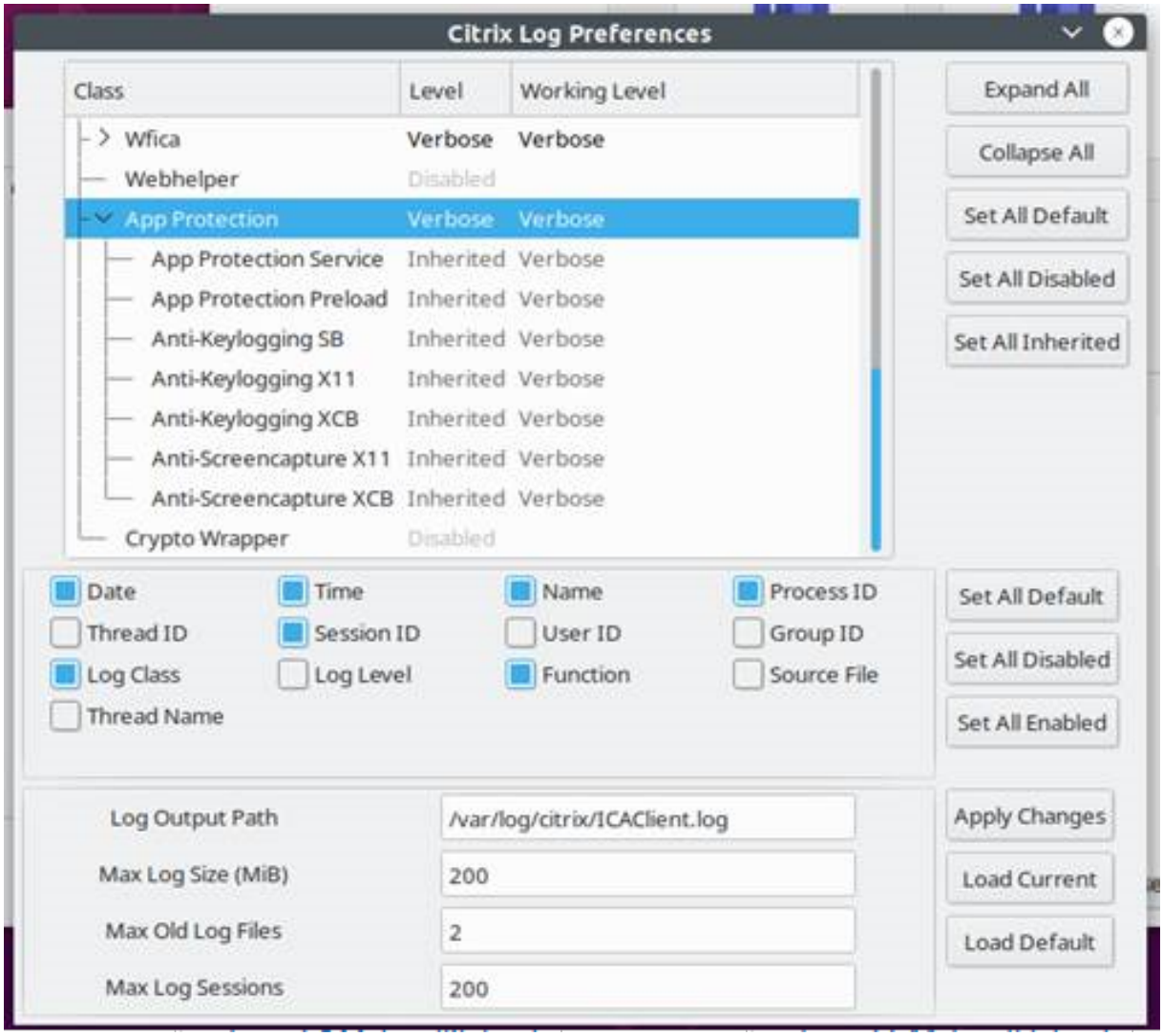
Application Citrix Workspace pour Mac

Obtenez les journaux en les collectant comme décrit dans la section Collecte des journaux.

Application Citrix Workspace pour Linux

1. Exécutez le fichier exécutable set log qui se trouve dans le dossier *util* de l'installation. Par exemple, `/opt/Citrix/ICAClient/util/setlog`.
2. Cliquez sur **Tout désactiver** (cette étape est facultative et permet de s'assurer que seuls les journaux requis sont collectés).
3. Accédez à la journalisation de la App Protection.
4. Définissez le niveau du journal de protection des applications sur Détaillé en cliquant avec le bouton droit de la souris et en sélectionnant Détaillé (seuls les avertissements et les erreurs sont enregistrés).
5. Développez la classe App Protection et cliquez avec le bouton droit sur son élément enfant. Sélectionnez **Groupe > Hérité**.

6. Activez les journaux pour **wfica**. Cliquez avec le bouton droit sur **wfica** et sélectionnez **Détaillé**. Si App Protection n'est pas installée ou n'est pas détectable par **wfica**, vous obtenez le journal comme **[NCS] < P3563 > citrix-wfica: App Protection is not installed**.
7. Lorsque vous lancez la session, les journaux sont enregistrés dans le fichier mentionné dans le *chemin de sortie du journal* défini.



Résolution des problèmes génériques

March 11, 2024

Les ressources dotées de stratégies App Protection ne s'affichent pas dans les applications natives

Si les ressources activées avec les stratégies App Protection ne s'affichent pas dans les applications natives, procédez comme suit :

1. Mettez à jour votre application Citrix Workspace vers une version supérieure si sa version est antérieure à la suivante :
    - Application Citrix Workspace 2108 pour Linux
    - Application Citrix Workspace 2203.1 LTSR pour Windows
    - Application Citrix Workspace 2002 pour Windows
    - Application Citrix Workspace 2305.1 pour Windows (Store)
    - Application Citrix Workspace 2001 pour Mac
2. Assurez-vous de ne pas avoir installé l'application Citrix Workspace dans un système d'exploitation Windows multisession tel que Windows 2K16 ou Windows 2K22.
3. Si les conditions précédentes sont remplies, mais que les ressources ne s'affichent toujours pas, collectez les journaux et contactez le support technique de Citrix. Pour en savoir plus sur la collecte des journaux, consultez la section Collecte de journaux.

Les ressources activées avec les stratégies App Protection ne s'affichent pas dans le navigateur lors de l'utilisation du magasin local

Si les ressources activées avec les stratégies App Protection ne s'affichent pas dans le navigateur lorsque vous utilisez le magasin local, procédez comme suit :

1. Assurez-vous que la version de Delivery Controller n'est pas antérieure à la version 1912.

    > **Remarque :**
    >
    > La fonctionnalité App Protection n'est pas prise en charge si vous utilisez un composant Delivery Controller antérieur à la version 1912.

2. Si vous utilisez des versions de StoreFront comprises entre 1912 et 2203, vérifiez si vous avez activé la personnalisation StoreFront. Pour de plus amples informations sur l'activation de la personnalisation StoreFront, consultez Activer la personnalisation StoreFront.
3. Si vous utilisez la version 2308 de StoreFront ou une version ultérieure, il n'est pas nécessaire d'activer la personnalisation StoreFront. Vérifiez si vous avez correctement activé App Protection pour le lancement hybride sur StoreFront en vous reportant à la section Lancement hybride via StoreFront version 2308 ou ultérieure.

4. Vérifiez si vous avez correctement activé les fonctionnalités App Protection pour le groupe de mise à disposition.
5. Si les conditions précédentes sont remplies mais que les ressources ne s'affichent toujours pas, collectez les journaux et contactez le support technique de Citrix. Pour de plus amples informations sur la collecte des journaux, consultez les pages Collecter des journaux pour l'application Citrix Workspace et Collecter des journaux pour StoreFront.

Impossible d'établir un environnement sécurisé lors du lancement de ressources compatibles avec App Protection

Pour l'application Citrix Workspace pour Windows, vous devez cocher la case **Démarrer App Protection après l'installation** pendant l'installation afin de garantir le démarrage des services App Protection et la mise en place de l'environnement sécurisé. Si vous n'avez pas coché la case **Démarrer App Protection après l'installation**, le service App Protection démarre automatiquement lorsque vous lancez une ressource activée avec les stratégies App Protection. En fonction de la charge du système, le démarrage de la fonctionnalité App Protection peut prendre du temps. Parfois, elle peut démarrer ou s'arrêter. C'est pourquoi, il est recommandé de cocher la case **Démarrer App Protection après l'installation** au cours de l'installation. En général, si vous relancez la ressource activée avec App Protection, vous devez établir une connexion sécurisée. Toutefois, si vous ne parvenez toujours pas à lancer la ressource activée avec App Protection, procédez comme suit :

1. Ouvrez l'invite de commande en tant qu'administrateur, exécutez la commande suivante et vérifiez si le service App Protection est en cours d'exécution :

```
sc query AppProtectionSvc
<!--NeedCopy-->
```

2. Si le service App Protection n'est pas en cours d'exécution, démarrez-le en exécutant la commande suivante :

```
sc start AppProtectionSvc
<!--NeedCopy-->
```

3. Si l'erreur persiste, collectez les journaux et contactez le support technique de Citrix. Pour en savoir plus sur la collecte des journaux, consultez la section Collecte de journaux.

Impossible d'activer ou de désactiver App Protection

Si vous ne parvenez pas à activer ou désactiver App Protection pour un groupe de mise à disposition local ou dans le cloud que ce soit via Web Studio ou PowerShell, procédez comme suit :

1. Vérifiez si vous possédez la licence requise. Si les licences requises ne sont pas disponibles, vous ne pouvez pas activer App Protection.

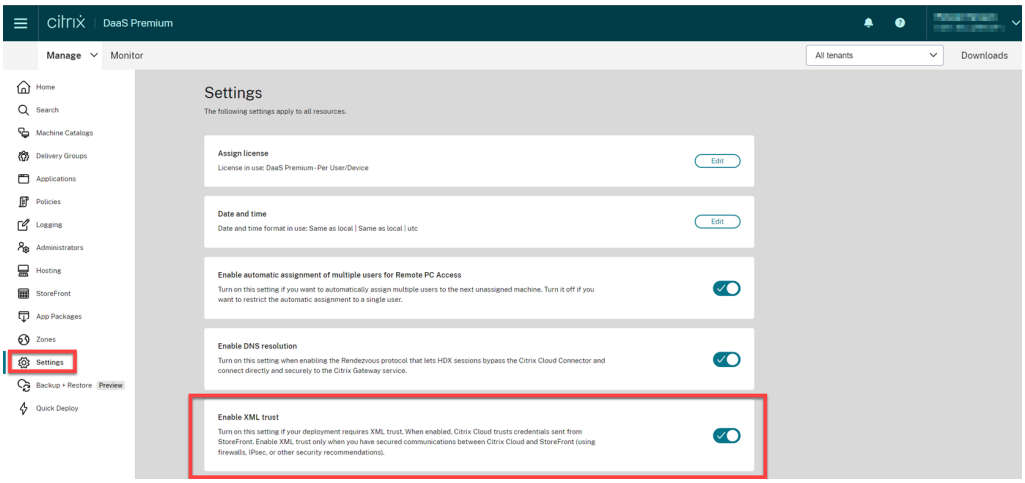
2. Dans pareil cas, récupérez les licences requises et ajoutez-les.
3. Une fois les licences ajoutées, redémarrez le serveur de licences et réessayez d'activer App Protection.
4. Si des licences valides sont disponibles mais que vous ne parvenez toujours pas à activer ou désactiver la fonctionnalité App Protection, vérifiez si `TrustRequestsSentToTheXmlServicePort` est activé en exécutant la commande suivante :

```
Get-BrokerSite | Select-Object
    TrustRequestsSentToTheXmlServicePort
<!--NeedCopy-->
```

5. Si `TrustRequestsSentToTheXmlServicePort` n'est pas activé, activez XML Trust à l'aide de l'une des méthodes suivantes :

   - **Utilisation de Web Studio :**

     a) Connectez-vous à votre compte Citrix DaaS et cliquez sur **Gérer** > **Paramètres** > **Activer l'approbation XML**.

     b) Activez le bouton **Activer l'approbation XML**.

   - **À l'aide de PowerShell :** exécutez la commande suivante pour activer l'approbation XML :

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
<!--NeedCopy-->
```

6. Après avoir activé `TrustRequestsSentToTheXmlServicePort`, réactivez App Protection.
7. Si les conditions précédentes sont remplies, mais que vous ne parvenez toujours pas à activer ou désactiver App Protection, contactez le support technique de Citrix.

Les stratégies App Protection ne s'appliquent pas correctement

1. Assurez-vous que les conditions suivantes sont remplies :
    - Vous utilisez une version prise en charge de l'application Citrix Workspace.
    - Les fonctions appropriées sont activées dans le groupe de mise à disposition.
    - La fonctionnalité est installée sur le point de terminaison.
    - L'application Citrix Workspace a été installée avec le commutateur `/includeappprotection` activé.
2. Si les conditions précédentes sont remplies, mais que les stratégies App Protection ne s'appliquent toujours pas correctement, collectez les journaux et contactez le support technique de Citrix. Pour de plus amples informations sur la collecte des journaux, consulter la page Collecter des journaux pour l'application Citrix Workspace

Les captures d'écran ne fonctionnent pas sur les fenêtres non Citrix :

- Réduisez ou fermez les fenêtres Citrix protégées, y compris l'application Citrix Workspace.

Résoudre les problèmes liés à la détection d'altération des stratégies

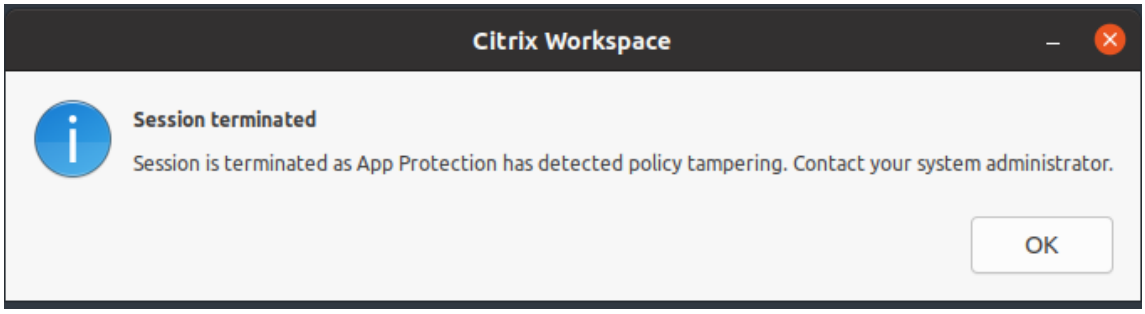
March 11, 2024

La section suivante décrit certains des problèmes que vous pouvez rencontrer et comment les résoudre :

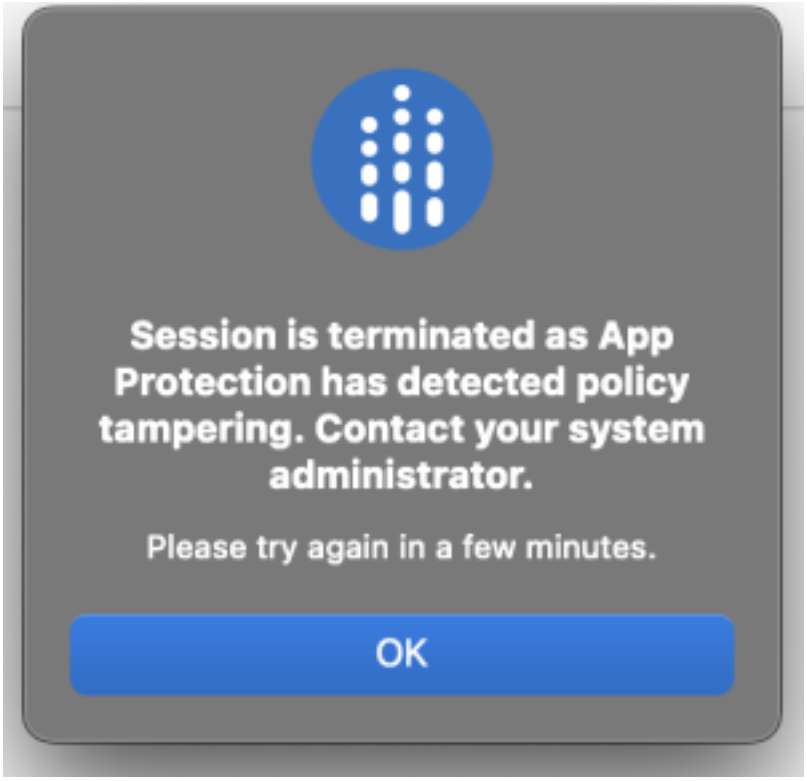
Le fichier ICA est altéré et la session est toujours en cours

Si le fichier ICA d'une application ou d'un bureau virtuel activé avec la fonctionnalité de détection d'altération des stratégies d'App Protection est altéré, la session doit être interrompue en affichant l'un des messages d'erreur suivants :

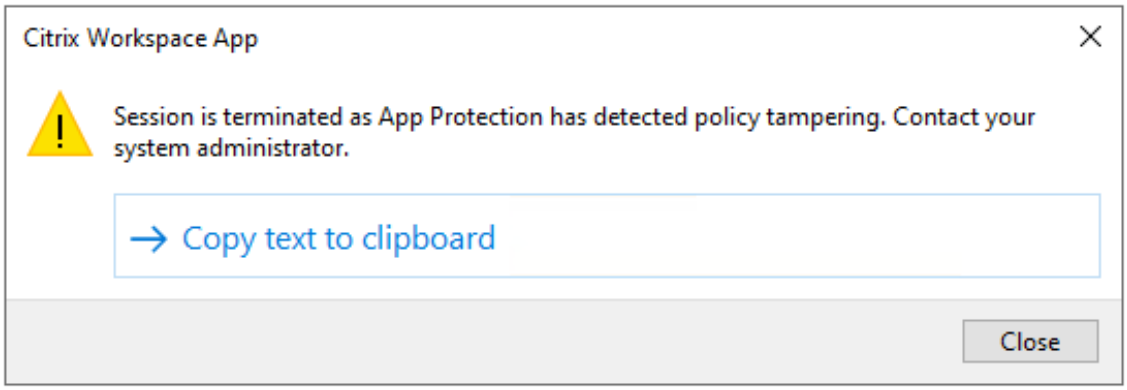
- Application Citrix Workspace pour Linux



- Application Citrix Workspace pour Mac



- Application Citrix Workspace pour Windows



Toutefois, si la session est en cours alors que le fichier .ica est altéré et que la détection d'altération des stratégies est activée, procédez comme suit :

1. Dans le Virtual Delivery Agent, procédez comme suit :

   a) Exécutez la commande suivante et vérifiez si le service `ctxappprotectionsv` est en cours d'exécution :

   ```
   sc query ctxappprotectionsvc
   ```


b) Si le service `ctxappprotectionsvc` n'est pas en cours d'exécution, procédez comme suit pour le démarrer :

i. Changez le type de démarrage du service `ctxappprotectionsvc` en mode automatique en exécutant la commande suivante :

```
sc config ctxappprotectionsvc start=auto
```

ii. Démarrez le service en exécutant la commande suivante :

```
sc start ctxappprotectionsvc
```

2. Dans le client, procédez comme suit :

a) Vérifiez si le fichier *vdappp.dll* se trouve à l'emplacement d'installation de l'application Citrix Workspace. L'emplacement d'installation par défaut de l'application Citrix Workspace est :

- Windows - C:\Program Files (x86)\Citrix\ICA Client
- Linux - /opt/Citrix/ICAClient
- Mac - Non applicable

b) Pour l'application Citrix Workspace pour Windows, utilisez *procexp.exe* et vérifiez si le fichier *vdappp.dll* est chargé dans *wfica32.exe*.

c) Pour l'application Citrix Workspace pour Linux, vérifiez si le fichier *vdappp.dll* est chargé dans *wfica.exe*.

3. Si la session est toujours en cours, collectez les journaux et contactez le support technique Citrix. Pour en savoir plus sur la collecte des journaux, consultez la section Collecte de journaux.

La fonction de détection d'altération des stratégies cesse de fonctionner après le redémarrage du Virtual Delivery Agent

Si vous redémarrez le Virtual Delivery Agent et que la fonctionnalité de détection d'altération des stratégies cesse de fonctionner, cela peut être dû au fait que le service App Protection ne fonctionne pas après le redémarrage. Procédez comme suit sur le Virtual Delivery Agent :

1. Exécutez la commande suivante et vérifiez si le service `ctxappprotectionsvc` est en cours d'exécution et s'il est réglé sur **automatique** :

```
sc query ctxappprotectionsvc
```

2. Si le service `ctxappprotectionsvc` n'est pas en cours d'exécution, procédez comme suit pour le démarrer :

a) Changez le type de démarrage du service `ctxappprotectionsvc`en mode **automatique** en exécutant la commande suivante :

```
sc config ctxappprotectionsvc start=auto
```

b) Démarrez le service en exécutant la commande suivante :

```
sc start ctxappprotectionsvc
```

3. Si la fonction de détection d'altération des stratégies ne fonctionne toujours pas, collectez les journaux et contactez le support technique Citrix. Pour en savoir plus sur la collecte des journaux, consultez la section Collecte de journaux.

Résolution des problèmes liés à App Protection Posture Check

March 11, 2024

La section suivante décrit certains des problèmes que vous pouvez rencontrer et comment les résoudre :

La session s'est terminée sans aucun message d'erreur

Si votre session d'application ou de bureau virtuel se termine brusquement sans afficher de message d'erreur, procédez comme suit :

1. Vérifiez si la version de votre application Citrix Workspace est antérieure à l'une des versions suivantes :

   - Application Citrix Workspace pour Windows 2309
   - Application Citrix Workspace pour Mac 2308
   - Application Citrix Workspace pour Linux 2308

   > **Remarque :**
   >
   > Si la version de l'application Citrix Workspace est antérieure aux versions répertoriées à l'étape 1 et que la fonctionnalité de vérification de l'état d'App Protection est activée, la session d'application ou de bureau virtuel se termine sans afficher de message d'erreur. Toutefois, si la version de l'application Citrix Workspace est ultérieure ou égale aux versions répertoriées à l'étape 1 et que la fonction App Protection Posture Check est activée, la session Virtual Apps or Desktop se termine et un message d'erreur apparaît.

2. Vérifiez si la fonction App Protection Posture Check est activée.

3. Si la version de l'application Citrix Workspace est ultérieure ou égale aux versions précédentes et que la fonction Posture Check est également active, collectez les journaux et contactez le support technique Citrix. Pour en savoir plus sur la collecte des journaux, consultez la section Collecte de journaux.

La fonction App Protection Posture Check est activée, mais la session n'est pas interrompue pour les anciennes versions

En règle générale, si la fonction App Protection Posture Check est activée et que vous vous connectez via une ancienne version de l'application Citrix Workspace, la session doit être interrompue.

Si la session n'est toutefois pas interrompue, procédez comme suit :

1. Dans le Virtual Delivery Agent, procédez comme suit :

    a) Exécutez la commande suivante et vérifiez si le service `ctxappprotectionsvc` est en cours d'exécution :

    ```
    sc query ctxappprotectionsvc
    ```

    b) Si le service `ctxappprotectionsvc` n'est pas en cours d'exécution, procédez comme suit pour démarrer le service :

        i. Changez le type de démarrage du `ctxappprotectionsvc service` en **automatique** en exécutant la commande suivante :

        ```
        sc config ctxappprotectionsvc start=auto
        ```

        ii. Démarrez le service en exécutant la commande suivante :

        ```
        sc start ctxappprotectionsvc
        ```

2. Vérifiez si les valeurs de vérification de l'état que vous avez saisies comportent l'un des préfixes suivants :

    - Pour l'application Citrix Workspace pour Windows, `windows-`
    - Pour l'application Citrix Workspace pour Linux, `linux-`
    - Pour l'application Citrix Workspace pour Mac, `mac-`

3. Vérifiez si les valeurs de la fonction Posture Check sont correctement ajoutées en fonction de la plate-forme concernée.

4. Vérifiez l'emplacement `reg` (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) pour vérifier si la fonctionnalité de vérification de l'état est synchronisée avec le Virtual Delivery Agent.

5. Si toutes les conditions précédentes sont remplies et que la session est toujours connectée pour les anciennes versions de l'application Citrix Workspace, collectez les journaux et contactez le support technique Citrix. Pour en savoir plus sur la collecte des journaux, consultez la section Collecte de journaux.

La fonction App Protection Posture Check fonctionne sur une plate-forme, mais ne fonctionne pas sur une autre

Parfois, la fonction App Protection Posture Check peut fonctionner sur une plate-forme, mais pas sur une autre. Par exemple, la fonctionnalité de vérification de l'état d'App Protection fonctionne sur l'application Citrix Workspace pour Windows, mais pas sur l'application Citrix Workspace pour Linux.

Dans de tels scénarios, procédez comme suit :

1. Vérifiez si les valeurs de vérification de l'état que vous avez saisies comportent l'un des préfixes suivants :
   - Pour l'application Citrix Workspace pour Windows, `windows-`
   - Pour l'application Citrix Workspace pour Linux, `linux-`
   - Pour l'application Citrix Workspace pour Mac, `mac-`
2. Vérifiez si les valeurs de la fonction Posture Check sont correctement ajoutées en fonction de la plate-forme concernée.
3. Vérifiez l'emplacement `reg` (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) sur le Virtual Delivery Agent pour vérifier si la fonctionnalité de vérification de l'état est synchronisée avec le Virtual Delivery Agent. Ils doivent correspondre à ce qui a été configuré dans Studio.
4. Si toutes les conditions précédentes sont remplies et que la session est toujours connectée pour les anciennes versions de l'application Citrix Workspace, collectez les journaux et contactez le support technique Citrix. Pour en savoir plus sur la collecte des journaux, consultez la section Collecte de journaux.

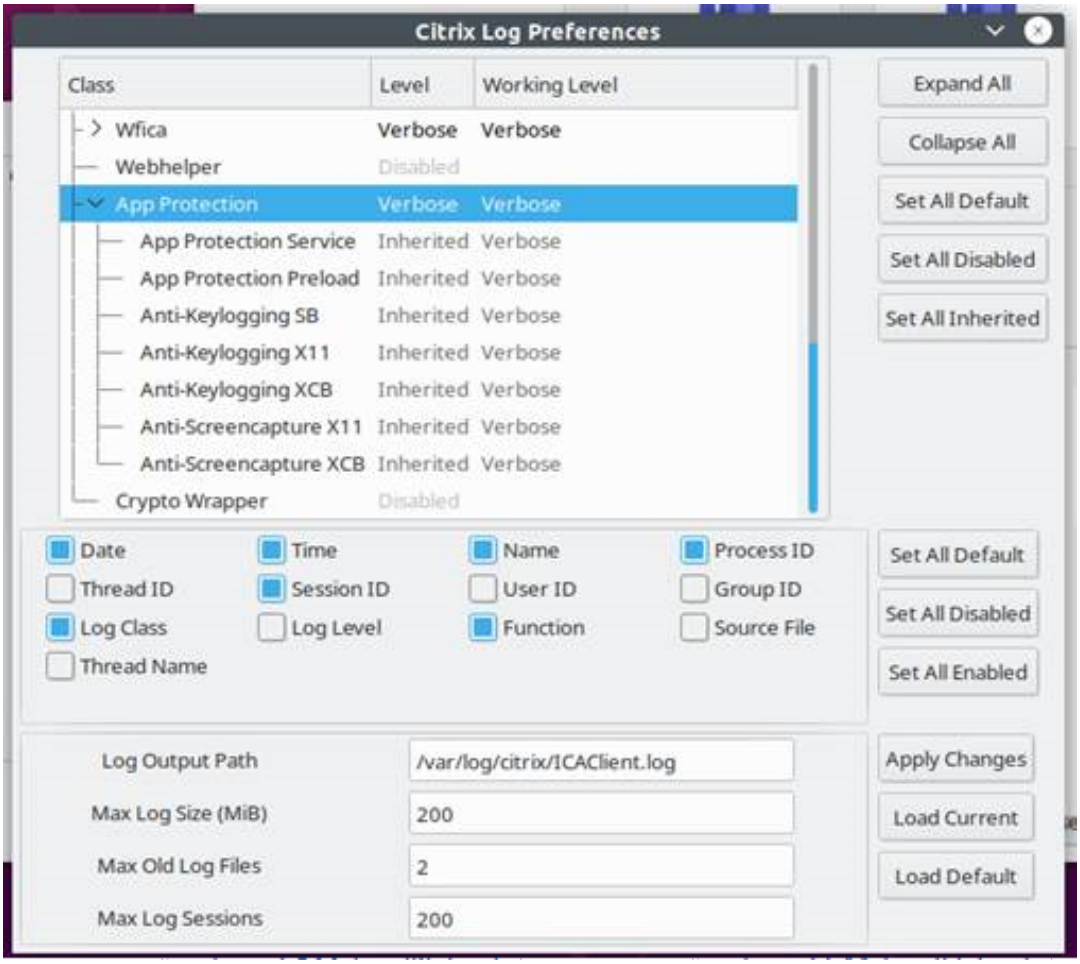
Collecte de journaux

March 11, 2024

- Pour collecter des journaux pour l'application Citrix Workspace pour Windows, consultez la section Collecte de journaux pour Windows.

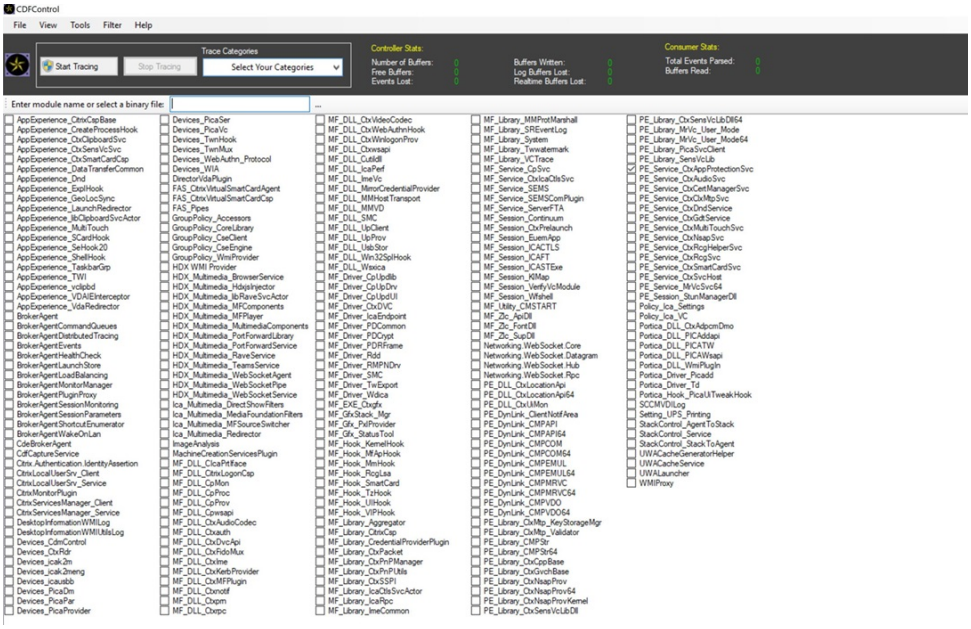
- Pour collecter des journaux pour l'application Citrix Workspace pour Mac, consultez la section Collecte de journaux pour Mac.
- Pour collecter des journaux pour l'application Citrix Workspace pour Linux, procédez comme suit :

  1. Exécutez le fichier exécutable set log qui se trouve dans le répertoire *util* de l'installation. Par exemple, */opt/Citrix/ICAClient/util/setlog*.
  2. (Facultatif) Cliquez sur **Tout désactiver** et assurez-vous que seuls les journaux requis sont collectés.
  3. Accédez à la journalisation de la App Protection.
  4. Définissez le niveau de journalisation d'App Protection sur Détaillé en cliquant avec le bouton droit de la souris et en sélectionnant **Détaillé** (seuls les avertissements et les erreurs sont enregistrés dans le journal).
  5. Développez la classe App Protection et cliquez avec le bouton droit sur son élément enfant. Sélectionnez **Groupe** > **Hérité**.
  6. Utilisez l'utilitaire de journalisation Linux (depuis le *répertoire d'installation*, lancez *util/setlog*) et définissez le niveau de journalisation du canal virtuel sur Détaillé.
  7. Activez les journaux pour **wfica**. Cliquez avec le bouton droit sur **wfica** et sélectionnez **Détaillé**. Si App Protection n'est pas installée ou n'est pas détectable par **wfica**, vous obtenez le journal **[NCS] < P3563 > citrix-wfica: App Protection is not installed**.
  8. Cliquez sur **wfica** et modifiez le niveau de journalisation du **pilote winstation** en **Détaillé**.
  9. Lorsque vous lancez la session, les journaux sont enregistrés dans le fichier mentionné dans le chemin de sortie du journal défini.



- Pour collecter des journaux pour le Virtual Delivery Agent, procédez comme suit :

  1. Pour obtenir des traces du service App Protection via le contrôle CDF, sélectionnez tous les modules.



2. Dans certains cas, nous devons capturer des traces CDF à partir d'une autre machine. Pour collecter des traces CDF, voir CTX237216.

App Protection contextuelle pour Workspace

March 11, 2024

La protection contextuelle des applications offre la flexibilité d'appliquer les stratégies de protection des applications de manière conditionnelle à un sous-ensemble d'utilisateurs, en fonction des utilisateurs, de leur appareil et de la position du réseau.

Mise en œuvre de la App Protection contextuelle

Vous pouvez mettre en œuvre l'App Protection contextuelle à l'aide des filtres de connexion définis dans la règle de stratégie Broker Access. Les stratégies Broker Access définissent les règles qui contrôlent l'accès d'un utilisateur aux groupes de mise à disposition. La stratégie comprend un ensemble de règles. Chaque règle se rapporte à un seul groupe de mise à disposition et contient un ensemble de filtres de connexion et de contrôles de droits d'accès.

Les utilisateurs ont accès à un groupe de mise à disposition lorsque les détails de leur connexion correspondent aux filtres de connexion d'une ou de plusieurs règles de la stratégie Broker Access. Par défaut, les utilisateurs n'ont accès à aucun groupe de mise à disposition au sein d'un site. Vous pouvez créer des stratégies Broker Access supplémentaires en fonction des exigences. Plusieurs règles

peuvent s'appliquer au même groupe de mise à disposition. Pour en savoir plus, consultez New-BrokerAccessPolicyRule.

Les paramètres suivants de la règle de stratégie Broker Access permettent d'activer App Protection de manière contextuelle si la connexion de l'utilisateur correspond aux filtres de connexion définis dans la règle de stratégie d'accès :

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

Utilisez les stratégies Smart Access référencées dans les règles de stratégie Broker Access pour affiner les filtres de connexion. Reportez-vous aux scénarios mentionnés dans cet article pour comprendre comment utiliser les stratégies Smart Access pour configurer App Protection contextuelle.

Scénarios d'App Protection contextuelle

Voici certains des scénarios permettant d'activer App Protection contextuelle :

- Activer App Protection pour les utilisateurs externes via Access Gateway
- Activer App Protection pour les appareils non sécurisés
- Activer App Protection en fonction des résultats de la Posture de l'appareil
- Activer App Protection pour des groupes d'utilisateurs spécifiques

Logiciels requis

March 11, 2024

Assurez-vous que vous disposez des éléments suivants :

- Service d'emplacement réseau (NLS, Network Location Service) pour les scénarios basés sur l'emplacement réseau de l'utilisateur
- Configuration requise pour le système de licences
  - Protection des applications pour DaaS
  - Droit d'accès à l'authentification adaptative pour les scénarios avec des stratégies Smart Access

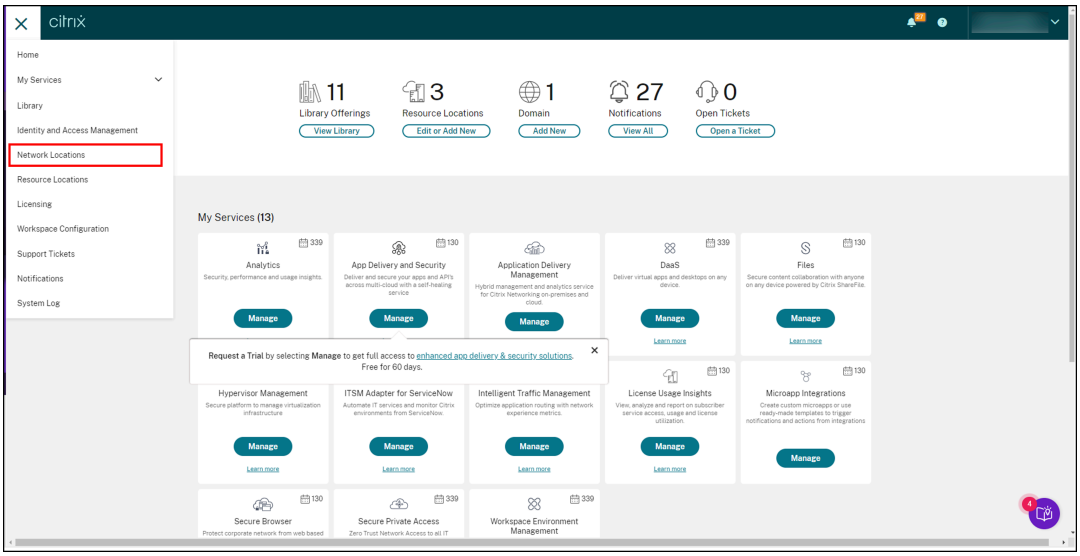
Scénario 1

April 10, 2024

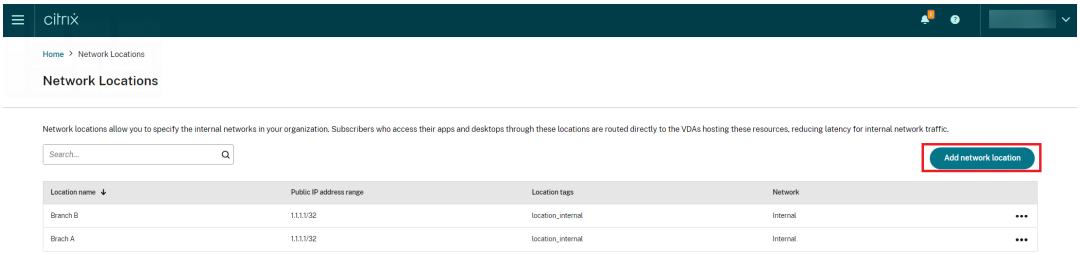
Ce scénario explique comment activer App Protection pour les utilisateurs externes via Access Gateway.

1. Configurez l'authentification adaptative.
2. Configurez l'accès adaptatif en fonction de l'emplacement de votre réseau.

   a) Connectez-vous à Citrix Cloud et cliquez sur **Emplacements réseau**.



   b) Cliquez sur **Ajouter un emplacement réseau**.



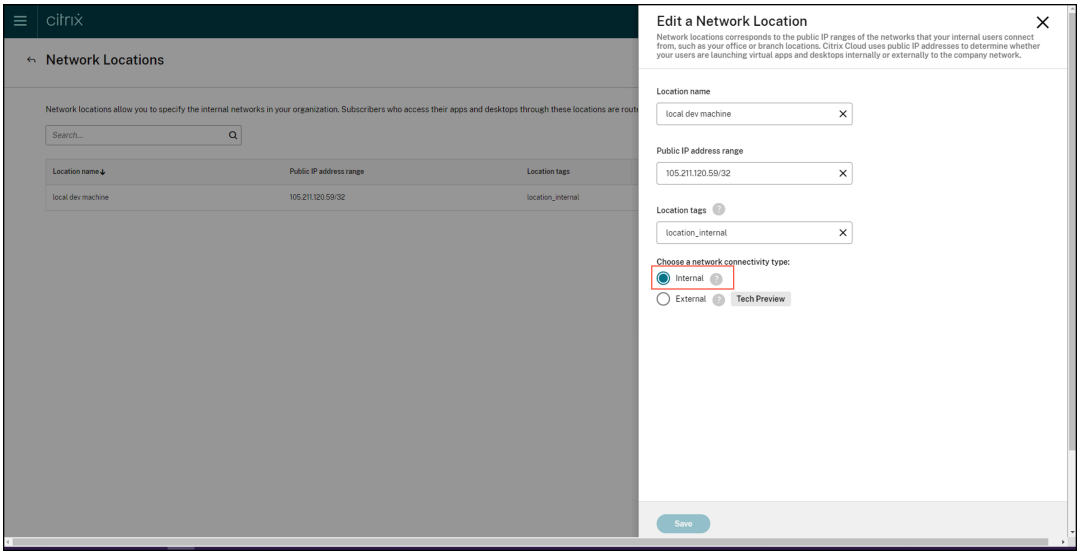
   L'écran **Ajouter un emplacement réseau** apparaît.

   c) Dans le champ **Nom de l'emplacement**, indiquez le nom de l'emplacement approprié.

   d) Dans le champ **Plage d'adresses IP publiques**, indiquez l'adresse IP réseau ou le sous-réseau que vous souhaitez considérer comme un réseau interne.

   e) Indiquez **location_internal** dans le champ **Balises d'emplacement**. Pour en savoir plus sur la balise d'emplacement, consultez la section Balises d'emplacement.

   f) Sous **Choisir un type de connectivité réseau**, sélectionnez *Interne*.



Si vous vous connectez au Cloud Store à partir d'un appareil dont l'adresse IP est configurée comme *interne* sous le paramètre **Choisir un type de connectivité réseau**, la connexion sera considérée comme une connexion interne.

3. Configurer les règles de stratégies Broker Access

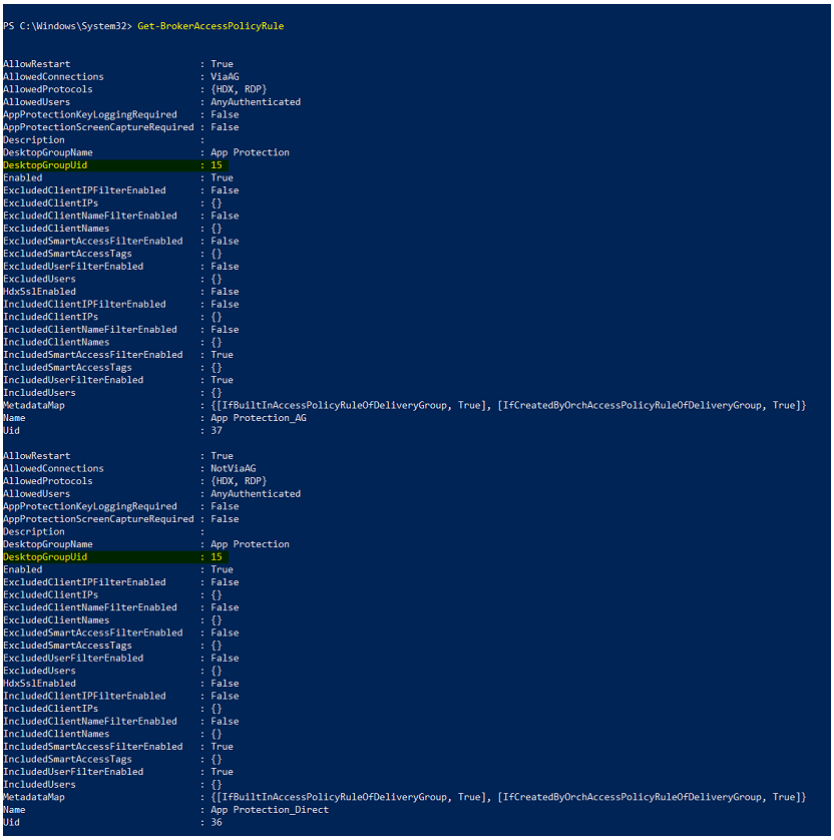
   Pour chaque groupe de mise à disposition, deux stratégies Broker Access sont créées par défaut. L'une des stratégies concerne les connexions passant par Access Gateway et l'autre les connexions directes. Vous pouvez activer App Protection uniquement pour les connexions passant par Access Gateway, c'est-à-dire les connexions externes. Suivez les étapes suivantes pour configurer les règles de stratégies Broker Access :

   a) Installez le SDK Citrix PowerShell et connectez-vous à l'API cloud comme expliqué sur la page Citrix Blog Getting started with PowerShell automation for Citrix Cloud.

   b) Exécutez la commande `Get-BrokerAccessPolicyRule`.

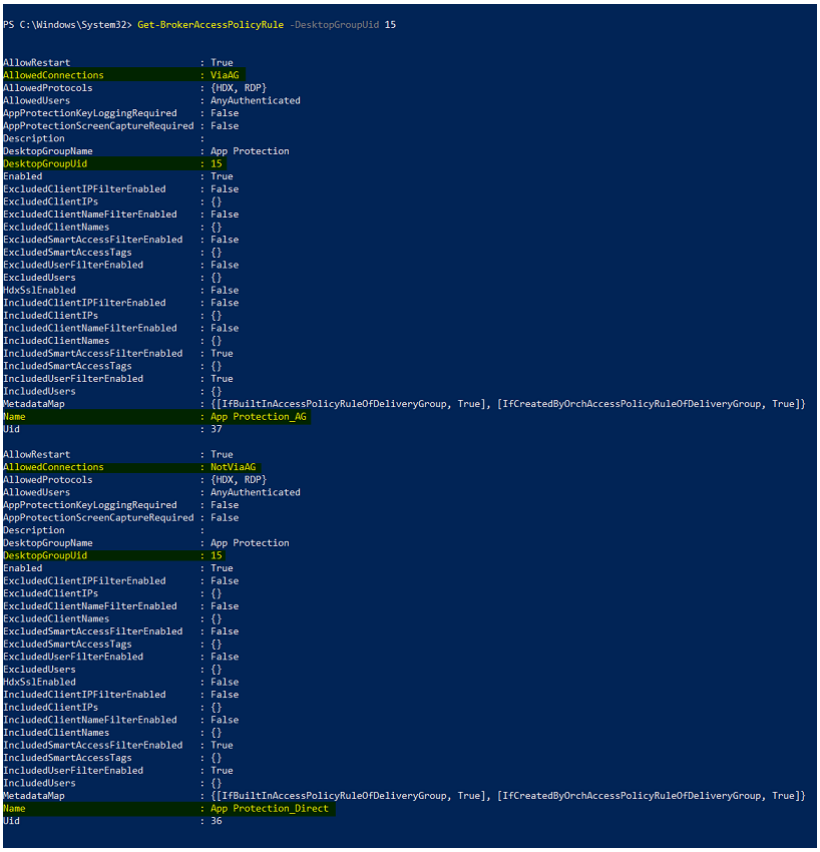
      Une liste de toutes les stratégies Broker Access pour tous les groupes de mise à disposition présents s'affiche.

   c) Recherchez le paramètre **DesktopGroupUid** pour le groupe de mise à disposition que vous souhaitez modifier.



d) Exécutez la commande suivante à l'aide de **DesktopGroupUid** pour récupérer les stratégies applicables au groupe de mise à disposition. Il existe au moins deux stratégies, l'une avec le paramètre *AllowedConnections* défini sur *ViaAG* et l'autre avec *NotViaAG*.

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 15
```

Sur la capture d'écran, vous pouvez voir deux stratégies :

- App Protection_AG - *AllowedConnections* avec *ViaAG*, qui est la stratégie de connexion via Access Gateway
- App Protection_Direct —*AllowedConnections* avec *NotViaAG*, qui est la stratégie de connexion sans Access Gateway

4. Activez les stratégies App Protection uniquement pour les connexions externes et désactivez-les pour les connexions internes à l'aide des commandes suivantes :

- `Set-BrokerAccessPolicyRule "App Protection_AG"-IncludedSmartAccessFilt $true -IncludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $false -AppProtectionKeyLoggingRequ $false`
- `New-BrokerAccessPolicyRule "App Protection_AG_Exclude"-ExcludedsmartAc $true -ExcludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $true -AppProtectionKeyLoggingRequi $true -DesktopGroupUid 15 -AllowedConnections ViaAG -AllowedProtocols HDX, RDP`
- `Remove-BrokerAccessPolicyRule "App Protection_Direct”`

5. Vérification :

   Déconnectez-vous de l'application Citrix Workspace, puis reconnectez-vous. Lancez la ressource protégée à partir d'une connexion externe. Notez que les stratégies de protection des applications sont appliquées. Lancez la même ressource à partir d'une connexion interne, un appareil appartenant à la plage d'adresses IP configurée lors de la première étape. Notez que les stratégies App Protection sont désactivées.

Scénario 2

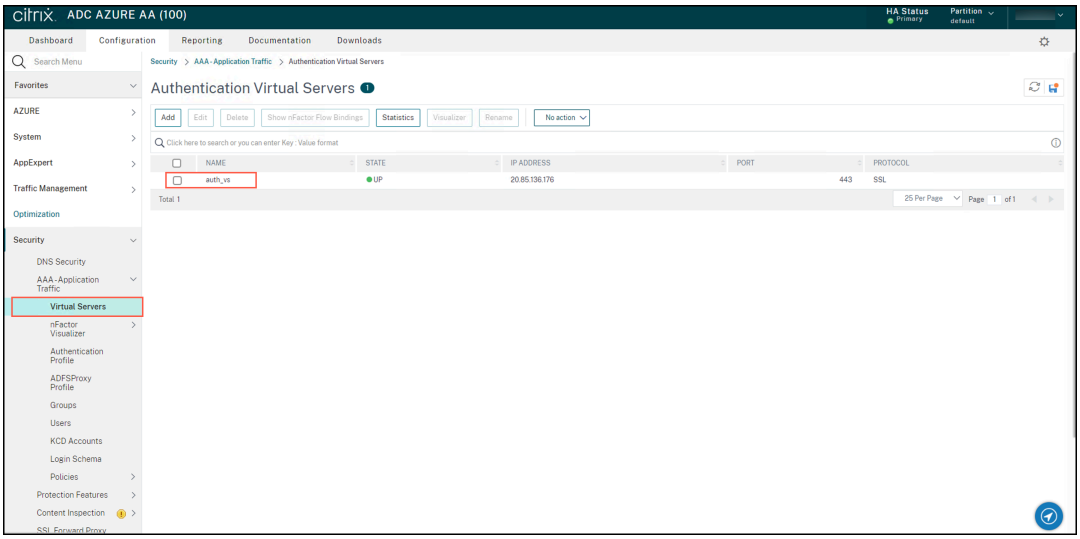
April 10, 2024

Ce scénario explique comment activer App Protection pour les appareils non sécurisés.

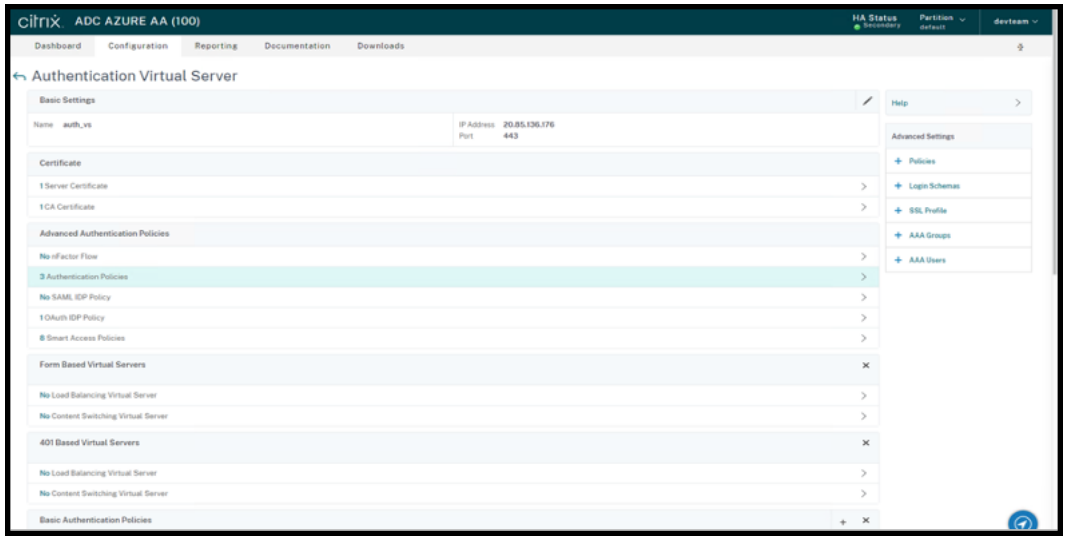
Il existe plusieurs définitions des appareils fiables et non fiables. Pour ce scénario, considérons qu'un appareil est fiable si l'analyse EPA (Endpoint Analysis) est réussie. Tous les autres appareils sont considérés comme des appareils non fiables.

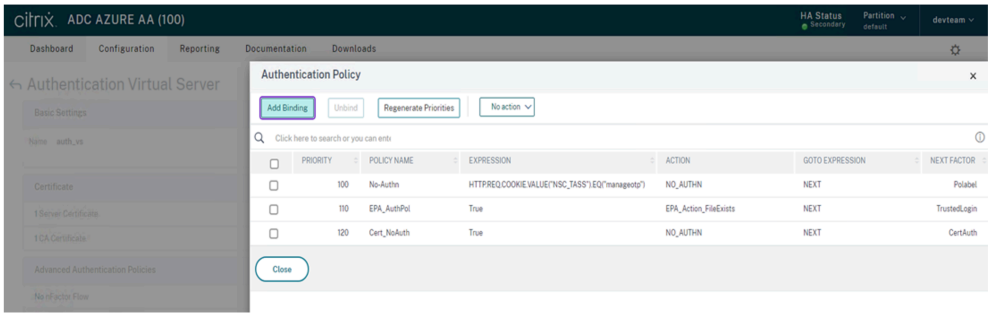
1. Configurez l'authentification adaptative.
2. Créez une stratégie d'authentification avec une analyse EPA en suivant les étapes suivantes :

   a) Connectez-vous à l'interface utilisateur ADC Administration de Citrix. Dans l'onglet **Configuration**, cliquez sur **Sécurité > AAA-Application Traffic > Serveurs virtuels**. Cliquez sur le serveur virtuel que vous souhaitez utiliser, *auth_vs* dans ce cas-ci.

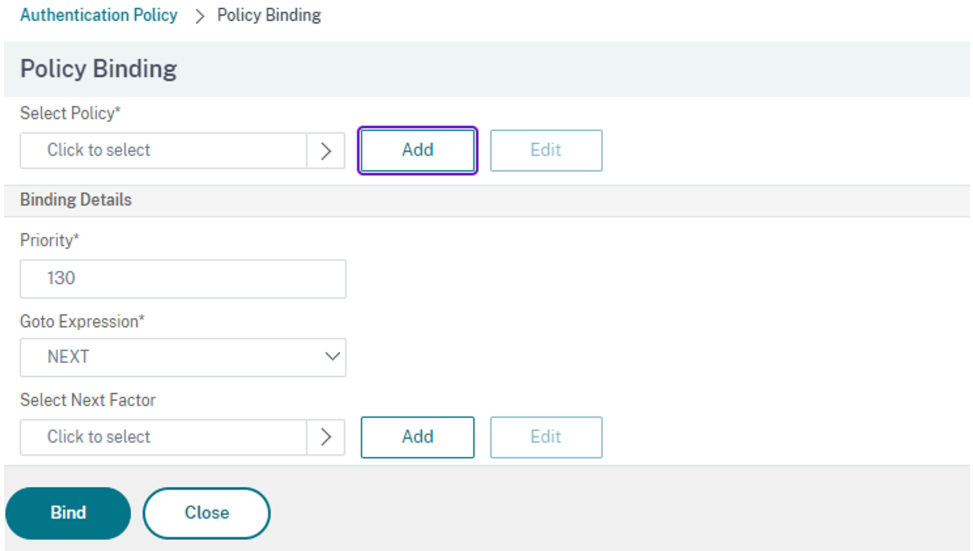


   b) Accédez à **Authentication Policies > Add Binding**.

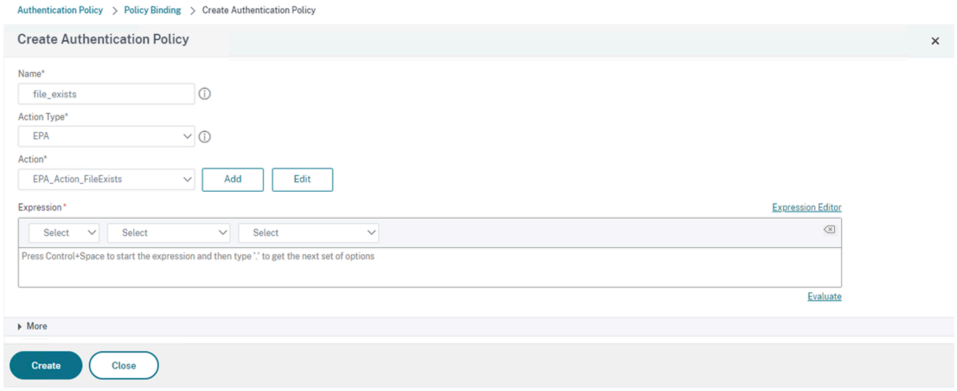




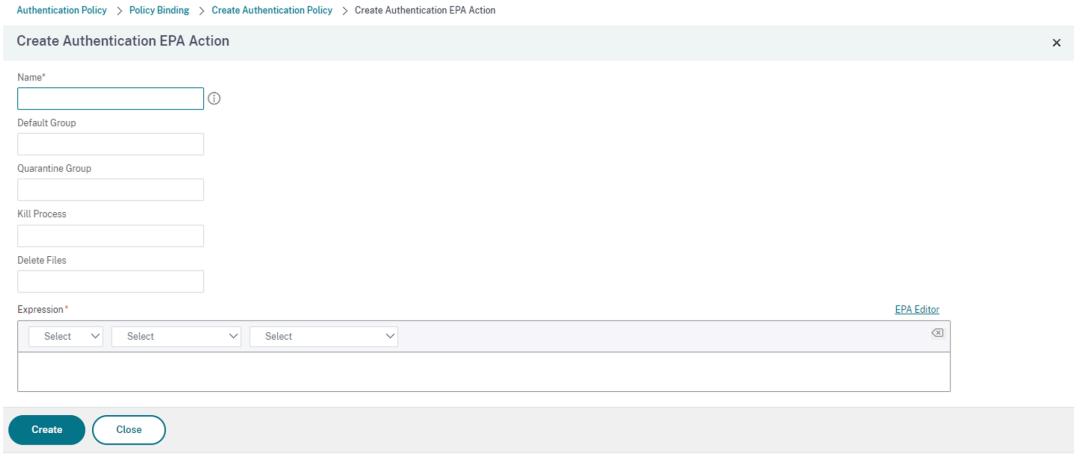
c) Cliquez sur **Add** pour créer une stratégie.



d) Créez une stratégie d'authentification basée sur l'analyse EPA. Entrez le nom de la stratégie. Définissez **Action Type** sur *EPA*. Cliquez sur **Add** pour créer une action.



L'écran **Créer une action d'analyse de point de terminaison d'authentification** s'affiche.

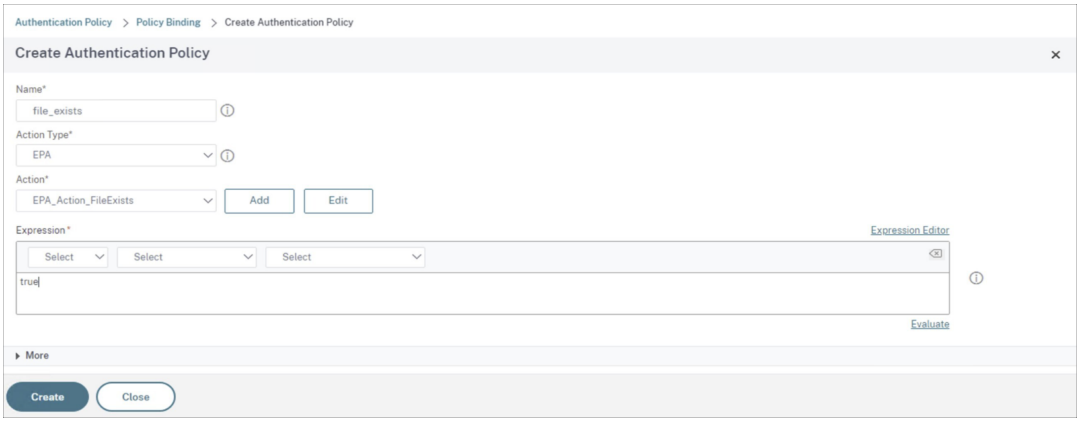


e) Sur l'écran **Créer une action d'analyse de point de terminaison d'authentification**, indiquez les informations suivantes et cliquez sur **Créer** pour créer une action :

- **Nom** : nom de l'action d'analyse de point de terminaison. Dans ce cas, *EPA_Action_FileExists*.
- **Groupe par défaut** : indiquez le nom du groupe par défaut. Si le paramètre « EPA expression » est défini sur *True*, les utilisateurs sont ajoutés au groupe par défaut. Dans ce cas, **Default Group** est défini sur *FileExists*.
- **Groupe de quarantaine** : indiquez le nom du groupe de quarantaine. Si le paramètre « EPA expression » est défini sur *False*, les utilisateurs sont ajoutés au groupe de quarantaine.
- **Expression** : ajoutez l'expression d'analyse de point de terminaison que vous souhaitez analyser. Dans cet exemple, nous considérons que l'analyse EPA est réussie si un fichier particulier est présent : `sys.client_expr("file_0_C:\\\\\epa\\\\\avinstalled.txt")`

Revenez à l'écran **Create Authentication Policy**.

f) Entrez **true** dans la zone Expression Editor, puis cliquez sur **Create**.



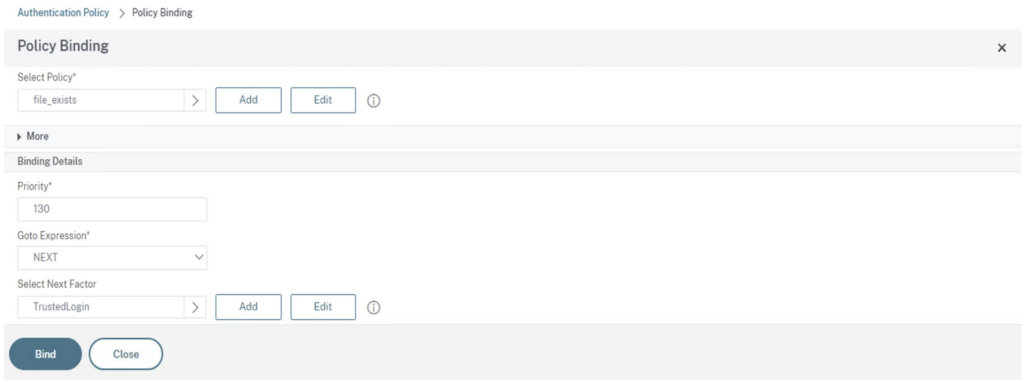
Revenez à l'écran **Policy Binding**.

g) Sur l'écran **Liaison de stratégie**, procédez comme suit :

i. Définissez **Goto Expression** sur **NEXT**.

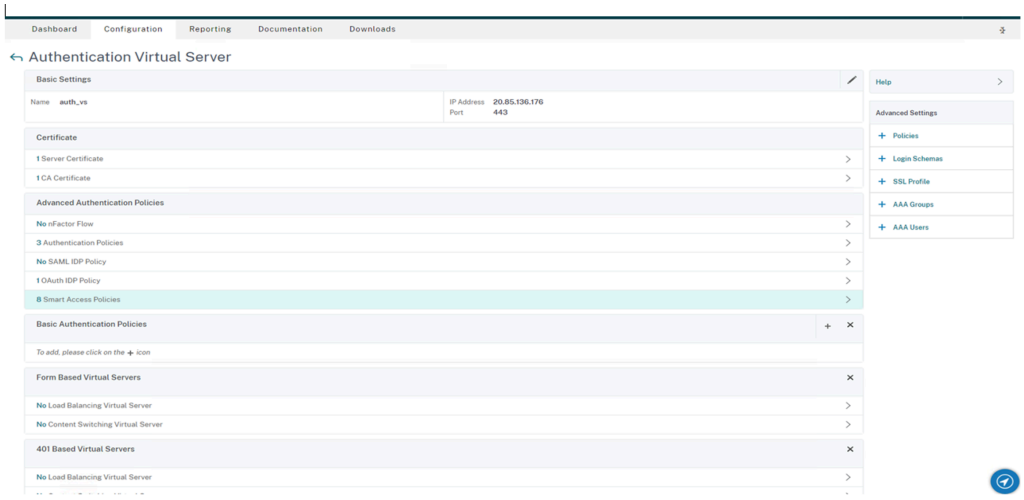
ii. Dans la section **Select Next Factor**, sélectionnez la stratégie LDAP que vous avez configurée pour l'authentification dans ADC (Application Delivery Controller).

iii. Cliquez sur **Bind**.

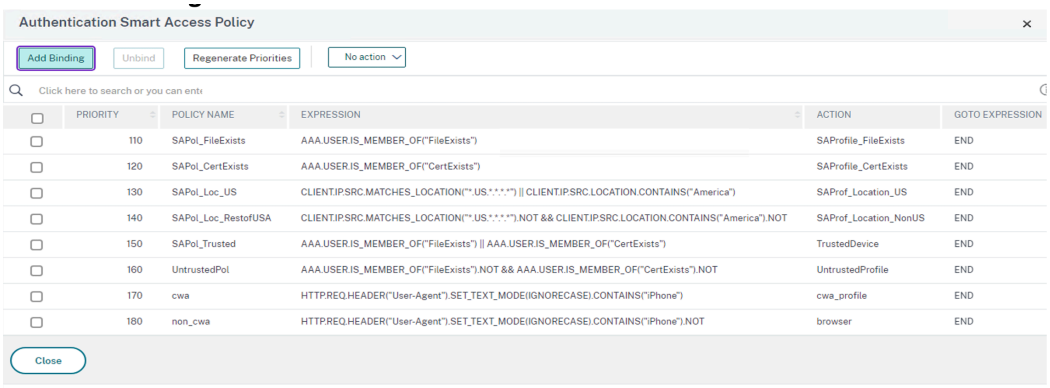


3. Créer une stratégie Smart Access pour les appareils sécurisés :

a) Sélectionnez **Smart Access Policies** sur la page **Authentication Virtual Server** du serveur *auth_vs*.

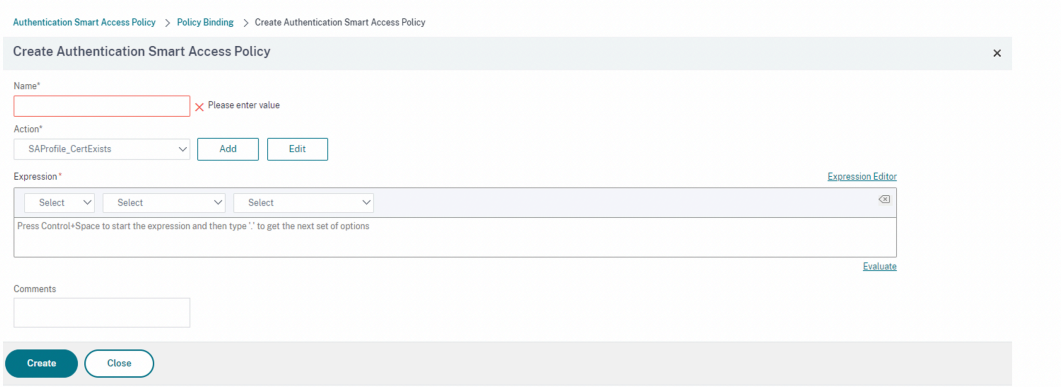


b) Cliquez sur **Add Binding**.



c) Sur l'écran **Policy Binding**, cliquez sur **Add** dans la section **Select Policy**.

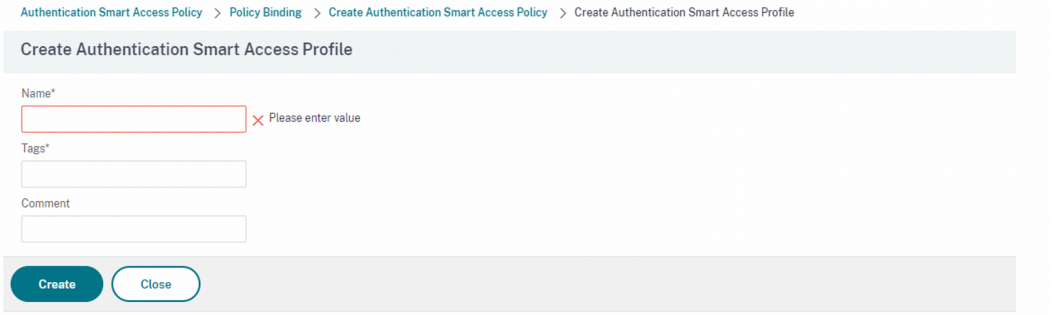
L'écran **Create Authentication Smart Access Policy** s'affiche.



d) Sur l'écran **Create Authentication Smart Access Policy**, sous **Name**, donnez un nom à la stratégie Smart Access et cliquez sur **Add** pour créer un profil Smart Access.

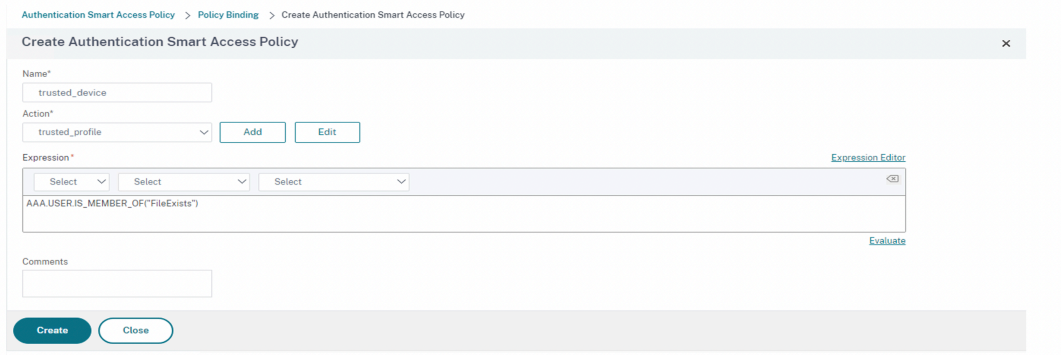
L'écran **Create Authentication Smart Access Profile** s'affiche.

e) Sous **Name**, ajoutez le nom de l'action. Entrez *trusted* dans le champ **Tags**. La balise est ensuite référencée dans la règle Broker Access Policy pour la configuration. Cliquez sur **Créer**.



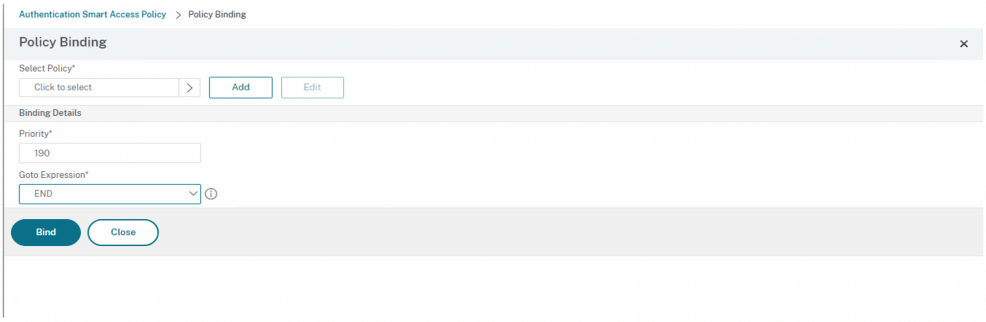
Revenez à l'écran **Create Authentication Smart Access Policy**.

f) Dans la section **Expression**, indiquez l'expression pour laquelle vous souhaitez intégrer la balise. Dans ce cas, la balise étant intégrées dans des appareils sécurisés, indiquez `AAA.USER.IS_MEMBER_OF("FileExists")`. Cliquez sur **Créer**.



Revenez à l'écran **Policy Binding**.

g) Sélectionnez **Goto Expression** comme *End*, puis cliquez sur **Lier**.



4. Créez une stratégie Smart Access pour les appareils non sécurisés :

   a) Suivez les instructions de l'étape précédente, à l'exception des sous-étapes **v** et **vi**.

   b) Pour la sous-étape **v**, sur l'écran **Create Authentication Smart Access Profile**, sous **Name**, ajoutez le nom de l'action. Entrez *untrusted* dans le champ **Tags**. La balise est ensuite référencée dans la règle Broker Access Policy pour la configuration. Cliquez sur **Créer**.

   c) Pour la sous-étape **vi**, dans la section **Expression** de l'écran **Create Authentication Smart Access Policy**, entrez l'expression pour laquelle vous souhaitez transmettre la balise. Dans ce cas, la balise étant intégrées dans des appareils non sécurisés, indiquez `AAA.USER.IS_MEMBER_OF("FileExists").NOT`.

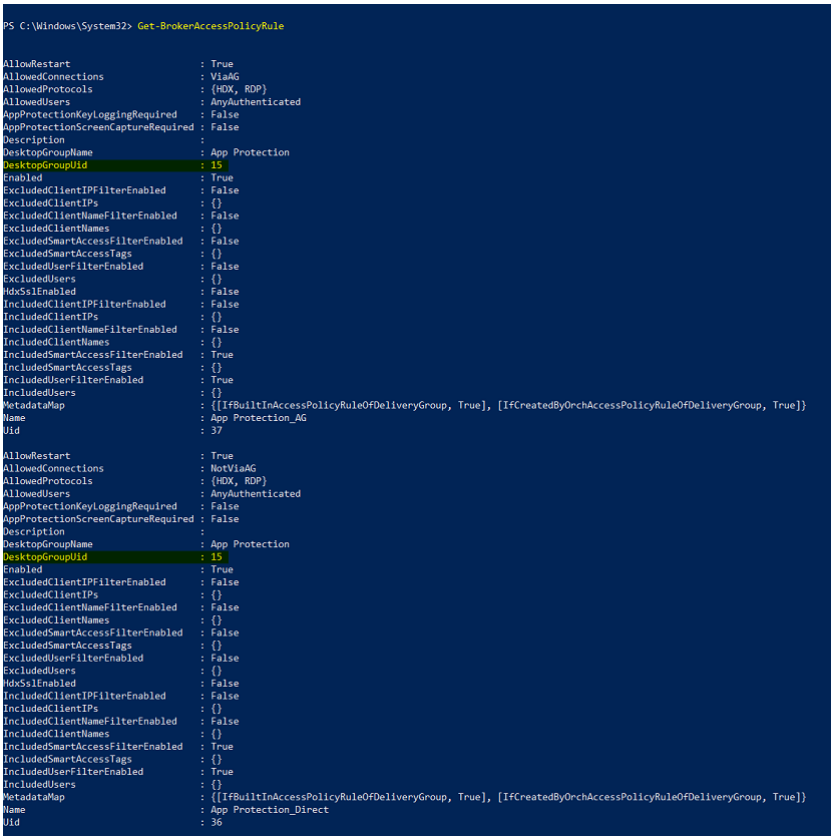
5. Configurez les règles de stratégies Broker Access.

   a) Installez le SDK Citrix PowerShell et connectez-vous à l'API cloud comme expliqué sur la page Citrix Blog Getting started with PowerShell automation for Citrix Cloud.

   b) Exécutez la commande `Get-BrokerAccessPolicyRule`.

   Une liste de toutes les stratégies Broker Access pour tous les groupes de mise à disposition présents s'affiche.

   c) Recherchez le paramètre **DesktopGroupUid** pour le groupe de mise à disposition que vous souhaitez modifier.



d) Obtenez les stratégies qui s'appliquent uniquement à un groupe de mise à disposition spécifique à l'aide de la commande :

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) Pour filtrer les utilisateurs utilisant des appareils sécurisés, créez une autre stratégie Broker Access à l'aide de la commande suivante :

```
New-BrokerAccessPolicyRule -Name CAP_Desktops_AG_Trusted-
DesktopGroupUid 7 - AllowedConnections ViaAG -AllowedProtocols
 HDX, RDP -AllowedUsers AnyAuthenticated - AllowRestart $true
 -Enabled $true-IncludedSmartAccessFilterEnabled $true
```

f) Pour désactiver App Protection pour les appareils sécurisés et activer App Protection pour les appareils non sécurisés, utilisez la commande suivante :

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG_trusted -IncludedSmartAcces
 Workspace:trusted -AppProtectionKeyLoggingRequired $false -
AppProtectionScreenCaptureRequired $false
```

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG -IncludedSmartAccessTags
 Workspace:untrusted -AppProtectionKeyLoggingRequired $true -
AppProtectionScreenCaptureRequired $true
```


6. Vérification :

   Déconnectez-vous de l'application Citrix Workspace, puis reconnectez-vous. Lancez la ressource protégée à partir d'un appareil fiable qui répond aux conditions d'analyse EPA. Notez que les stratégies App Protection ne sont pas appliquées. Lancez la même ressource à partir d'un appareil non fiable. Notez que les stratégies App Protection sont appliquées.

Scénario 3

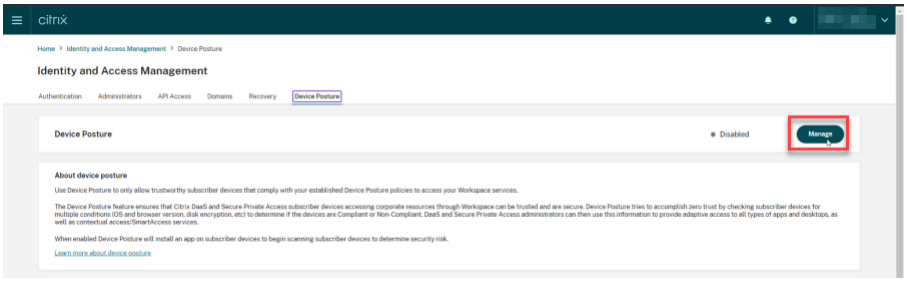
March 11, 2024

Ce scénario explique comment activer App Protection en fonction des résultats de la Posture de l'appareil.

1. Configurer le service Posture de l'appareil :

   a) Connectez-vous à Citrix Cloud.

   b) Cliquez sur **Gestion des identités et des accès** > **Posture de l'appareil**, puis sur **Gérer**.

   c) Cliquez sur **Créer une stratégie pour l'appareil**.

      La page **Créer une stratégie pour l'appareil** s'affiche.

   d) Sous **Règles de stratégie**, cliquez sur le menu déroulant **Sélectionner une règle**, puis sélectionnez *Version de l'application Citrix Workspace*.

   e) Cliquez sur le menu déroulant **Sélectionner une règle**, puis sélectionnez *Supérieur ou égal à >=*.

   f) Indiquez la version de l'application Citrix Workspace que vous souhaitez définir comme condition. Dans cet exemple, il s'agit de la version *23.7.0.19*.

   g) Sous **Résultat de la stratégie**, sélectionnez **Compatible**.

   h) Dans le champ **Nom**, indiquez le nom de la stratégie.

   i) Dans le champ **Priorité**, indiquez la priorité de la stratégie.

j) Cochez la case **Activer lors de la création** pour activer la stratégie lors de sa création.

k) Cliquez sur **Créer**.

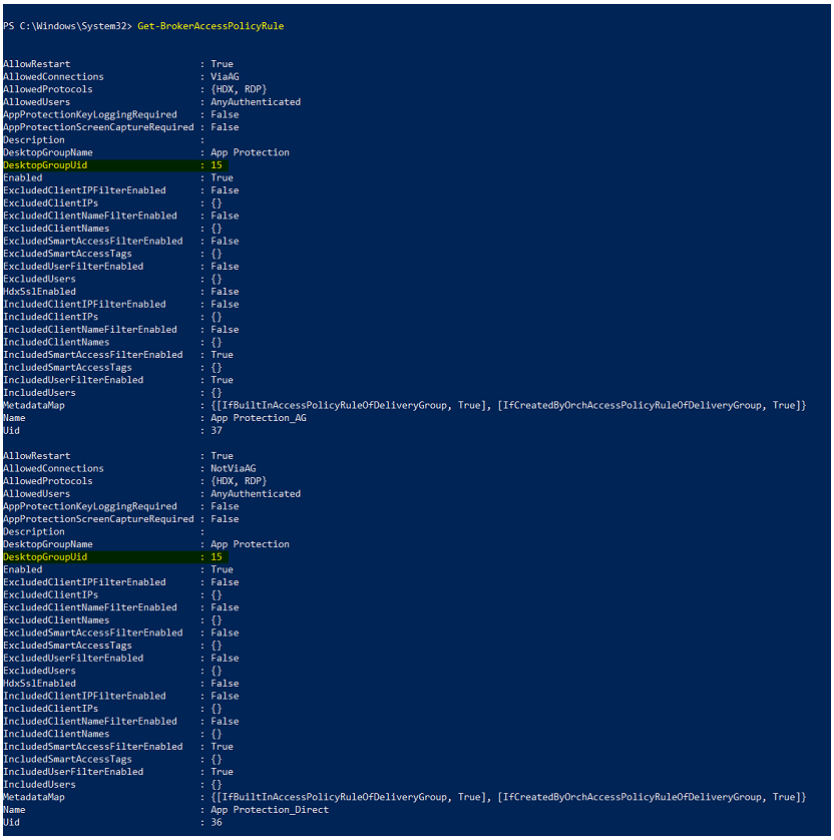
2. Configurez les règles de stratégies Broker Access.

a) Installez le SDK Citrix PowerShell et connectez-vous à l'API cloud comme expliqué sur la page Citrix Blog Getting started with PowerShell automation for Citrix Cloud.

b) Exécutez la commande `Get-BrokerAccessPolicyRule`.

Une liste de toutes les stratégies Broker Access pour tous les groupes de mise à disposition présents s'affiche.

c) Recherchez le paramètre **DesktopGroupUid** pour le groupe de mise à disposition que vous souhaitez modifier.



d) Obtenez les stratégies qui s'appliquent uniquement à un groupe de mise à disposition spécifique à l'aide de la commande :

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) Pour appliquer App Protection aux appareils compatibles, exécutez la commande suivante :


```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG"-IncludedSmartAccessFilterEnabled $true -IncludedSmartAccess
 Workspace:COMPLIANT
```

f) Pour appliquer App Protection aux appareils non compatibles, exécutez la commande suivante :

```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG_NonCompliant"-DesktopGroupUid 7 -AllowedConnections
 ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
 $true -ExcludedSmartAccessFilterEnabled $true -ExcludedSmartAccessTag
 Workspace:COMPLIANT-IncludedSmartAccessFilterEnabled $true
```

3. Vérification :

   Déconnectez-vous de l'application Citrix Workspace. Connectez-vous à partir d'une version de l'application Citrix Workspace compatible avec la stratégie de l'appareil. Notez que les stratégies App Protection ne sont pas appliquées. Déconnectez-vous à nouveau de l'application Citrix Workspace et connectez-vous à partir d'une version de l'application Citrix Workspace non compatible avec la stratégie de l'appareil. Notez que les stratégies App Protection sont appliquées.

Scénario 4

March 11, 2024

Ce scénario explique comment activer App Protection pour des groupes d'utilisateurs spécifiques.

Les étapes suivantes vous permettent d'activer App Protection pour les utilisateurs d'un groupe spécifique :

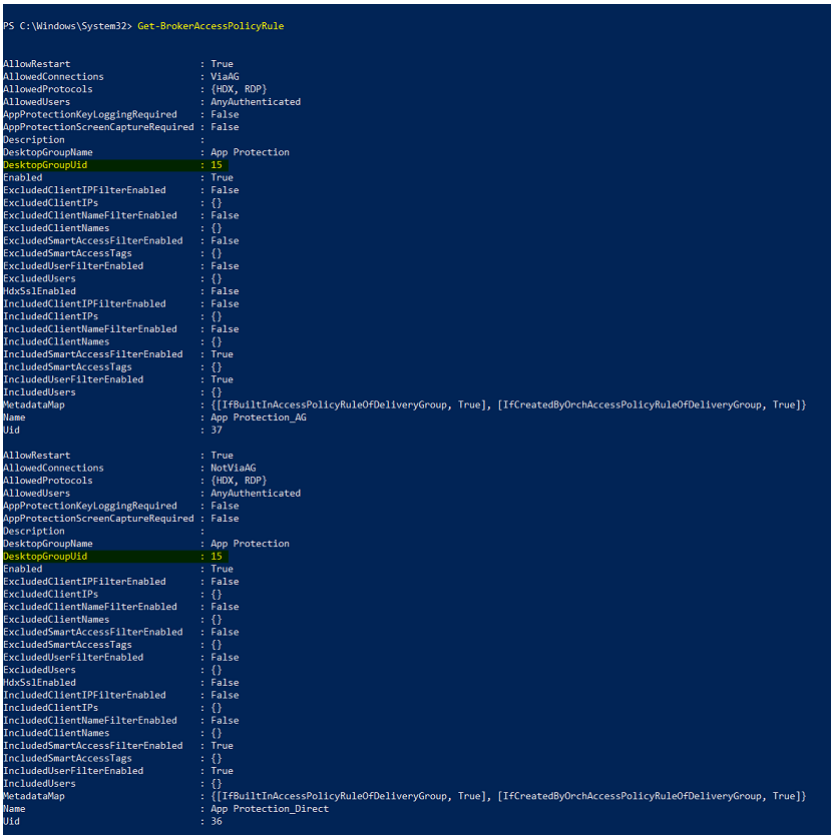
1. Sélectionnez le groupe d'utilisateurs Active Directory pour lequel vous souhaitez activer les stratégies App Protection pour les utilisateurs. Dans cet exemple, le groupe d'utilisateurs Active Directory est **ProductManagers**.
2. Configurez les règles de stratégies Broker Access.

   a) Installez le SDK Citrix PowerShell et connectez-vous à l'API cloud comme expliqué sur la page Citrix Blog Getting started with PowerShell automation for Citrix Cloud.

   b) Exécutez la commande `Get-BrokerAccessPolicyRule`.

   Une liste de toutes les stratégies Broker Access pour tous les groupes de mise à disposition présents s'affiche.

c) Recherchez le paramètre **DesktopGroupUid** pour le groupe de mise à disposition que vous souhaitez modifier.



d) Obtenez les stratégies qui s'appliquent uniquement à un groupe de mise à disposition spécifique à l'aide de la commande :

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) Pour activer les stratégies App Protection pour les utilisateurs du groupe d'utilisateurs **ProductManagers**, exécutez les commandes suivantes :

```
New-BrokerAccessPolicyRule "Example Rule Name_1"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $true -IncludedUserFilte
 $true -IncludedUsers domain.com\ProductManagers
```

f) Pour désactiver les stratégies App Protection pour les utilisateurs qui ne font pas partie du groupe d'utilisateurs **ProductManagers**, exécutez les commandes suivantes :

```
New-BrokerAccessPolicyRule "Example Rule Name_2"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $false-ExcludedUserFilte
 $true -ExcludedUsers domain.com\ProductManagers
```

3. Vérification :

Déconnectez-vous de l'application Citrix Workspace, si elle est déjà ouverte. Connectez-vous à l'application Citrix Workspace en tant qu'utilisateur du groupe d'utilisateurs Active Directory **ProductManagers**. Lancez la ressource protégée et vous verrez que App Protection est désactivé. Déconnectez-vous de l'application Citrix Workspace, puis reconnectez-vous en tant qu'utilisateur ne faisant pas partie du groupe d'utilisateurs Active Directory **ProductManagers**. Lancez la ressource protégée et vous verrez qu'App Protection est activée.

App Protection contextuelle pour StoreFront

March 11, 2024

La protection contextuelle des applications offre la flexibilité d'appliquer les stratégies de protection des applications de manière conditionnelle à un sous-ensemble d'utilisateurs, en fonction des utilisateurs, de leur appareil et de la position du réseau.

Mise en œuvre de la protection contextuelle des applications

Vous pouvez mettre en œuvre l'App Protection contextuelle à l'aide des filtres de connexion définis dans la règle de stratégie Broker Access. Les stratégies Broker Access définissent les règles qui contrôlent l'accès d'un utilisateur aux groupes de mise à disposition. La stratégie comprend un ensemble de règles. Chaque règle se rapporte à un seul groupe de mise à disposition et contient un ensemble de filtres de connexion et de contrôles de droits d'accès.

Les utilisateurs ont accès à un groupe de mise à disposition lorsque les détails de leur connexion correspondent aux filtres de connexion d'une ou de plusieurs règles de la stratégie Broker Access. Par défaut, les utilisateurs n'ont accès à aucun groupe de bureaux au sein d'un site. Vous pouvez créer des stratégies Broker Access supplémentaires en fonction des exigences. Plusieurs règles peuvent s'appliquer au même groupe de mise à disposition. Pour en savoir plus, consultez New-BrokerAccessPolicyRule.

Les paramètres suivants de la règle de stratégie Broker Access permettent d'activer App Protection de manière contextuelle si la connexion de l'utilisateur correspond aux filtres de connexion définis dans la règle de stratégie d'accès :

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

Utilisez les filtres Smart Access référencés dans les stratégies Broker Access pour affiner les filtres de connexion. Pour en savoir plus sur la configuration des filtres Smart Access, consultez CTX227055.

Reportez-vous aux scénarios ci-dessous afin de comprendre comment utiliser les stratégies Smart Access pour configurer l'App Protection contextuelle.

> **Remarque :**
>
> Si App Protection est activée sur le groupe de mise à disposition, l'App Protection contextuelle ne peut être appliquée par défaut. Désactivez App Protection sur le groupe de mise à disposition à l'aide de la commande suivante :

```
Set-BrokerDesktopGroup -Name "Admin Desktop" -
   AppProtectionKeyLoggingRequired $false -
   AppProtectionScreenCaptureRequired $false
<!--NeedCopy-->
```

Logiciels requis

Pour activer l'App Protection contextuelle pour StoreFront, assurez-vous de répondre aux exigences mentionnées dans la section Conditions préalables.

Activer App Protection contextuelle

1. Téléchargez les stratégies d'App Protection contextuelle (tableau des fonctionnalités) pour votre version de Citrix Virtual Apps and Desktops à partir de la page Téléchargements Citrix.
2. Exécutez les commandes PowerShell suivantes dans le Delivery Controller :

   ```
   asnp Citrix*
   Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
   <!--NeedCopy-->
   ```

3. Exécutez les commandes suivantes pour activer l'App Protection contextuelle dans le Delivery Controller :

   ```
   Import-ConfigFeatureTable <path to the downloaded feature table>
   <!--NeedCopy-->
   ```

   Par exemple,

   ```
   Import-ConfigFeatureTable\Downloads\FeatureTable.OnPrem.
      AppProtContextualAccess.xml
   <!--NeedCopy-->
   ```

Scénarios d'App Protection contextuelle

Voici certains des scénarios d'activation ou de désactivation d'App Protection contextuelle :

- Désactiver App Protection pour certains types d'appareils
- Désactiver App Protection pour les connexions lancées depuis un navigateur et activer App Protection pour les connexions lancées depuis l'application Citrix Workspace
- Désactiver App Protection pour les utilisateurs d'un groupe Active Directory spécifique
- Activer App Protection pour des appareils en fonction des résultats de l'analyse de point de terminaison
- Activer App Protection pour des groupes d'utilisateurs spécifiques

Logiciels requis

March 11, 2024

Assurez-vous que vous disposez des éléments suivants :

- Citrix Virtual Apps and Desktops version 2109 ou ultérieures
- Delivery Controller version 2109 ou versions ultérieures
- StoreFront version 1912 LTSR ou versions ultérieures
- Configurations de la passerelle ou du serveur virtuel VPN et du serveur virtuel d'authentification
- Connexion réussie entre NetScaler et StoreFront. Pour plus d'informations, consultez Intégrer NetScaler Gateway à StoreFront
- L'importation de tables XML est requise jusqu'à la version 2006 de Citrix Virtual Apps and Desktops
- L'importation de la table des fonctionnalités contextuelle d'App Protection est nécessaire jusqu'à la version 2209 de Citrix Virtual Apps and Desktops
- Activez Smart Access sur NetScaler Gateway, pour les scénarios qui nécessitent des balises Smart Access. Pour de plus amples informations, consultez cet article de support.
- Configuration requise pour le système de licences
  - Licence sur site de protection des applications
  - Licence universelle Citrix Gateway pour les scénarios avec des balises Smart Access

Scénario 1

March 11, 2024

Ce scénario explique comment désactiver App Protection pour certains types d'appareils.

Les étapes suivantes permettent de désactiver App Protection pour les utilisateurs d'iPhone sur un groupe de mise à disposition appelé `Win10Desktop` :

1. Créez une stratégie Smart Access :

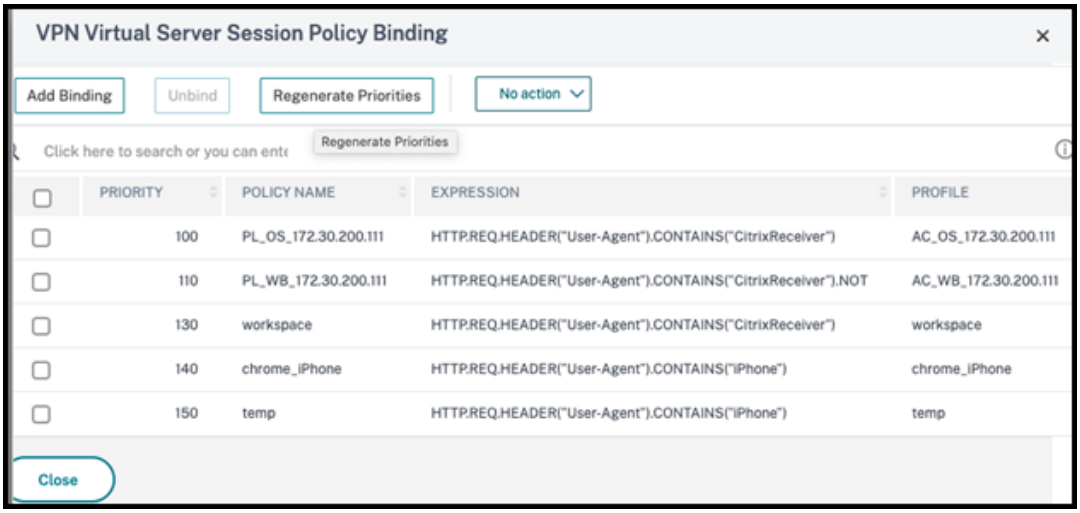
   a) Connectez-vous à l'interface utilisateur d'administration de Citrix ADC.

   b) Dans le menu de navigation de gauche, accédez à **Citrix Gateway** > **Serveurs virtuels**.

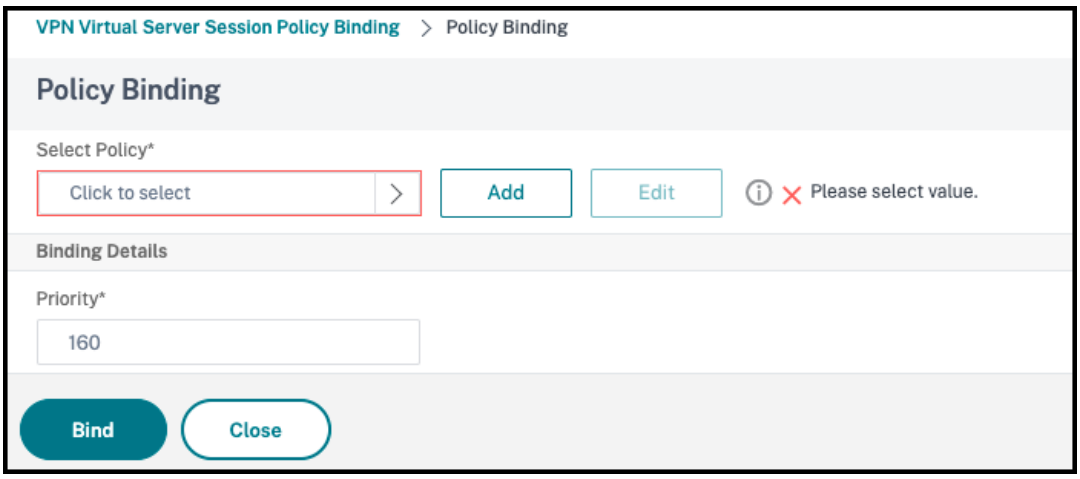
   Notez le nom du serveur virtuel VPN requis pour configurer ultérieurement la stratégie Broker Access.

   c) Cliquez sur **VPN Virtual Server**. Faites défiler la page vers le bas et cliquez sur **Session policies**. La liste des stratégies de session s'affiche.

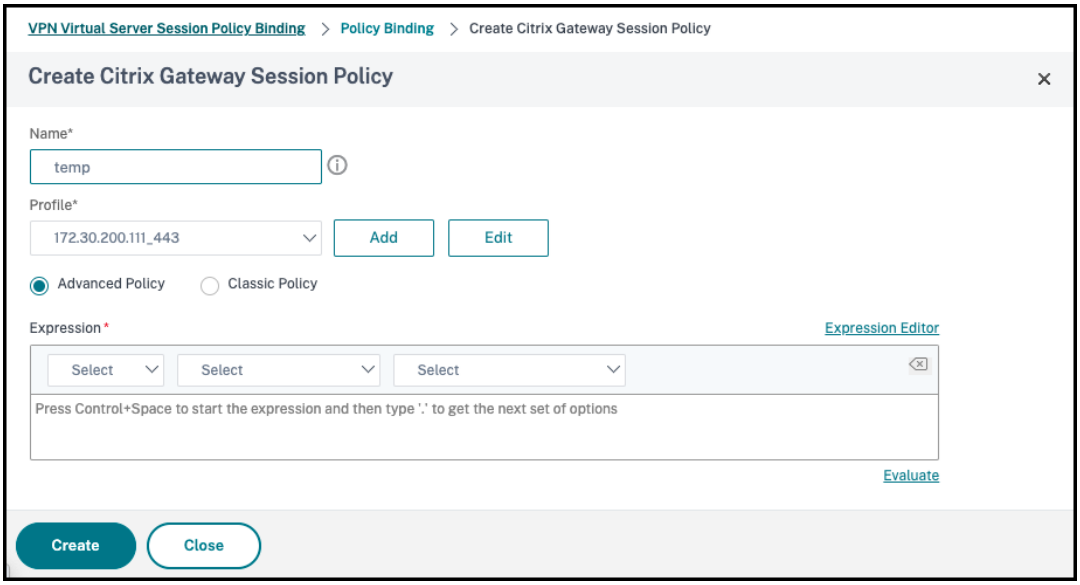
   d) Cliquez sur **Add Binding**.



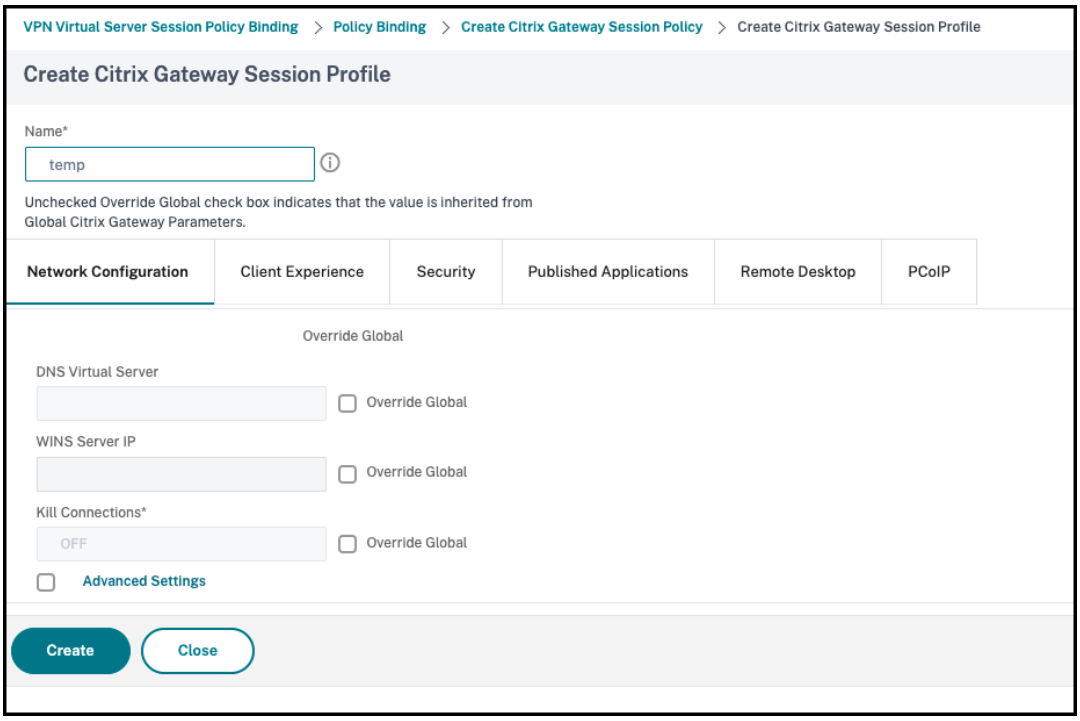
   e) Cliquez sur **Add to create a session policy**.



   f) Entrez un nom pour la stratégie de session. Dans ce scénario, le nom est *temp*.



g) Cliquez sur **Add** en regard de Profile pour spécifier un nom de profil. Cliquez sur **Créer**.



h) Cliquez sur **Expression Editor** dans la fenêtre Session Policy.

i) Créez l'expression suivante pour rechercher *iPhone* dans la chaîne **User Agent** :

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")
<!--NeedCopy-->
```


j) Cliquez sur **Bind** pour créer la stratégie de session.

2. Créer des règles de stratégie Broker Access :

   Pour appliquer la stratégie aux utilisateurs d'iPhone accédant à `Win10Desktop` via Access Gateway, procédez comme suit :

   a) Exécutez la commande suivante dans le Delivery Controller (DDC) :

   ```
   Get-BrokerAccessPolicyRule
   <!--NeedCopy-->
   ```

   qui répertorie toutes les stratégies Broker Access définies dans le DDC. Dans ce scénario, les stratégies Broker Access pour le groupe de mise à disposition `Win10Desktop` sont `Win10Desktop_AG` et `Win10Desktop_Direct`. Notez l'UID du groupe de mise à disposition pour l'étape suivante.

   b) Créez une règle de stratégie Broker Access pour `Win10Desktop` afin de filtrer les utilisateurs d'iPhone passant par Access Gateway à l'aide de la commande suivante :

   ```
   New-BrokerAccessPolicyRule -Name Win10Desktop_AG_iPhone -
       DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
       ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
       AnyAuthenticated -AllowRestart $true -
       AppProtectionKeyLoggingRequired $false -
       AppProtectionScreenCaptureRequired $false -Enabled $true -
       IncludedSmartAccessFilterEnabled $true
   <!--NeedCopy-->
   ```

   Uid_of_desktopGroup est le DesktopGroupUID du groupe de mise à disposition obtenu en exécutant la règle GetBrokerAccessPolicy à l'étape 1.

   c) Pour désactiver App Protection pour les utilisateurs d'iPhone `Win10Desktop` passant par Access Gateway, indiquez la balise Smart Access *temp* créée à l'étape 1. Créez une stratégie Smart Access à l'aide de la commande suivante :

   ```
   Set-BrokerAccessPolicyRule Win10Desktop_AG_iPhone -
       IncludedSmartAccessTags Primary_HDX_Proxy:temp -
       AppProtectionScreenCaptureRequired $false -
       AppProtectionKeyLoggingRequired $false
   ```



```
<!--NeedCopy-->
```

Primary_HDX_Proxy est le nom du serveur virtuel VPN indiqué précédemment à l'étape 1, Créer une stratégie Smart Access.

d) Pour activer les stratégies App Protection pour le reste des utilisateurs `Win10desktop`, utilisez la commande suivante :

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

3. **Vérification**

   Pour iPhone : déconnectez-vous de l'application Citrix Workspace, si elle est déjà ouverte sur l'iPhone. Connectez-vous en externe à l'application Citrix Workspace via une connexion Access Gateway. Vous pouvez constater que les ressources requises par StoreFront et App Protection doivent être désactivées.

   Pour les appareils autres qu'iPhone : déconnectez-vous de l'application Citrix Workspace, si elle est déjà ouverte sur l'appareil. Connectez-vous en externe à l'application Citrix Workspace via une connexion Access Gateway. Vous pouvez constater que les ressources requises par StoreFront et App Protection doivent être désactivées.

Scénario 2

March 11, 2024

Ce scénario explique comment désactiver App Protection pour les connexions lancées depuis un navigateur et activer App Protection pour les connexions lancées depuis l'application Citrix Workspace.

Les étapes suivantes permettent de désactiver App Protection pour un groupe de mise à disposition appelé `Win10Desktop` lorsque les connexions sont lancées depuis un navigateur et pour activer App Protection pour les connexions lancées depuis l'application Citrix Workspace :

1. Créez des stratégies Smart Access :

   a) Créez une stratégie Smart Access pour filtrer les connexions lancées depuis l'application Citrix Workspace, comme défini dans le scénario précédent **Désactiver App Protection pour certains types d'appareils**. Créez l'expression suivante pour rechercher **CitrixReceiver** dans la chaîne **User Agent** :


```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
<!--NeedCopy-->
```

Dans ce scénario, la stratégie Smart Access est `cwa`.

b) Créez une autre stratégie Smart Access pour filtrer les connexions qui ne sont pas démarrées depuis l'application Citrix Workspace `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT`. Dans ce cas, cette stratégie Smart Access est *browser*.

2. Créer des règles de stratégie Broker Access :

a) Exécutez `GetBrokerAccessPolicyRule` pour afficher les deux stratégies Broker Access pour `Win10Desktop`. Pour le groupe de mise à disposition `Win10Desktop`, les stratégies Broker Access sont `Win10Desktop_AG` et `Win10Desktop_Direct`. Notez l'UID du groupe de bureaux de `Win10Desktop`.

b) Créez une stratégie Broker Access pour `Win10Desktop` afin de filtrer les connexions lancées depuis l'application Citrix Workspace à l'aide de la commande suivante :

```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_CWA -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
    AnyAuthenticated -AllowRestart $true -Enabled $true -
    IncludedSmartAccessFilterEnabled $true
<!--NeedCopy-->
```

Uid_of_desktopGroup est le DesktopGroupUID du groupe de mise à disposition obtenu en exécutant la règle GetBrokerAccessPolicy à l'étape 1.

c) Utilisez la commande suivante pour activer les stratégies App Protection uniquement pour les connexions via l'application Citrix Workspace en indiquant la balise Smart Access `cwa` :


```
Set-BrokerAccessPolicyRule Win10Desktop_AG_CWA -
    IncludedSmartAccessTags Primary_HDX_Proxy:cwa -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

Primary_HDX_Proxy est le nom du serveur virtuel VPN indiqué plus haut à l'étape 1, Créer une stratégie Smart Access.

d) Utilisez la commande suivante pour désactiver les stratégies App Protection pour les autres connexions via le navigateur :

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    IncludedSmartAccessTags Primary_HDX_Proxy:browser -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

3. **Vérification**

   Déconnectez-vous de l'application Citrix Workspace, si elle est déjà ouverte. Connectez-vous à l'application Citrix Workspace et lancez la ressource requise via une connexion externe via Access Gateway. Vous voyez que les stratégies App Protection sont activées pour la ressource. Lancez la même ressource depuis le navigateur via une connexion externe et vous constaterez que les stratégies App Protection sont désactivées.

Scénario 3

March 11, 2024

Ce scénario explique comment désactiver App Protection pour les utilisateurs d'un groupe Active Directory spécifique.

Les étapes suivantes permettent de désactiver App Protection pour les utilisateurs `Win10Desktop` qui font partie du groupe Active Directory **xd.local\sales** :

1. Exécutez `Get-BrokerAccessPolicyRule` pour afficher les deux stratégies Broker Access pour `Win10Desktop`. Pour un groupe de mise à disposition `Win10Desktop`, il existe deux stratégies Broker Access : `Win10Desktop_AG` et `Win10Desktop_Direct`. Notez l'UID du groupe de bureaux de `Win10Desktop`.
2. Créez une règle de stratégie Broker Access pour `Win10Desktop` afin de filtrer les connexions des utilisateurs du groupe Active Directory `xd.local\sales`.


```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_Sales_Group -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections ViaAG
     -AllowedProtocols HDX, RDP -AllowedUsers Filtered -
    AllowRestart $true -Enabled $true
<!--NeedCopy-->
```

Uid_of_desktopGroup est le DesktopGroupUID du groupe de mise à disposition obtenu en exécutant la règle GetBrokerAccessPolicy à l'étape 1.

3. Utilisez la commande suivante pour désactiver les stratégies App Protection pour les utilisateurs de Windows 10 Desktop, qui font partie du groupe Active Directory **xd.local\sales** :

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_Sales_Group -
    AllowedUsers Filtered -IncludedUsers xd.local\sales -
    IncludedUserFilterEnabled $true -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

4. Utilisez la commande suivante pour activer les stratégies App Protection pour le reste des connexions Gateway, à l'exception des utilisateurs de **xd.local\sales** :

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -AllowedUsers
    Anyauthenticated -ExcludedUserFilterEnabled $true -
    ExcludedUsers xd.local\sales -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

5. **Vérification**

   Déconnectez-vous de l'application Citrix Workspace, si elle est déjà ouverte. Connectez-vous à l'application Citrix Workspace en tant qu'utilisateur du groupe Active Directory **xd.local\sales**. Lancez la ressource protégée et vous verrez que App Protection est désactivé.

   Déconnectez-vous de l'application Citrix Workspace, puis reconnectez-vous en tant qu'utilisateur ne faisant pas partie de **xd.local\sales**. Lancez la ressource protégée et vous verrez qu'App Protection est activée.

Scénario 4

March 11, 2024

Ce scénario explique comment activer App Protection pour les appareils en fonction des résultats de l'analyse de point de terminaison.

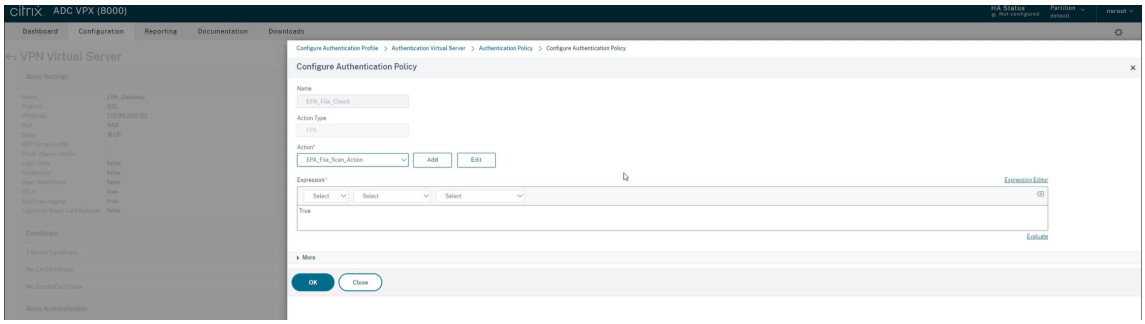
Suivez les étapes suivantes pour activer App Protection pour les appareils approuvés par les analyses de point de terminaison :

Conditions préalables :

Assurez-vous que vous disposez des éléments suivants :

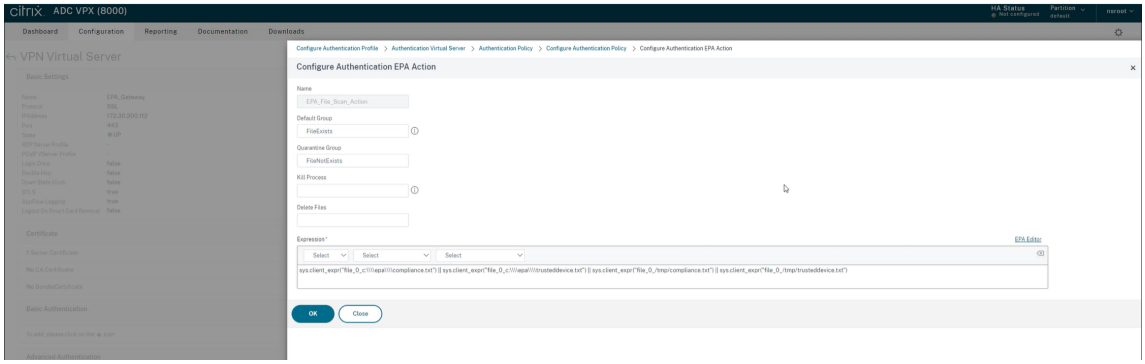
- Authentification, autorisation et audit de groupes d'utilisateurs (pour les groupes d'utilisateurs par défaut et en quarantaine) et stratégies associées
- Configurations du serveur LDAP et stratégies associées

1. Connectez-vous à Citrix ADC et accédez à **Configuration** > **Citrix Gateway** > **Serveurs virtuels**.
2. Sélectionnez le serveur virtuel approprié et cliquez sur **Modifier**.
3. Modifiez le profil d'authentification existant.
4. Sélectionnez le serveur virtuel approprié et cliquez sur **Modifier**.
5. Cliquez sur **Stratégies d'authentification** > **Ajouter une liaison**.
6. Sous **Sélectionner une stratégie**, cliquez sur **Ajouter**.
7. Dans le champ **Nom**, indiquez le nom de la stratégie d'authentification.
8. Dans la liste déroulante **Type d'action**, sélectionnez **Analyse de point de terminaison**.
9. Dans le champ **Expression**, indiquez `True`.



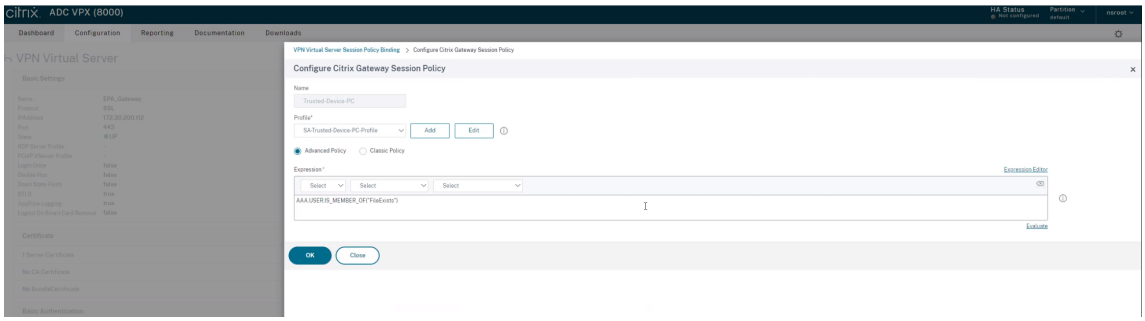
10. Sous **Action**, cliquez sur **Ajouter**.
11. Dans le champ **Nom**, indiquez le nom de l'action d'analyse de point de terminaison.
12. Indiquez les noms du **Groupe par défaut** et du **Groupe de quarantaine**. Dans ce scénario, le nom du **Groupe par défaut** est **FileExists** et le nom du **Groupe de quarantaine** est **FileNotExists**.
13. Dans le champ **Expression**, indiquez la valeur suivante :

```
1 sys.client_expr("file_0_c:\\epa\\compliance.txt") || sys.
     client_expr("file_0_c:\\epa\\trusteddevice.txt") || sys.
     client_expr("file_0_/tmp/compliance.txt") || sys.client_expr("
     file_0_/tmp/trusteddevice.txt")
2 <!--NeedCopy-->
```

14. Cliquez sur **Créer**, puis sur **Lier**.
15. Cliquez sur **Stratégies de session** > **Ajouter une liaison**.
16. Sous **Sélectionner une stratégie**, cliquez sur **Ajouter**.
17. Dans le champ **Nom**, indiquez le nom de la stratégie de session.
18. Dans le champ **Expression**, indiquez la valeur suivante :

```
AAA.USER.IS_MEMBER_OF("FileExists")
<!--NeedCopy-->
```



19. Cliquez sur **Créer**, puis sur **Lier**.
20. Dans la partie la plus à gauche de la barre des tâches, cliquez sur l'icône **Rechercher** .
21. Entrez **Powershell**, puis ouvrez **Windows Powershell**.
22. Utilisez la commande suivante pour désactiver les stratégies App Protection pour les appareils approuvés par les analyses de point de terminaison en indiquant la **balise Smart Access « EPA_GW:Trusted-Device-PC »** :

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
    Group_AG" -IncludedSmartAccessFilterEnabled $true -
    IncludedSmartAccessTags EPA_GW:Trusted-Device-PC -
    AppProtectionScreenCaptureRequired $false
<!--NeedCopy-->
```

où *EPA_GW* est le nom du serveur virtuel VPN.

23. Utilisez la commande suivante pour activer les stratégies App Protection pour les appareils non approuvés par les analyses de point de terminaison en indiquant la **balise Smart Access « EPA_GW:Trusted-Device-PC »** :

```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
    Group_AG_NonCompliant"-DesktopGroupUid 17 -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
    $true -ExcludedSmartAccessFilterEnabled $true -
    ExcludedSmartAccessTags EPA_GW:Trusted-Device-PC -
    IncludedSmartAccessFilterEnabled $true -
    AppProtectionScreenCaptureRequired $true
<!--NeedCopy-->
```

24. **Vérification**

    Déconnectez-vous de l'application Citrix Workspace, si elle est déjà ouverte. Connectez-vous à l'application Citrix Workspace à partir d'un appareil sécurisé. Lancez la ressource protégée et vous verrez que App Protection est désactivé.

    Déconnectez-vous de l'application Citrix Workspace, puis reconnectez-vous depuis un appareil non sécurisé. Lancez la ressource protégée et vous verrez qu'App Protection est activée.

Scénario 5

November 27, 2023

Ce scénario explique comment activer App Protection pour des groupes d'utilisateurs spécifiques.

Pour activer App Protection pour les utilisateurs d'un groupe spécifique, consultez la section Activer App Protection pour des groupes d'utilisateurs spécifiques

Prise en charge d'App Protection pour le lancement hybride via Workspace

March 11, 2024

Le lancement hybride de Citrix Virtual Apps and Desktops se produit lorsque vous vous connectez à Citrix Workspace pour le Web, en saisissant l'URL du magasin dans le navigateur natif, puis en lançant les applications et les bureaux virtuels via l'application Citrix Workspace native et son moteur HDX. Le terme hybride désigne le résultat de l'utilisation combinée de l'application Citrix Workspace pour le Web et de l'application native Citrix Workspace pour connecter et utiliser les ressources.

> **Remarque :**
>
> Lorsqu'aucun composant natif de l'application Citrix Workspace n'est installé sur le point de terminaison, il s'agit d'une configuration sans installation dans laquelle le magasin Citrix Workspace et le moteur HDX résident dans le navigateur. Ce scénario est connu sous le nom d'application Citrix Workspace pour HTML5, qui est hébergée sur Citrix Workspace ou Citrix StoreFront. Ce document ne traite pas de ce scénario.

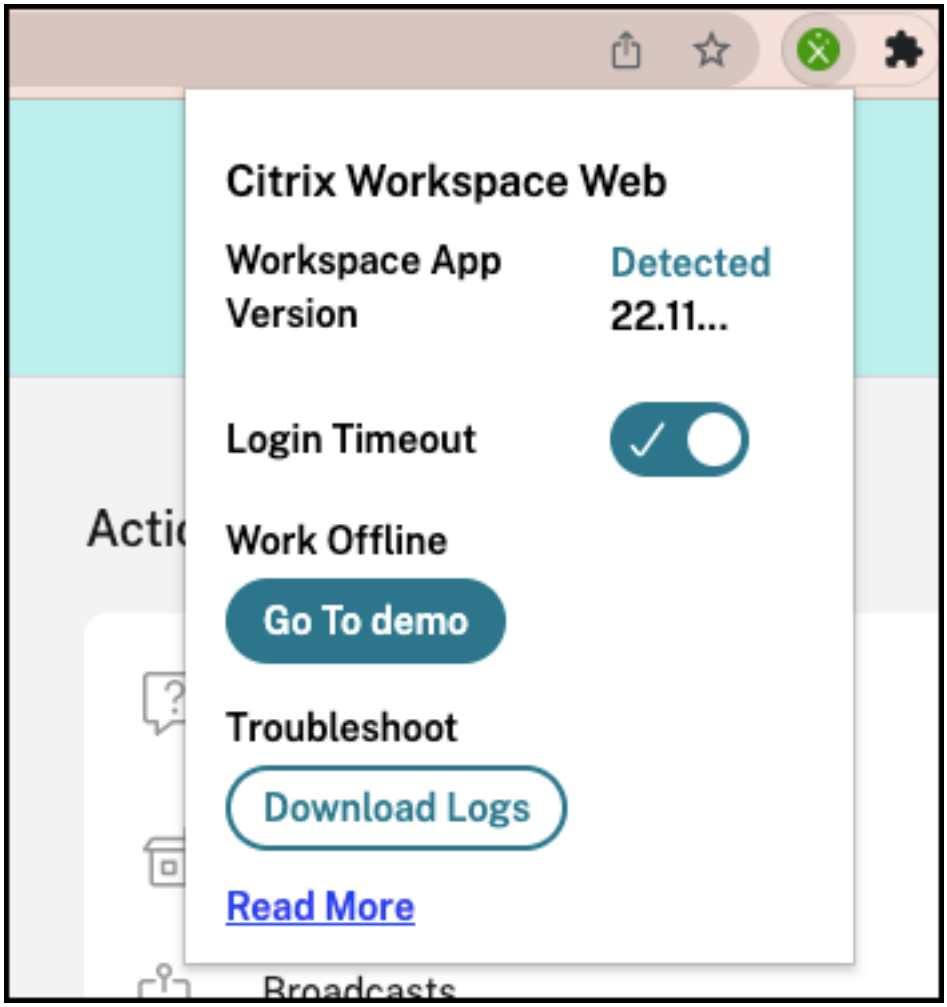
Logiciels requis

- Assurez-vous que vous utilisez un navigateur prenant en charge l'extension Web Citrix Workspace.
- Assurez-vous que le suffixe DNS de votre URL Workspace est cloud.com. Actuellement, les domaines personnalisés ne sont pas pris en charge.
- Vérifiez que vous utilisez l'une des versions suivantes de l'application Citrix Workspace :
  - Application Citrix Workspace pour Windows 2106 ou versions ultérieures
  - Application Citrix Workspace pour macOS 2106 ou versions ultérieures

Activer la protection des applications pour un lancement hybride

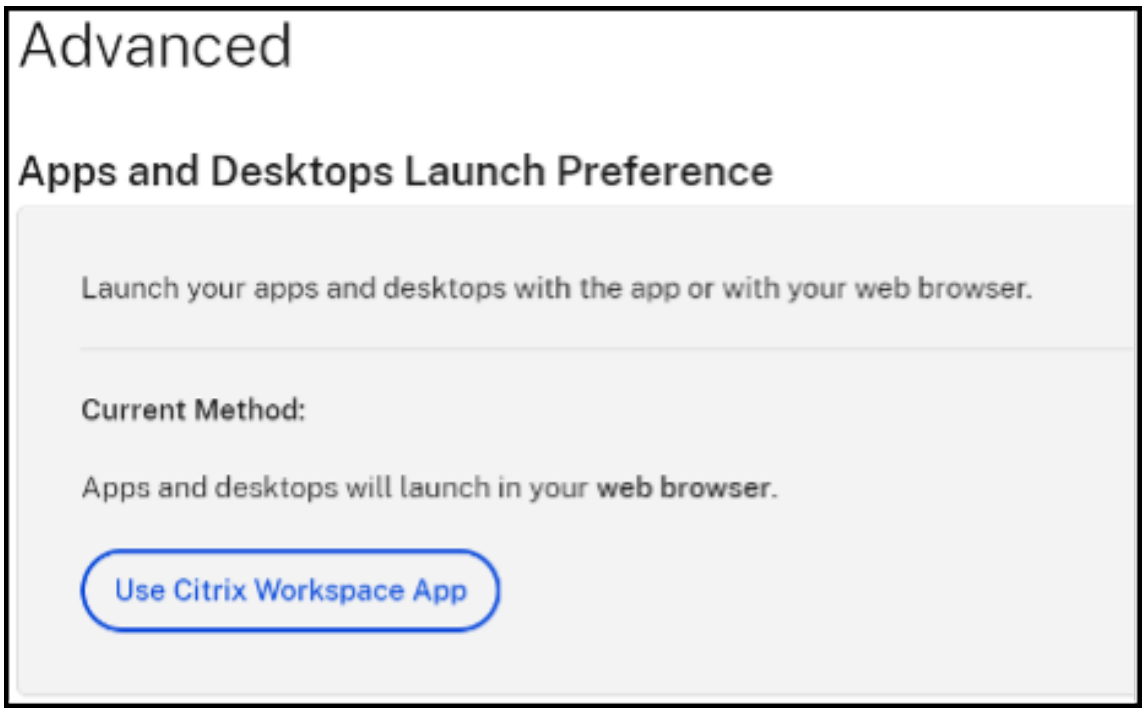
1. Installez l'extension Web Citrix Workspace pour votre navigateur avant d'ajouter le magasin. Utilisez l'un des liens suivants en fonction de votre navigateur :
   - Chrome
   - Edge Chromium

   Une fois l'extension installée, elle apparaît dans la section des extensions de votre navigateur.

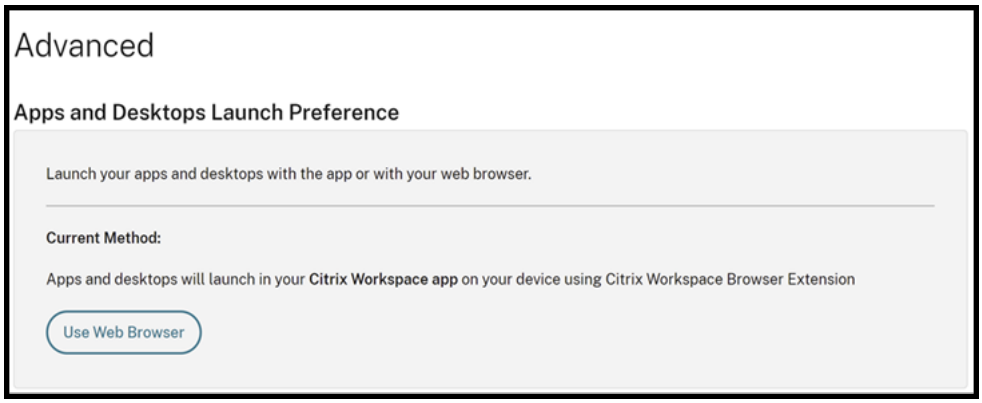


2. Connectez-vous au magasin depuis votre navigateur natif.
3. Accédez à votre **profil > Paramètres du compte > Avancé**.

   Dans la section **Préférences de lancement des applications et des postes de travail**, vous pouvez voir la méthode selon laquelle les applications et les postes de travail sont actuellement lancés dans votre navigateur Web. Cliquez sur **Utiliser l'application Citrix Workspace**.



Si vous utilisez l'application Citrix Workspace pour lancer les ressources, l'option suivante s'affiche. Dans ce cas, aucune modification n'est requise.

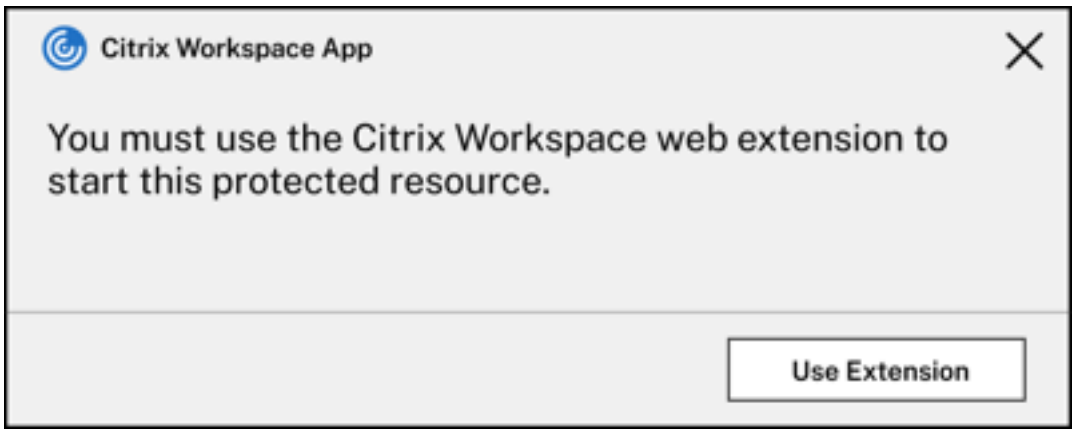


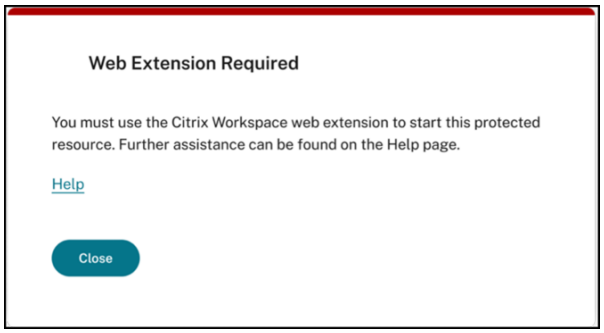
4. Vous pouvez maintenant lancer votre application ou bureau virtuel protégé.

Scénarios d'échec courants

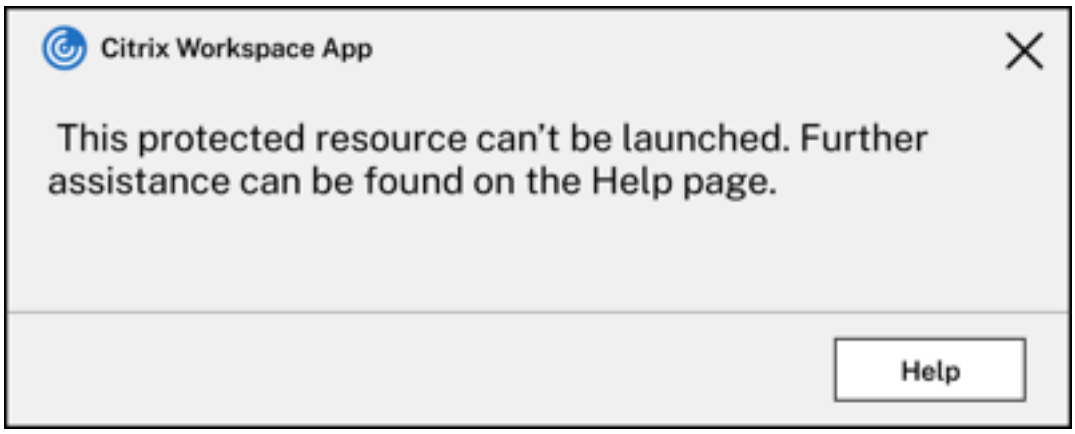
Voici quelques scénarios d'échec des lancements et des instructions pour y remédier.

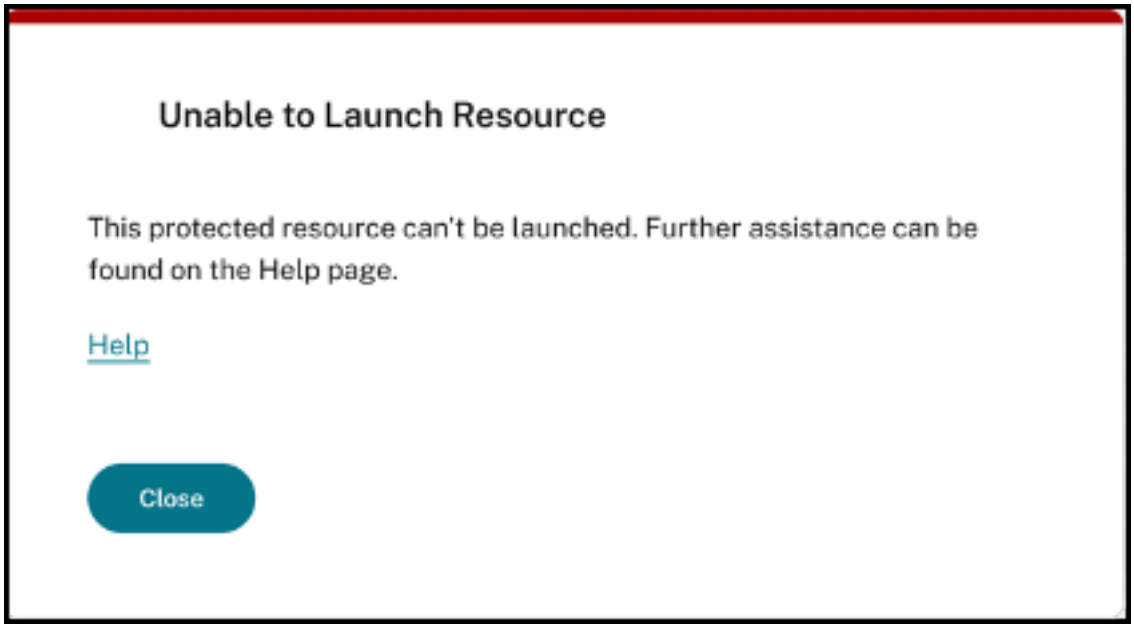
- L'une des erreurs suivantes s'affiche lorsque vous désactivez ou désinstallez l'extension Web Citrix Workspace avant de lancer l'application protégée. Pour l'éviter, installez l'extension avant de vous connecter à Citrix Workspace pour le Web.





- L'une des erreurs suivantes s'affiche lorsque la préférence de lancement est définie sur **Navigateur Web**. Pour résoudre cette erreur, définissez la préférence de lancement sur **Utiliser l'application Citrix Workspace**. Pour de plus amples informations, consultez cet article de support.





Prise en charge d'App Protection pour le lancement hybride via StoreFront

March 11, 2024

Le lancement hybride de Citrix Virtual Apps and Desktops se produit lorsque vous vous connectez à StoreFront pour le Web en saisissant l'URL du magasin dans le navigateur natif, puis que vous lancez Citrix Virtual Apps and Desktops via l'application Citrix Workspace native et son moteur HDX. Le terme hybride désigne le résultat de l'utilisation combinée de StoreFront pour le Web et de l'application Citrix Workspace native pour connecter et utiliser les ressources.

> **Remarque :**
>
> Lorsqu'aucun composant natif de l'application Citrix Workspace n'est installé sur le point de terminaison, il s'agit d'une configuration sans installation dans laquelle le magasin Citrix Workspace et le moteur HDX résident dans le navigateur. Ce scénario est connu sous le nom d'application Citrix Workspace pour HTML5, qui est hébergée sur Citrix Workspace ou Citrix StoreFront. Ce document ne traite pas de ce scénario.

La prise en charge d'App Protection pour le lancement hybride via StoreFront permet d'afficher et de lancer des ressources activées pour App Protection à partir de navigateurs.

> **Remarque :**
>
> Si vous sélectionnez les options **Utiliser la version simplifiée** (qui utilise le client HTML5) ou **Déjà installé**, les sessions activées pour App Protection sont bloquées car l'application Citrix Workspace n'est pas détectée correctement dans le navigateur.

Si vous utilisez StoreFront 2308 ou une version ultérieure, vous pouvez accéder aux applications et aux bureaux dotés de stratégies App Protection à l'aide d'un navigateur Web si StoreFront est configuré correctement et si le navigateur détecte correctement l'application Citrix Workspace native. Si vous utilisez des versions comprises entre StoreFront 1912 et 2203, vous devez appliquer la personnalisation comme décrit dans la section Déploiement.

> **Limitation :**
>
> StoreFront détermine la version de l'application Citrix Workspace lorsque vous vous connectez au site Web pour la première fois. Si vous installez ensuite une version différente de l'application Citrix Workspace, StoreFront ne prendra pas en compte la modification. Il peut donc autoriser ou interdire à tort le lancement des applications et des bureaux virtuels activés avec les stratégies d'App Protection. Citrix recommande de configurer la vérification de l'état d'App Protection, qui bloque le lancement d'applications et de bureaux virtuels à partir de versions précédentes de l'application Citrix Workspace qui ne prennent pas en charge App Protection. Pour en savoir plus sur la vérification de la posture, consultez Vérification de la posture d'App Protection.

Lancement hybride via StoreFront version 2308 ou ultérieure

Les versions 2308 et ultérieures de StoreFront prennent automatiquement en charge le lancement hybride d'applications et de bureaux virtuels activés avec les stratégies d'App Protection. Pour en savoir plus sur l'activation de App Protection pour un lancement hybride sur StoreFront 2308 ou version ultérieure, consultez la section App Protection pour lancement hybride via StoreFront.

Lancement hybride via StoreFront versions 1912 à 2203

Les versions 1912 à 2203 de StoreFront permettent le lancement hybride d'applications et de bureaux virtuels dotés de stratégies App Protection et personnalisés comme suit :

Citrix recommande de supprimer cette configuration lors de la mise à niveau vers StoreFront 2308 ou version ultérieure.

Logiciels requis

Pour en savoir plus sur les versions requises des composants Citrix pour App Protection, consultez la section Configuration système requise.

Déploiement

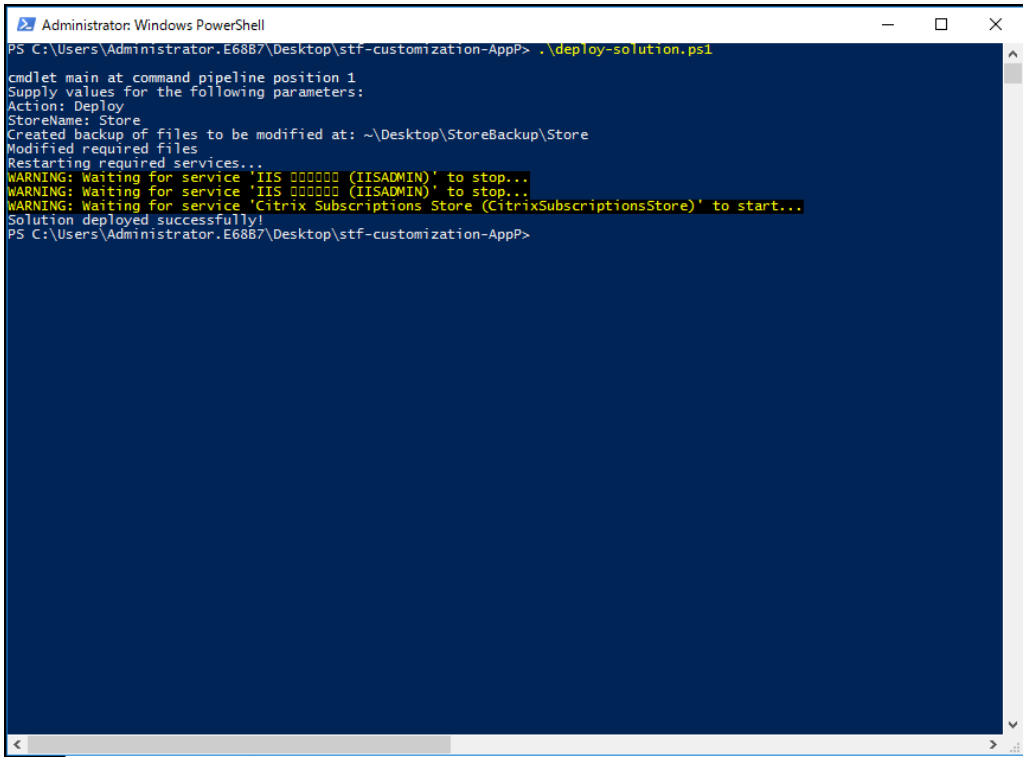
1. Téléchargez le fichier Zip nommé *stf-customization-AppP.zip* qui contient tous les fichiers requis que vous devez déployer sur la machine serveur StoreFront. Téléchargez le fichier depuis la page Téléchargements de Citrix. Le fichier inclut les éléments suivants :

    - DLL que vous devez copier dans le dossier bin du magasin
    - Fichiers JavaScript et autres fichiers nécessaires au fonctionnement de la solution
    - Script PowerShell*deploy-solution.ps1* que l'administrateur StoreFront utilise pour déployer la solution

2. Décompressez le fichier *stf-customization-AppP.zip* et ouvrez une invite de commande PowerShell en tant qu'administrateur à l'emplacement où les fichiers sont extraits. Exécutez la commande `deploy-solution.ps1` qui utilise les arguments suivants :

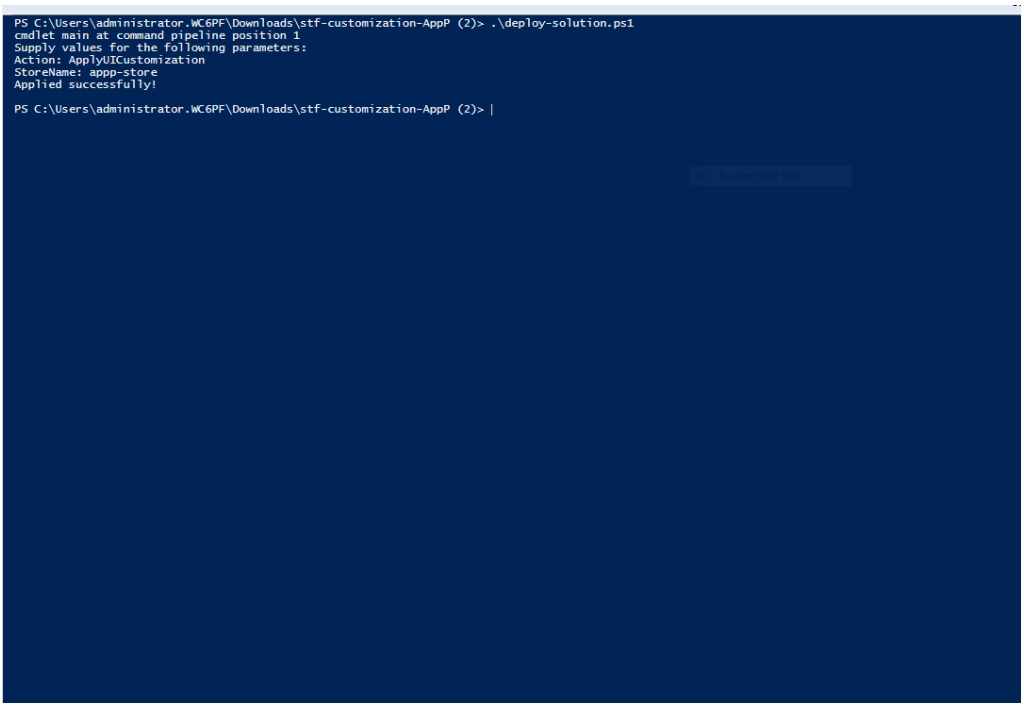
    - `-Action` : action exécutée par le script. Les valeurs autorisées sont les suivantes :

        - L'action `Deploy` déploie la solution de manière fluide. Elle crée une sauvegarde des fichiers que la solution modifie, copie les fichiers de solution et redémarre les services. La capture d'écran suivante décrit la commande permettant de déployer la solution sur le serveur StoreFront :



        - L'action `ApplyUICustomization` applique une personnalisation à l'interface utilisateur du magasin afin que les options **Déjà installé** et **Utiliser la version simplifiée** ne s'affichent pas. Cette action permet de détecter l'application Citrix

Workspace native dans le navigateur et de contourner les scénarios bloqués ou non pris en charge.



  - L'action `RemoveUICustomization` annule l'action `ApplyUICustomization`, et les options **Déjà installé** et **Utiliser la version simplifiée** apparaissent à nouveau.

- `-StoreName` : nom du magasin pour lequel l'action doit être entreprise. Ce paramètre est obligatoire et doit être transmis en même temps que l'action `Deploy`.
- `-BackupDir` : paramètre pouvant être transmis avec l'action `Deploy` permettant de créer une sauvegarde dans le répertoire requis. S'il n'est pas transmis, la sauvegarde est créée sur le bureau. Ce paramètre est facultatif.

> **Remarque :**
>
> S'il existe des personnalisations dans *StoreCustomization_Input.dll* ou *StoreCustomization_Launch.dll*, le déploiement de cette solution les remplace.

Les applications et les bureaux activés par App Protection ne seront affichés qu'après le déploiement des configurations. Sans ce déploiement, les applications et les bureaux ne s'affichent pas.

Comment annuler la configuration personnalisée de StoreFront

Procédez comme suit pour annuler la configuration personnalisée précédente de StoreFront :

1. Accédez au répertoire *\Desktop\StoreBackup<store name>* et copiez les fichiers suivants dans les répertoires respectifs :

- Fichiers *StoreCustomization_Input.dll* et *StoreCustomization_Launch.dll* dans le répertoire *IISINETPub\Citrix<store name>\bin*
- Fichier *web.config* dans le répertoire *IISINETPub\Citrix\StoreWeb*
- Fichiers **.js* et *style.css* dans le répertoire *IISINETPub\Citrix\StoreWeb\Custom*

> **Remarque :**
>
> Si des fichiers de personnalisation autres que les fichiers précédents existent dans le répertoire \Desktop\StoreBackup<store name>, copiez ces fichiers et répertoires dans les répertoires appropriés selon vos besoins.

2. Ouvrez PowerShell.
3. Arrêtez les services **IISADMIN** et **CitrixSubscriptionsStore** à l'aide des commandes suivantes :

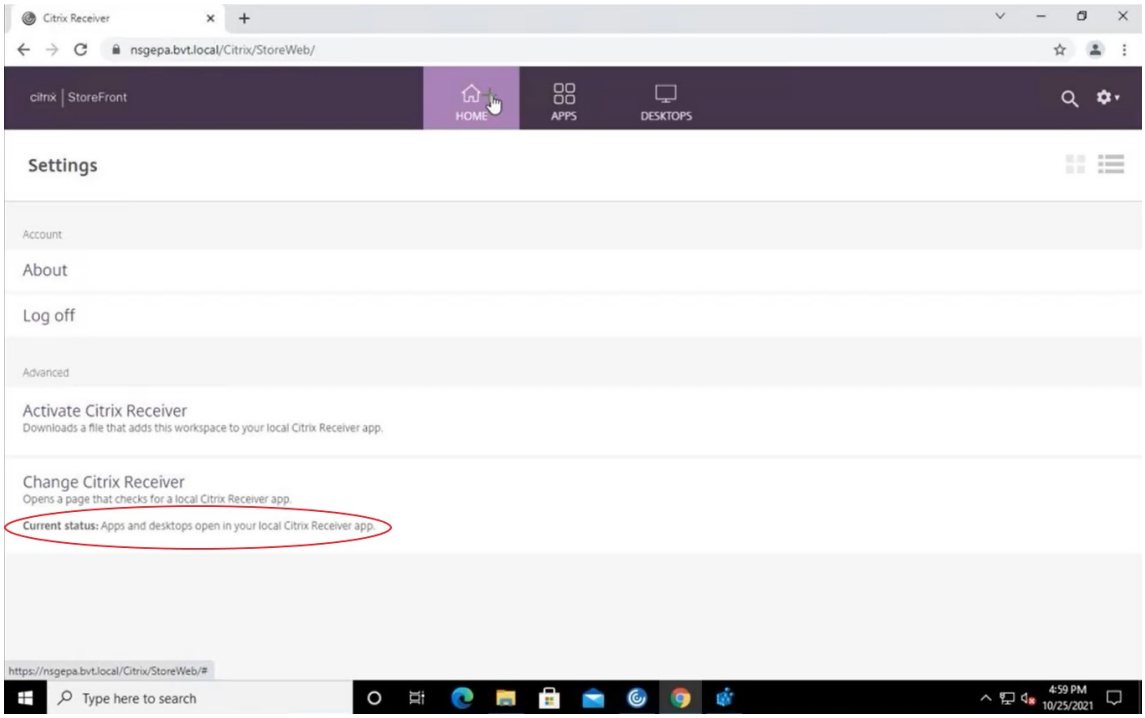
```
sc stop IISADMIN
sc stop CitrixSubscriptionsStore
<!--NeedCopy-->
```

4. Redémarrez les services **IISADMIN** et **CitrixSubscriptionsStore** à l'aide des commandes suivantes :

```
sc start IISADMIN
sc start CitrixSubscriptionsStore
<!--NeedCopy-->
```

Expérience utilisateur pour un lancement hybride des ressources protégées

1. Après le déploiement de la solution par l'administrateur sur le serveur StoreFront, connectez-vous à votre magasin côté client, puis accédez à StoreFront à l'aide de l'URL dans un navigateur Web.
2. Pour savoir si l'application Citrix Workspace est correctement détectée dans le navigateur, vérifiez le champ **État actuel** sur l'écran **Paramètres de compte**.



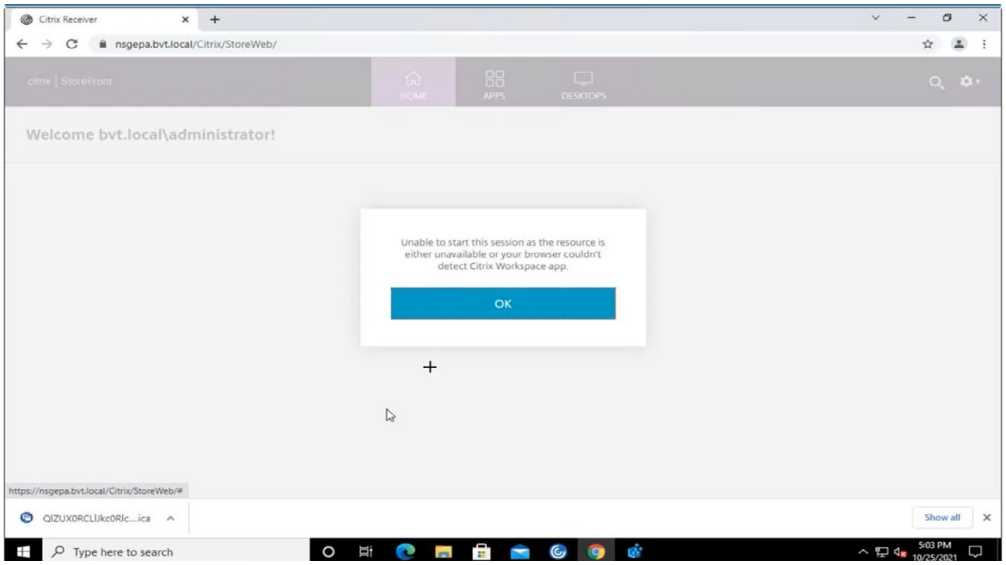
Une fois l'application Citrix Workspace détectée, vous pouvez voir et lancer toutes les applications et tous les bureaux virtuels activés avec App Protection.

Activer le suivi sur StoreFront

Pour activer le suivi dans StoreFront, consultez la documentation StoreFront. Ce suivi peut être utilisé pour vérifier si les étiquettes de stratégie de session NetScaler Gateway configurées sont correctement transmises au magasin.

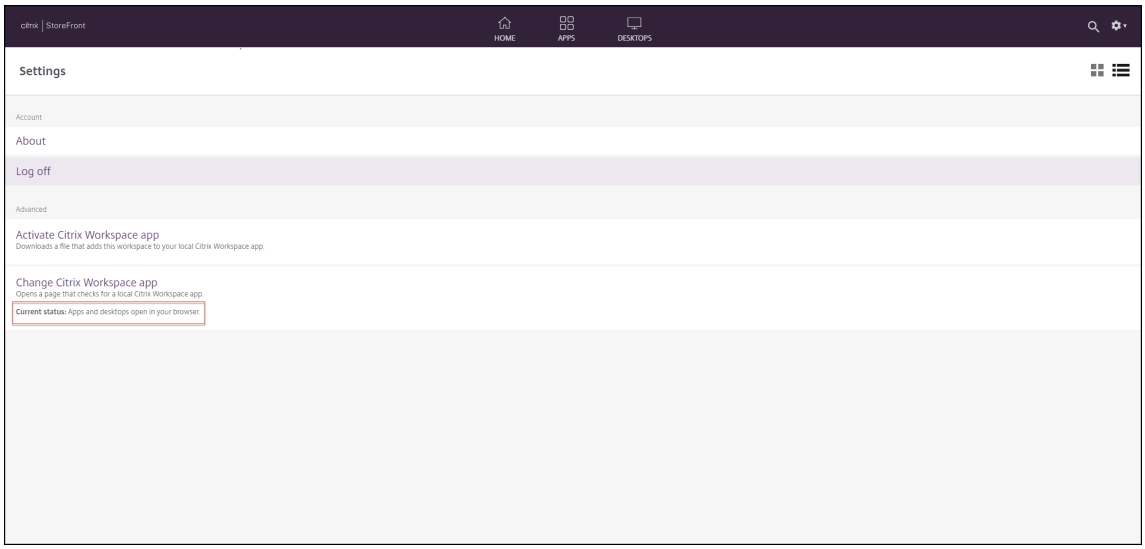
Dépannage

Lorsque vous lancez les sessions activées d'App Protection, l'erreur suivante peut parfois se produire :

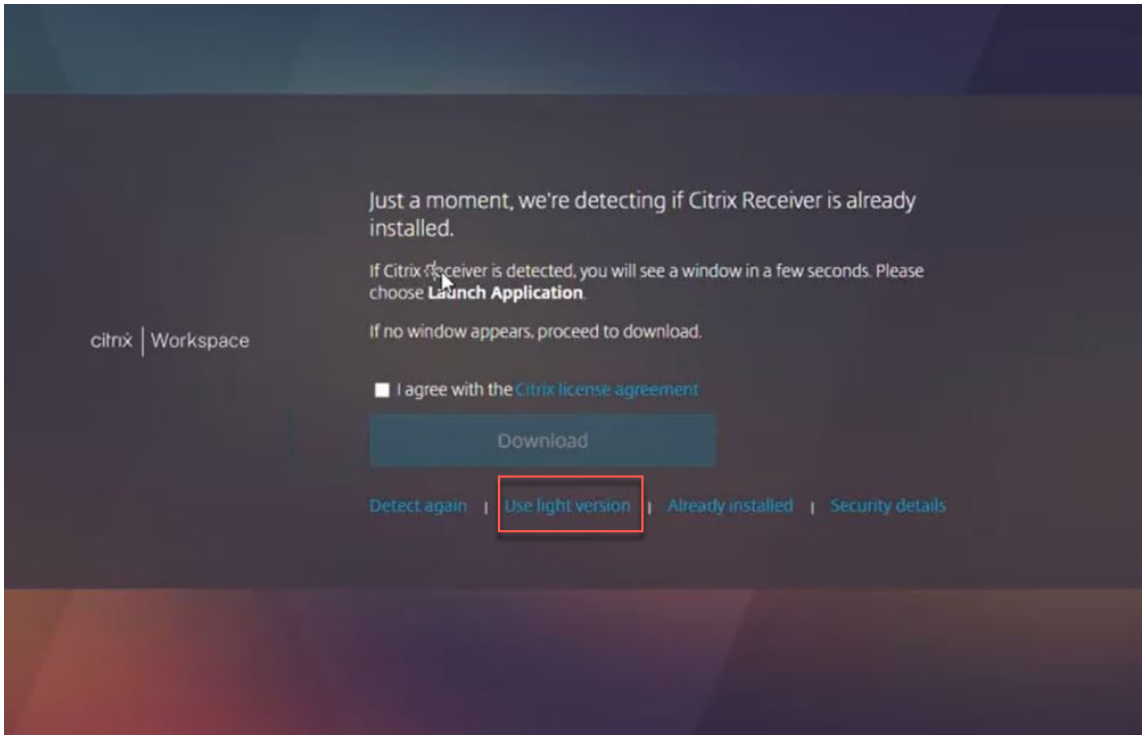


Les raisons possibles de cette erreur sont les suivantes :

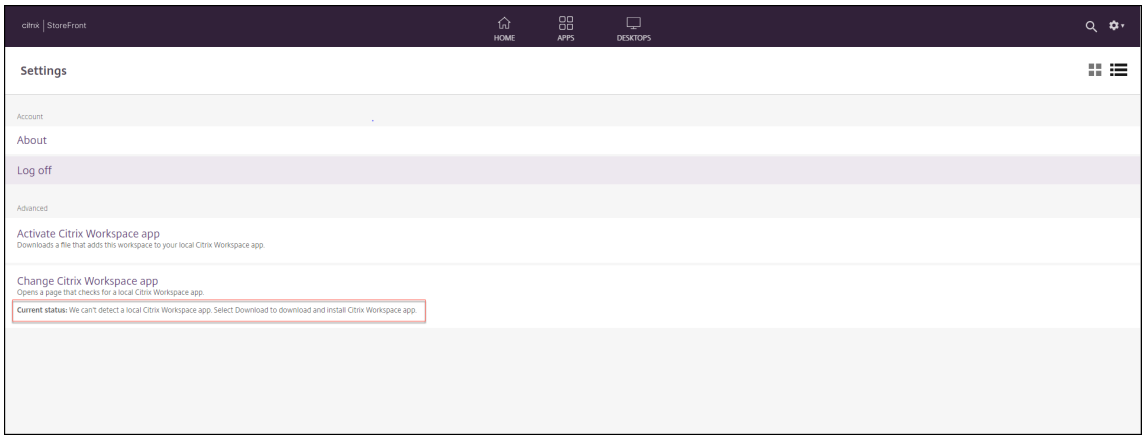
- Les applications et les bureaux sont configurés pour s'ouvrir dans un navigateur.



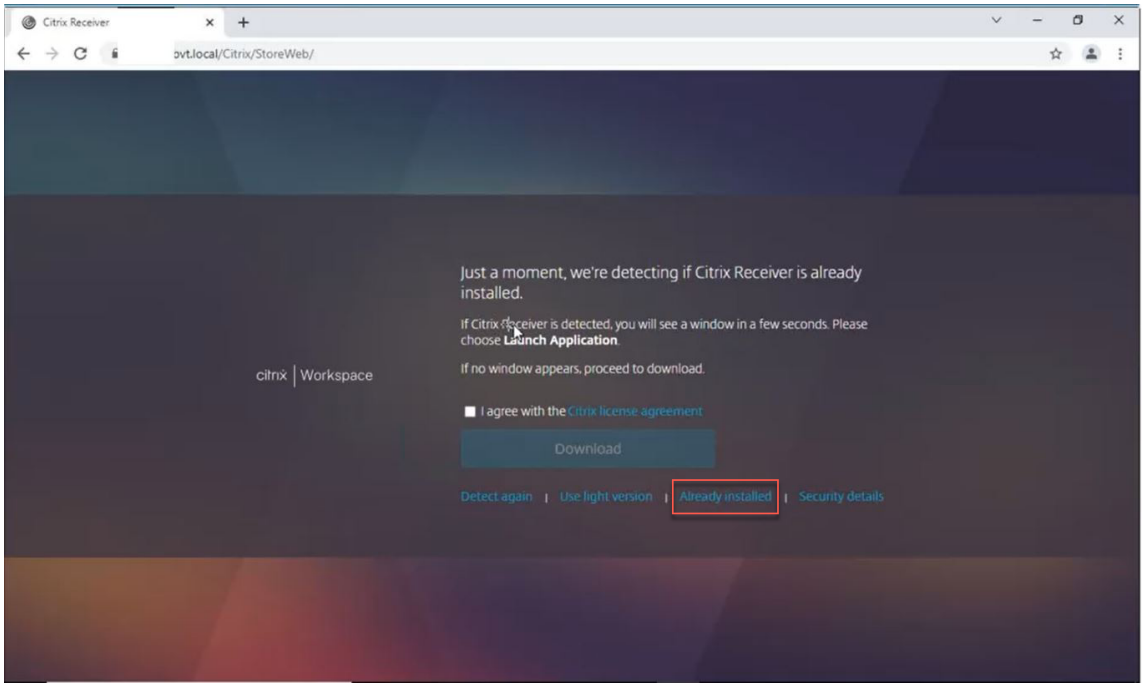
Ce cas de figure peut se produire si vous avez cliqué sur **Utiliser la version simplifiée** lors de la détection de l'application Citrix Workspace, comme indiqué sur l'écran suivant :



- Le navigateur ne détecte pas l'application Citrix Workspace.



Ce cas de figure peut se produire si vous avez cliqué sur **Déjà installé** lors de la détection de l'application Citrix Workspace, comme indiqué sur l'écran suivant :



Solution : pour corriger les cas de figure précédents et lancer les sessions activées d'App Protection, cliquez sur **Changer l'application Citrix Workspace** dans les **Paramètres de compte** et attendez que l'application Citrix Workspace soit détectée.

Optimisation

La détection de l'application Citrix Workspace est nécessaire pour lancer les sessions activées d'App Protection. Pour éviter les échecs lors des lancements hybrides de sessions protégées, les administrateurs de StoreFront peuvent utiliser l'action `ApplyUICustomization` de la commande `deploy-solution.ps1`, et masquer les options **Utiliser la version simplifiée** et **Déjà installé**.

Calendrier de publication de l'application Citrix Workspace

May 31, 2024

Ce calendrier de publication illustre la fréquence de publication des versions de l'application Citrix Workspace. Bien que les dates exactes peuvent changer, nous souhaitons vous aider à planifier à l'avance. Nous voulons également faciliter la gestion des déploiements de l'application Citrix Workspace.

Vous pouvez télécharger les nouvelles versions à partir de la page Téléchargements de l'application Citrix Workspace. Les applications Citrix Workspace pour Android, Citrix Workspace pour iOS et Citrix

Workspace pour Windows (Store) sont également disponibles en téléchargement depuis leurs magasins d'applications respectifs. Si vous avez activé les mises à jour de Citrix Workspace pour l'application Citrix Workspace pour Mac ou Windows, vous êtes invité à accepter le téléchargement et l'installation des mises à jour. Envisagez de vous abonner à notre flux RSS pour recevoir des alertes lorsque de nouvelles versions sont disponibles.

Pour de plus amples informations sur les fonctionnalités disponibles dans chaque application Citrix Workspace, consultez le Tableau des fonctionnalités de l'application Citrix Workspace.

Pour de plus amples informations, consultez la section Étapes clés du cycle de vie de l'application Citrix Workspace.

Cadence de publication

Les plates-formes d'application Citrix Workspace suivantes suivent une cadence de publication trimestrielle :

- Linux
- Mac
- Windows

Les plates-formes d'application Citrix Workspace suivantes suivent une cadence de publication de six semaines :

- ChromeOS
- HTML5

Les plates-formes d'application Citrix Workspace suivantes suivent une cadence de publication mensuelle :

- Android
- iOS

> **Remarque :**
>
> Les applications Citrix Workspace pour Windows, Citrix Workspace pour Mac, Citrix Workspace pour Android et Citrix Workspace pour iOS proposeront à l'avenir des versions majeures et mineures au cours d'un trimestre. Les versions mineures seront désignées par la mention « .10 » et elles incluront des améliorations mineures en termes de qualité et de performances. Les versions mineures « .10 » ne devraient pas comporter de fonctionnalités majeures.

Dates de sortie cibles pour les applications de bureau

Application Citrix Workspace	Février 2024	Mars 2024	Avril 2024	Mai 2024	Juin 2024	Juillet 2024	Août 2024	Septembre 2024	Octobre 2024	Novembre 2024	Décembre 2024
Windows		-	☑	☑	☒	-	☑	☒	-	☑	-
Windows LTSR	☒	-	☑	-	☒	-	-	☒	-	-	☒
Mac	-	-	☑	☒	☑	-	☑	☒	-	☑	-
ChromeOS	☒	-	☑	☑	☑	-	☑	☑	☑	-	☑
HTML5 Linux	-	☑	-	☑	-	-	☑	-	-	☑	-

Application Citrix Workspace	Février 2024	Mars 2024	Avril 2024	Mai 2024	Juin 2024	Juillet 2024	Août 2024	Septembre 2024	Octobre 2024	Novembre 2024	Décembre 2024

Remarque : le symbole ☑ indique les versions majeures et le symbole ☒ indique les versions mineures. Le symbole ☒ indique des mises à jour cumulatives (CU, Cumulative Update).

Dates de sortie cibles pour les applications mobiles et tablettes

Les applications Citrix Workspace pour Android et Citrix Workspace pour iOS suivent une cadence de publication mensuelle.

Application Citrix Workspace	Mars 2024	Avril 2024	Mai 2024	Juin 2024	Juillet 2024	Août 2024	Septembre 2024	Octobre 2024	Novembre 2024	Décembre 2024
Android et iOS	☑	☒	☑	☒	☑	☒	☑	☒	☑	☒

Application Citrix Workspace	Mars 2024	Avril 2024	Mai 2024	Juin 2024	Juillet 2024	Août 2024	Septembre 2024	Octobre 2024	Novembre 2024	Décembre 2024

Remarque : le symbole ☑ indique les versions majeures et le symbole ☒ indique les versions mineures. Les versions mineures sont des versions facultatives conçues pour répondre à des exigences ou à des amélio-

> **Clause d'exclusion de responsabilité**
>
> Le développement, la publication et les échéances indiqués pour nos produits restent à notre seule discrétion et sont susceptibles d'être modifiés sans préavis ni consultation. Les informations sont fournies à titre informatif uniquement et ne constituent pas un engagement, une promesse ou une obligation juridique de fournir du matériel, du code ou des fonctionnalités et ne doivent pas être utilisées pour motiver des décisions d'achat ou être incorporées à un contrat.

Tableau des fonctionnalités de l'application Citrix Workspace

June 19, 2024

L'application Citrix Workspace fournit une gamme de fonctionnalités selon les plates-formes ou les systèmes d'exploitation. Grâce à ce tableau des fonctionnalités, vous pouvez clairement comprendre la disponibilité des fonctionnalités sur différentes plates-formes. Dans chaque section, sous le tableau des fonctionnalités, vous trouverez le tableau des définitions qui décrit chaque fonctionnalité en bref.

Citrix Workspace

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Citrix Virtual Apps	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Citrix Virtual Desktops	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Citrix Secure Private Access	Oui	Oui	Non	Oui	Oui	Oui	Non	Non

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Citrix Enterprise Browser (anciennement Citrix Workspace Browser)	Oui	Non	Oui	Oui	Non	Non	Non	Non
Applications Web/SaaS avec SSO	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Applications mobiles	Non	Non	Non	Non	Oui	Oui	Non	Non
Citrix Service de personnalisation des applications	Oui	Non	Non	Oui	Oui	Oui	Non	Non

Fonctionnalité	Définition
Citrix Virtual Apps	Accédez à Citrix Virtual Apps via les droits Citrix DaaS ou Citrix Virtual Apps and Desktops.
Citrix Virtual Desktops	Accédez à Citrix Virtual Desktops via les droits Citrix DaaS ou Citrix Virtual Apps and Desktops.

Fonctionnalité	Définition
Citrix Secure Private Access	Grâce à Citrix Secure Private Access, les administrateurs informatiques peuvent contrôler l'accès aux applications SaaS approuvées. En outre, grâce à une expérience d'authentification unique simplifiée, les administrateurs peuvent protéger le réseau et les appareils des utilisateurs finaux de l'entreprise contre les logiciels malveillants et les fuites de données en filtrant l'accès à des sites Web et à des catégories de sites Web spécifiques.
Citrix Enterprise Browser	Navigateur fourni avec l'application Citrix Workspace pour accéder aux applications SaaS et Web en toute sécurité.
Applications Web/SaaS avec SSO	Accédez aux applications SaaS/Web configurées à l'aide de Secure Workspace Access avec l'authentification unique (SSO).
Applications mobiles Citrix	Accédez aux applications mobiles Citrix agrégées par Citrix Endpoint Management, anciennement connu sous le nom de XenMobile.
Mises à niveau des applications mobiles Citrix	Accédez aux applications mobiles Citrix agrégées par Citrix Endpoint Management, anciennement connu sous le nom de XenMobile.
Service de personnalisation des applications	Permet de configurer une expérience personnalisée selon l'entreprise. Vous pouvez utiliser un nom d'application personnalisé et une icône avec co-branding pour votre application Citrix Workspace dans tout le flux de travail de l'application.

Gestion de Workspace

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Configuration automatique à l'aide de DNS pour la détection basée sur une adresse e-mail	Oui	Oui	Non	Oui	Oui	Oui	Non	Non
Paramètres de gestion centralisée	Oui	Oui	Oui	Non	Non	Non	Non	Oui
Global App Config service (Workspace)	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui
Global App Config Service (StoreFront)	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui
Mises à jour de l'App Store	Non	Non	Non	Non	Oui	Oui	Non	Non

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Mises à jour automatiques de Citrix	Oui	Oui	Non	Oui	Non	Non	Non	Non
Gestion des applications clientes	Oui	Non	Non	Non	Non applicable	Non applicable	Non applicable	Non applicable

Fonctionnalité	Définition
Configuration automatique à l'aide de DNS pour la détection basée sur une adresse e-mail	Activez la configuration de l'application Citrix Workspace via des paramètres détectés automatiquement.
Paramètres de gestion centralisée	Configuration de l'application à partir d'un service centralisé, par exemple, la gestion Google Chrome ou les objets de stratégie de groupe
Global App Config service (Workspace)	Global App Config Service pour Citrix Workspace permet à un administrateur Citrix de fournir les URL du service Workspace et les paramètres de l'application Citrix Workspace via un service géré de manière centralisée.
Global App Config Service (StoreFront)	Global App Config Service pour Citrix StoreFront permet à un administrateur Citrix de fournir les paramètres de l'application Citrix Workspace via un service géré de manière centralisée.
Mises à jour de l'App Store	Mises à jour du magasin d'applications du fournisseur

Fonctionnalité	Définition
Mises à jour automatiques de Citrix	Mises à jour pour Windows et Mac via la fonctionnalité de mise à jour automatique de Citrix
Gestion des applications clientes	Permet à l'application Citrix Workspace de devenir une application cliente unique requise sur le terminal pour installer et gérer des agents tels que Secure Access Agent et le plug-in Endpoint Analysis (EPA). Grâce à cette fonctionnalité, les administrateurs peuvent facilement déployer et gérer les agents requis à partir d'une console de gestion unique.

Interface utilisateur

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Desktop Viewer/Barre d'outils	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Multi-tâches	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Sessions Follow Me (Contrôle de l'espace de travail)	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Fonctionnalité	Définition
Desktop Viewer/Barre d'outils	Active le contrôle en session des fonctions de session telles que l'envoi de Ctrl+Alt+Suppr via une barre d'outils.
Multi-tâches	Permet d'utiliser plusieurs applications et bureaux en même temps.
Sessions Follow Me (Contrôle de l'espace de travail)	Permet aux utilisateurs de passer d'un appareil à l'autre et de se connecter automatiquement à toutes leurs sessions.

HDX Host Core

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Transport adaptatif	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
Débit adaptatif HDX	Oui	Oui	Non	Non	Non	Non	Non	Non
Prise en charge de SDWAN	Oui	Oui	Oui	Oui	Non	Non	Oui	Oui
Fiabilité de session	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Reconnexion automatique des clients	Oui	Oui	Oui	Oui	Non	Oui	Non	Non

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Partage de session	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
ICA multiport	Oui	Oui	Oui	Non	Non	Non	Non	Non

Fonctionnalité	Définition
Transport adaptatif	Permet le transport EDT pour HDX afin d'améliorer le débit indépendamment des conditions du réseau.
Prise en charge de SDWAN	Permet l'accélération SDWAN pour QoS, TCP, la compression et la déduplication.
Fiabilité de session	Maintient les sessions actives sur l'écran de l'utilisateur lorsque la connectivité au réseau est interrompue.
Reconnexion automatique des clients	Affiche une invite et reconnecte la session en cas d'interruption de connexion.
Partage de session	Permet à l'application publiée de s'exécuter sur la même connexion que les autres applications publiées lorsqu'elle est déjà exécutée sur le même serveur.
ICA multiport	Permet la prise en charge de plusieurs ports TCP pour le trafic HDX afin d'améliorer la qualité de service.

E/S HDX/Périphériques/Impression

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Impression locale	Oui	Oui	Oui	Oui	Oui	Non	Oui	Oui
Redirection USB générique	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Mappage des lecteurs clients/-Transfert de fichiers	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
TWAIN 2.0	Oui	Non	Non	Non	Non	Non	Non	Non

Fonctionnalité	Définition
Impression locale	Permet aux utilisateurs d'imprimer des documents via des imprimantes partagées ou locales.
Redirection USB générique	Permet d'utiliser des périphériques USB au sein de la session. Par exemple, clavier, souris, webcam externe, etc.
Mappage des lecteurs clients/Transfert de fichiers	Permet d'utiliser des lecteurs clients intégrés ou connectés pour le stockage des données.
TWAIN	Autorise le mappage des périphériques TWAIN clients, tels que des appareils photo numériques ou des scanneurs.

Intégration HDX

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Local App Access	Oui	Oui	Non	Non	Non	Non	Non	Non
Multipoint	Oui	Oui	Non	Non	Oui	Oui	Oui	Oui
Mobility Pack	Oui	Oui	Non	Non	Oui	Oui	Oui	Oui
HDX Insight	Oui	Oui	Oui	Oui	Non	Non	Oui	Oui
HDX Insight avec NSAP VC	Oui	Oui	Oui	Oui	Oui *(3)*	Oui *(3)*	Non	Non
Matrice d'expérience EUEM	Oui	Oui	Oui	Oui	Non	Oui	Oui	Oui
Redirection bidirectionnelle du contenu	Oui	Oui	Non	Non	Non	Non	Non	Non
Redirection des URL	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Redirection de contenu du navigateur	Oui	Non	Oui	Non	Non	Non	Non	Oui

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Ouverture de fichier dans l'application Citrix Workspace	Oui	Oui	Oui	Non	Oui	Oui	Non	Oui
Services basés sur la localisation (localisation disponible via la description dans l'API)	Oui	Oui	Non	Non	Oui	Oui	Non	Non

Fonctionnalité	Définition
Local App Access	Accédez à l'application locale sur un appareil client au sein de la session.
Multipoint	Permet le contrôle multipoint à 10 doigts des applications et des bureaux Windows/Linux.

Fonctionnalité	Définition
Mobility Pack	Permet d'utiliser les fonctionnalités d'expérience native des appareils (par exemple, le clavier contextuel automatique et les commandes de l'interface utilisateur de l'appareil local) et les ordinateurs de bureau optimisés pour les tablettes.
HDX Insight	Fournit une visibilité sur les heures de démarrage/fin de session à l'aide des mesures de performance réseau ICA.
HDX Insight avec canal virtuel NSAP	Fournit une visibilité sur l'heure de démarrage/fin de session à l'aide de l'expérience d'application NetScaler ou du canal virtuel NSAP pour obtenir des informations HDX.
Matrice d'expérience EUEM	Fournit aux administrateurs Citrix une visibilité sur les durées d'ouverture de session via le bureau virtuel Citrix appelé auparavant XenDesktop 7 Director.
Redirection bidirectionnelle du contenu	Permet la redirection d'URL client vers hôte et hôte vers client.
Redirection des URL	Permet l'exécution d'applications localement sur le client.
Redirection de contenu du navigateur	Permet de rediriger une page Web entière (fenêtre d'affichage d'un navigateur) vers le point de terminaison pour un rendu local, déchargeant ainsi le serveur.
Ouverture de fichier dans l'application Citrix Workspace	Permet d'ouvrir un fichier local dans l'application Citrix Workspace à l'aide d'une application hébergée (redirection de contenu client vers serveur).
Services basés sur la localisation (localisation disponible via la description dans l'API)	Permet aux informations d'emplacement d'être utilisées par les applications fournies par Citrix Virtual Desktops, appelé auparavant XenDesktop.

Multimédia HDX

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Lecture audio	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Audio bidirectionnel (VoIP)	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Redirection de webcam	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Lecture vidéo	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Optimisation pour Microsoft Teams	Oui	Oui	Oui (x64 uniquement)	Oui	Non	Non	Oui	Oui
Pack d'optimisation pour Skype Entreprise	Oui	Oui	Oui	Oui	Non	Non	Non	Non
Optimisation des communications unifiées Cisco Jabber	Oui	Oui	Oui	Non	Non	Non	Non	Non

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Redirection multimédia Windows	Oui	Oui	Oui	Non	Non	Non	Non	Non
Audio UDP	Oui	Oui	Oui	Non	Non	Non	Non	Non

Fonctionnalité	Définition
Lecture audio	Permet d'utiliser la lecture audio rendue par le serveur.
Audio bidirectionnel (VoIP)	Permet d'utiliser des applications de collaboration par softphone et chat audio hébergées.
Redirection de webcam	Permet d'utiliser des applications de collaboration par chat vidéo à l'aide d'une webcam locale.
Lecture vidéo	Permet de visualiser des vidéos enregistrées.
Optimisation pour Microsoft Teams	Décharge le traitement multimédia Microsoft Teams du serveur Citrix vers l'appareil utilisateur.
Optimisation pour Skype Entreprise	Décharge le traitement multimédia Skype Entreprise du serveur Citrix vers l'appareil utilisateur. Pour l'application Citrix Workspace pour Android, nous prenons uniquement en charge les appareils Chrome.
Optimisation des communications unifiées Cisco Jabber	Décharge le traitement multimédia Jabber du serveur Citrix vers l'appareil utilisateur.
Redirection multimédia Windows	Permet le rendu multimédia Windows sur l'appareil utilisateur, déchargeant ainsi le serveur.

Fonctionnalité	Définition
Audio UDP	Prise en charge de l'entrée et de la sortie audio via UDP.

Sécurité

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
TLS 1.2	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
TLS 1.0/1.1	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
DTLS 1.0	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
DTLS 1.2	Oui	Oui	Oui	Oui	Non	Non	Non	Non
Certificat SHA2	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Smart Access	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Accès à distance via Citrix Gateway	Oui *(1)*	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Workspace pour Web Access	Oui	Oui	Oui	Oui	Via un fichier ICA	Oui	Oui	Oui
IPv6	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
App Protection	Oui	Oui	Oui	Oui	Non	Non	Non	Non

Fonctionnalité	Définition
TLS 1.2	Successeur de SSL, forte sécurité des canaux de communication.
TLS 1.0/1.1	Successeur de SSL, forte sécurité des canaux de communication.
DTLS 1.0	DTLS est un dérivé du protocole SSL. Il fournit les mêmes services de sécurité (intégrité, authentification et confidentialité) mais via le protocole UDP.
DTLS 1.2	DTLS est un dérivé du protocole SSL. Il fournit les mêmes services de sécurité (intégrité, authentification et confidentialité) mais via le protocole UDP.
Certificat SHA2	Possibilité d'utiliser des certificats SHA2.
Smart Access	Contrôle l'accès aux applications disponibles à l'aide de stratégies et de filtres Gateway.
Accès à distance via Gateway	Fournit aux utilisateurs un accès sécurisé aux applications d'entreprise, aux bureaux virtuels et aux données, où qu'ils soient, sans client VPN.
Workspace pour Web Access	Accès aux applications hébergées ou aux bureaux virtuels à l'aide d'un navigateur.
IPv6	Permet une utilisation sur les réseaux IPV6.

Graphiques HDX

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
SuperCodec amélioré H.264	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Accélération matérielle client	Oui	Oui	Oui	Oui	Non	Oui	Non	Non
Graphiques 3DPro	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Prise en charge de moniteur externe	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Redirection Desktop Composition	Oui	Oui	Non	Non	Non	Non	Non	Non
Véritable multi-moniteurs	Oui	Oui	Oui	Oui	Non	Non	Oui	Oui

Fonctionnalité	Définition
SuperCodec amélioré H.264	Permet une mise à disposition rationalisée des applications à l'aide du supercodec XenApp/Desktop 7.X amélioré H264.
Accélération matérielle client	Permet l'accélération matérielle pour les fonctionnalités HDX telles que les graphiques et la webcam. L'utilisation des capacités matérielles varie en fonction des différentes applications Citrix Workspace.
Graphiques 3DPro	Permet d'utiliser des applications graphiques professionnelles 3D hébergées dans le centre de données.
Prise en charge de moniteur externe	Permet l'utilisation d'un moniteur externe.

Fonctionnalité	Définition
Redirection Desktop Composition	Permet d'utiliser la commande graphique distante du client pour le rendu afin de garantir la capacité à monter en charge du serveur. Déconseillé dans la version 12.9 de Receiver pour Mac.
Véritable multi-moniteurs	XenApp ou XenDesktop crée le même nombre de moniteurs que celui pris en charge par le client.

Authentification

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Authentification fédérée (SAML/Azure AD)	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
VPN complet ADC	Oui	Oui	Oui	Oui	Non	Non	Non	Non
Jeton logiciel RSA	Non	Non	Non	Non	Oui	Oui	Non	Non
SMS de réponse à une demande d'authentification (Radius)	Oui	Oui	Non	Oui	Non	Non	Non	Non

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Authentification du certificat utilisateur via Gateway (via l'application Workspace native)	Non	Non	Non	Non	Oui	Oui	Oui	Oui
Authentification du certificat utilisateur via Gateway (via le navigateur)	Oui *(4)*	Oui *(4)*	Non	Oui	Non	Non	Oui	Oui
Carte à puce (CAC, PIV, etc.)	Oui	Oui	Oui	Oui	Oui	Oui	Non	Oui
Carte de proximité/sans contact	Oui	Oui	Oui	Non	Non	Non	Non	Oui

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Insertion d'informations d'identification (par exemple, Fast Connect, Store-browse)	Oui	Oui	Oui	Non	Non	Non	Non	Oui
Authentification pass-through	Oui	Oui	Non	Non	Non	Non	Non	Non
Enregistrer les informations d'identification *Sur site et Store-Front uniquement	Oui	Oui	Non	Oui	Non	Non	Non	Non
Authentification ADC nFactor	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
OTP natif ADC	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Authentification bio-métrique (Touch ID, Face ID)	Non	Non	Non	Non	Oui	Non	Non	Non
Authentification unique pour les applications mobiles Citrix	Non	Non	Non	Non	Oui	Oui	Non	Non
Accès anonyme au magasin	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

Fonctionnalité	Définition
Authentification fédérée (SAML/Azure AD)	Permet au serveur FAS d'utiliser l'authentification utilisateur qui délègue le serveur Microsoft ADFS (ou tout autre IdP compatible SAML) via Azure AD ou SAML.
VPN complet ADC (NetScaler)	Crée un tunnel VPN complet pour Gateway.
Jeton logiciel RSA	Permet une authentification simplifiée lors de l'utilisation de jetons logiciels RSA.
SMS de réponse à une demande d'authentification (Radius)	Permet d'utiliser l'authentification par réponse, par exemple l'utilisation de codes d'accès SMS.

Fonctionnalité	Définition
Authentification du certificat utilisateur via Gateway (via le navigateur uniquement)	Permet d'utiliser les certificats des utilisateurs comme facteur d'authentification avec Gateway, pour l'authentification basée sur un navigateur sous Windows.
Carte à puce (CAC, PIV, etc.)	Permet d'utiliser une carte à puce cryptographique compatible PC/SC standard pour l'authentification et la signature.
Carte de proximité/sans contact	Permet aux utilisateurs d'utiliser des applications ou des bureaux Citrix en s'authentifiant avec une carte à puce de proximité ou sans contact.
Insertion d'informations d'identification (par exemple, Fast Connect, Storebrowse)	Permet aux utilisateurs d'utiliser des applications ou des bureaux Citrix en s'authentifiant avec une carte à puce de proximité ou sans contact. Storebrowse est un utilitaire de ligne de commande disponible avec l'application Citrix Workspace pour Windows. Vous pouvez utiliser Storebrowse pour personnaliser l'application Citrix Workspace en scriptant l'utilitaire Storebrowse.
Authentification pass-through	Transmet les informations d'identification de l'utilisateur à un site d'interface Web, puis aux serveurs Citrix Virtual Apps and Desktops. Ce processus empêche les utilisateurs de s'authentifier explicitement à tout moment pendant le processus de lancement de l'application Citrix.
Enregistrer les informations d'identification *Sur site et StoreFront uniquement	Permet l'enregistrement des informations d'identification sur site et uniquement à l'aide de Citrix StoreFront.
OTP natif Gateway	Gateway prend en charge les mots de passe à usage unique (OTP) sans avoir à utiliser de serveur tiers, en conservant l'intégralité de la configuration sur l'appliance NetScaler.

Fonctionnalité	Définition
Authentification nFactor NetScaler	L'authentification nFactor permet des flux d'authentification dynamiques basés sur le profil de l'utilisateur. Parfois, ces flux peuvent être de simples flux intuitifs pour l'utilisateur. La version minimale de NetScaler requise est 12.1.49.x.
Authentification biométrique (Touch ID, Face ID)	Permet les authentifications biométriques telles que Touch ID et Face ID.
Authentification unique pour les applications mobiles Citrix	Active l'authentification unique pour les applications mobiles Citrix.
Accès anonyme au magasin	Prise en charge de l'accès des utilisateurs non authentifiés (anonymes)

Expérience de saisie

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Synchronisation de la disposition du clavier : client vers VDA (Windows VDA)	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Synchronisation de la disposition du clavier : client vers VDA (Linux VDA)	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
Synchronisation de la disposition du clavier : VDA vers client (Windows VDA)	Non	Non	Non	Non	Non	Non	Non	Non
Synchronisation de la disposition du clavier : VDA vers client (Linux VDA)	Non	Non	Non	Non	Non	Non	Non	Non

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Mappage de disposition du clavier Unicode	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui
Mode de saisie du clavier : Unicode	Non	Non	Oui	Oui	Oui	Oui	Oui	Oui
Mode de saisie du clavier : scancode	Oui	Oui	Oui	Oui	Non	Non	Oui	Oui
Éditeur IME du serveur	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Éditeur IME client générique (CTXIME) pour les éditeurs IME CJK	Oui	Oui	Non	Oui	Oui	Oui	Oui	Oui
Interface de ligne de commande	Oui	Oui	Non	Non	Non	Non	Non	Non

Fonctionnalité	Windows 2403.1 et Windows Store 2403.1	Windows 2402 LTSR	Linux 2405	Mac 2402.10	iOS 24.5.0	Android 24.5.0	HTML5 2404.1	ChromeOS 2405
Interface utilisateur des paramètres de synchronisation du clavier et configurations	Oui	Oui	Oui	Oui	Oui	Oui	Non	Non
Interface utilisateur des paramètres de mode de saisie et configurations	Non	Non	Oui	Oui	Oui	Non	Non	Non
Interface utilisateur des paramètres de la barre de langue et configurations	Oui	Oui	Non	Oui	Non	Non	Non	Non

Fonctionnalité	Définition
Synchronisation de la disposition du clavier : client vers VDA (Windows VDA)	Permet aux utilisateurs de synchroniser les dispositions de clavier actives ou de basculer entre leurs dispositions de clavier préférées sur la machine cliente. La disposition du clavier sur la machine cliente est automatiquement définie sur le Windows VDA.
Synchronisation de la disposition du clavier : client vers VDA (Linux VDA)	Permet aux utilisateurs de synchroniser les dispositions de clavier actives ou de basculer entre leurs dispositions de clavier préférées sur la machine cliente. La disposition du clavier sur la machine cliente est automatiquement définie sur le Linux VDA.
Synchronisation de la disposition du clavier : VDA vers client (Windows VDA)	Permet aux utilisateurs de synchroniser les dispositions de clavier actives ou de basculer entre leurs dispositions de clavier préférées sur le Windows VDA. La disposition du clavier sur le Windows VDA est automatiquement définie sur la machine cliente.
Synchronisation de la disposition du clavier : VDA vers client (Linux VDA)	Permet aux utilisateurs de synchroniser les dispositions de clavier actives ou de basculer entre leurs dispositions de clavier préférées sur le Linux VDA. La disposition du clavier sur le Linux VDA est automatiquement définie sur la machine cliente.
Mappage de disposition du clavier Unicode	Prise en charge du mappage de disposition du clavier Unicode pour VDA Windows avec une application Citrix Workspace non Windows.
Mode de saisie du clavier : Unicode	Le mode de saisie Unicode envoie la touche du clavier côté client au VDA et le VDA génère le même caractère dans le VDA. Applique la disposition du clavier côté client.
Mode de saisie du clavier : scancode	Le mode de saisie Scancode envoie la position des touches du clavier côté client au VDA et le VDA génère le caractère correspondant. Applique la disposition du clavier côté serveur.
Éditeur IME du serveur	Fournit la convivialité et l'expérience de l'éditeur IME côté service (ou VDA).

Fonctionnalité	Définition
Éditeur IME client générique (CTXIME) pour les éditeurs IME CJK	Fournit une meilleure utilisabilité de l'éditeur IME client et une expérience plus homogène pour les langues d'Asie de l'Est (chinois, japonais, coréen).
Interface de ligne de commande	Les utilisateurs peuvent activer ou désactiver l'éditeur IME client à l'aide des interfaces de ligne de commande.
Interface utilisateur des paramètres de synchronisation du clavier et configurations	Les utilisateurs peuvent choisir différentes options de synchronisation de la disposition du clavier à l'aide de l'interface graphique.
Interface utilisateur des paramètres de mode de saisie et configurations	Les utilisateurs peuvent choisir différentes options de mode de saisie du clavier à l'aide de l'interface graphique.
Interface utilisateur des paramètres de la barre de langue et configurations	Les utilisateurs peuvent choisir d'afficher ou de masquer la barre de langue distante dans une session d'application VDA à l'aide de l'interface graphique. La barre de langue affiche la langue d'entrée préférée dans une session.
Modèle d'administration GPO pour la synchronisation de la disposition du clavier	Les administrateurs peuvent remplacer les configurations de synchronisation de la disposition du clavier en déployant les stratégies correspondantes à partir du modèle d'administration de l'objet de stratégie de groupe de l'application Citrix Workspace.

Indicateurs de table

Indicateur	Description
1	StoreFront uniquement
2	HDX 3D Pro revient au format JPEG pour ces applications Citrix Workspace. 3 Mbit/s sont recommandés plutôt que 1,5 Mbit/s avec la compression profonde H.264.

Indicateur	Description
3	Pour le canal virtuel NSAP, prise en charge de l'application Workspace pour iOS/Android, mais pour ADC/ADM, la prise en charge est toujours en attente.
4	La méthode d'authentification User Cert Auth via Gateway (via le navigateur uniquement) ne prend pas en charge la détection des clients de l'application Citrix Workspace. Vous ne pouvez ouvrir une application ou un bureau virtuel à l'aide de l'application Citrix Workspace qu'après avoir téléchargé le fichier ICA.

> **Remarque :**
>
> Le développement, la publication et les échéances de toutes les fonctionnalités indiqués pour nos produits restent à notre seule discrétion. Les informations sont fournies ici à titre informatif uniquement et ne constituent pas un engagement, une promesse ou une obligation juridique de fournir du matériel, du code ou des fonctionnalités et ne doivent pas être utilisées pour motiver des décisions d'achat ou être incorporées à un contrat. Le développement, la publication et les échéances de toutes les fonctionnalités indiqués pour nos produits restent à notre seule discrétion et sont susceptibles d'être modifiés sans préavis ni consultation.