Citrix Remote Browser Isolation

Machine translated content

Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

Contents

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Remote Browser Isolation

July 2, 2024

Citrix Remote Browser Isolation Service (anciennement Secure Browser Service) protège le réseau d'entreprise contre les attaques basées sur les navigateurs en isolant les activités de navigation sur le Web. Remote Browser Isolation Service fournit un accès distant sécurisé et cohérent aux applications Web hébergées sur Internet sans configuration du terminal. Les administrateurs peuvent déployer des navigateurs isolés distants rapidement, ce qui offre un retour sur investissement instantané. En isolant la navigation Internet, les administrateurs informatiques peuvent offrir aux utilisateurs un accès Internet sécurisé sans compromettre la sécurité.

Les utilisateurs se connectent via Citrix Workspace (ou Citrix Receiver) et peuvent ouvrir des applications Web dans le navigateur Web configuré. Le site Web ne transfère pas directement les données de navigation vers ou depuis l'appareil utilisateur, ce qui garantit une expérience sécurisée.

Remote Browser Isolation Service peut publier des navigateurs isolés distants à utiliser avec :

- **Des applications Web externes authentifiées par code secret partagé.** Si vous publiez un navigateur avec une authentification par code secret partagé, les utilisateurs doivent entrer le code secret pour lancer une application.
- **Des applications Web externes authentifiées.** Lorsque vous publiez des applications Web externes authentifiées et que vous lancez les applications à l'aide de Citrix Workspace, Remote Browser Isolation Service nécessite un emplacement de ressources contenant au moins un Cloud Connector (deux ou plus sont recommandés). Pour plus de détails, voir Citrix Cloud Connector. Pour les applications authentifiées, vous devez ajouter des utilisateurs avec la bibliothèque Citrix Cloud.
- **Des applications Web externes non authentifiées.** Lorsque vous publiez des applications Web externes non authentifiées et que vous lancez les applications à l'aide de Citrix Workspace, Remote Browser Isolation Service nécessite un emplacement de ressources contenant au moins un Cloud Connector (deux ou plus sont recommandés). Pour plus de détails, voir Citrix Cloud Connector.

  Bien que cela ne soit généralement pas recommandé, des applications Web externes non authentifiées peuvent être utilisées pour une preuve de concept simple.

Pour plus d'informations, voir Publier un navigateur isolé distant.

Le service propose également :

- Intégration d'applications publiées avec Citrix Workspace
- Intégration d'applications publiées avec StoreFront local

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Liste d'autorisation d'adresses URL simples pour garantir la sécurité
- Surveillance de l'utilisation
- Commandes d'utilisation du presse-papiers, de l'impression, du mode kiosque, du basculement de région et du mappage de lecteurs clients

Service Remote Browser Isolation avec Citrix Secure Private Access

Vous pouvez lancer les navigateurs publiés du service Remote Browser Isolation à l'aide de la console Citrix Secure Private Access pour accéder aux applications Web, TCP et SaaS d'entreprise. Vous pouvez également rediriger les sites Web non autorisés de sorte qu'ils s'ouvrent dans les navigateurs publiés du service Remote Browser Isolation via Citrix Secure Private Access.

Pour plus d'informations sur l'accès aux navigateurs distants isolés via Citrix Secure Private Access, consultez les sections Configurer une stratégie d'accès avec plusieurs règles et sites Web non autorisés dans la documentation de Citrix Secure Private Access.

Articles de référence

- Présentation du service Secure Private Access
- Citrix Cloud
- Recherche en libre-service pour Remote Browser Isolation (Secure Browser)
- Citrix Enterprise Browser
- Informations sur la sécurité et la conformité
- documentation du développeur

Nouveautés dans les produits associés

- Secure Private Access
- Citrix Enterprise Browser
- Citrix Analytics for Security

Nouveautés

October 13, 2022

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Juillet 2022

- **Remote Browser Isolation prend en charge l'authentification pour toutes les applications avec Azure Active Directory.**
  - Les utilisateurs peuvent désormais se connecter à toute application Remote Browser Isolation à partir de Citrix Workspace à l'aide des informations d'identification Azure Active Directory.
  - Lorsque les utilisateurs de Remote Browser Isolation se connectent, ils utilisent la page de connexion Workspace que vous avez configurée pour votre site. Pour plus d'informations, consultez la section Intégration avec Citrix Workspace.

Septembre 2021

- **Remote Browser Isolation prend en charge l'audio bidirectionnel**. L'audio bidirectionnel est disponible dans Remote Browser Isolation.
- **Les lancements de Remote Browser Isolation à partir de launch.cloud.com sont authentifiés par l'authentification Citrix Cloud**. Lorsque les utilisateurs lancent des applications Remote Browser Isolation à l'aide de l'URL launch.cloud.com, l'authentification Citrix Cloud gère leurs informations d'identification. Cela permet d'améliorer la sécurité mais ne modifie pas l'expérience utilisateur.

March 2021

- **Remote Browser Isolation prend en charge l'authentification avec Azure Active Directory**. Les utilisateurs peuvent désormais se connecter à des applications Remote Browser Isolation à partir de Citrix Workspace à l'aide des informations d'identification Azure Active Directory. Pour plus d'informations, consultez la section Intégration avec Citrix Workspace.
- **Remote Browser Isolation vous permet de surveiller et de fermer les sessions actives des utilisateurs**. Remote Browser Isolation fournit le nom d'utilisateur, l'ID de session, l'adresse IP du client, le type d'authentification, le nom de l'application, l'heure de début de session et la durée de session associés aux sessions actives des utilisateurs. Vous pouvez afficher des informations de base sur chaque session active et déconnecter la session si nécessaire. Pour plus d'informations, consultez la section Surveiller les sessions actives.

Versions publiées en 2020

Toutes les versions publiées en 2020 contiennent des améliorations au niveau de la stabilité et des performances globales.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

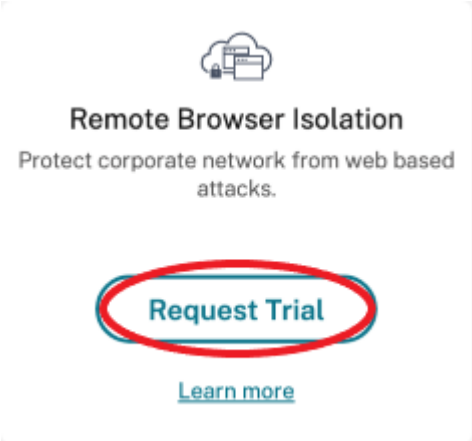
Découvrir Remote Browser Isolation

October 13, 2022

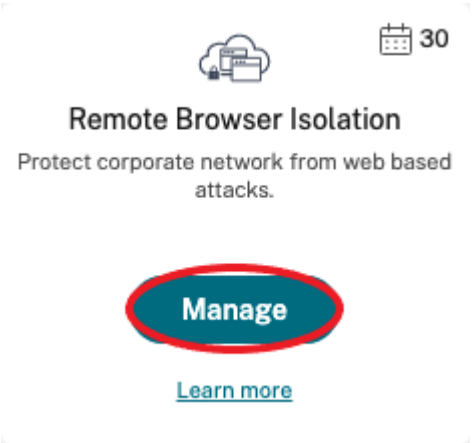
Vous trouverez ci-dessous une vidéo sur la mise en route de Remote Browser Isolation Service (anciennement Secure Browser Service).

1. Connectez-vous à Citrix Cloud. Si vous n'avez pas de compte, consultez Ouvrir un compte Citrix Cloud. Vous pouvez demander une version d'évaluation de 30 jours de Citrix Remote Browser Isolation.
2. Dans la vignette **Remote Browser Isolation**, cliquez sur **Demander version d'évaluation**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

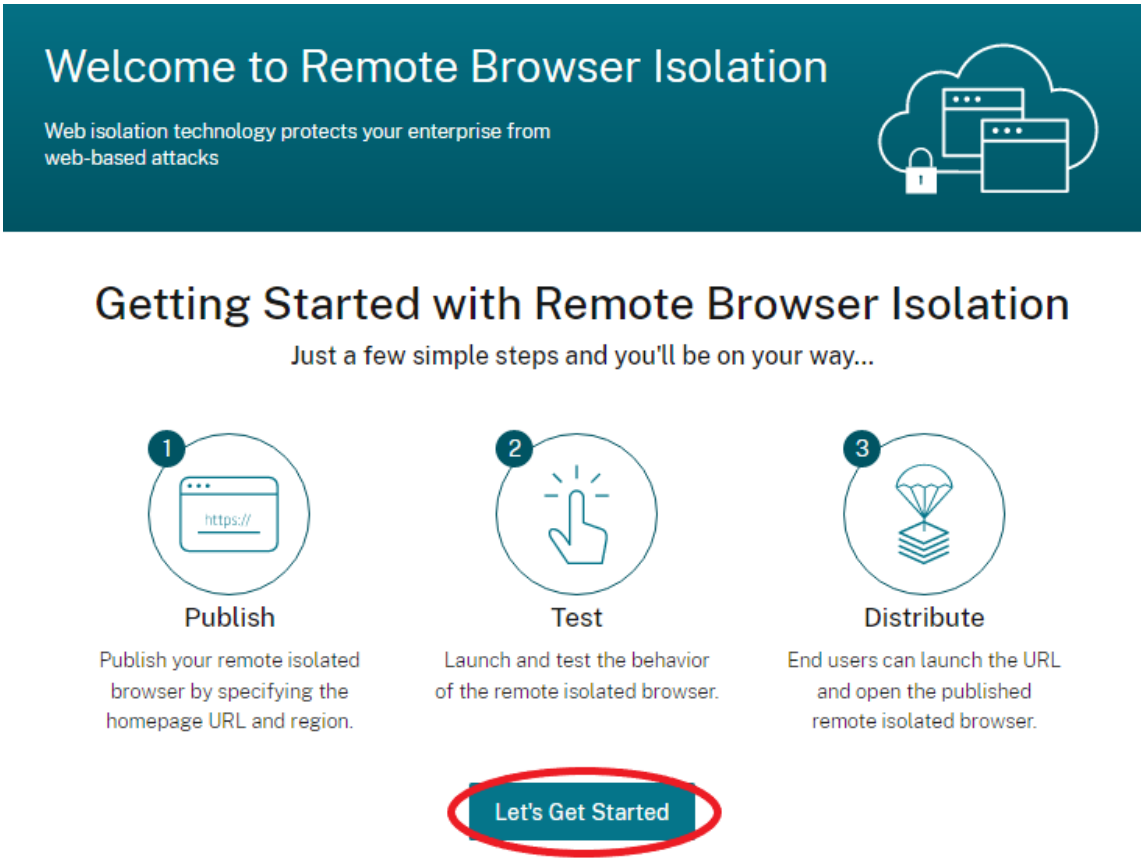


3. Vous allez recevoir un e-mail dans quelques instants (l'e-mail associé à votre compte Citrix Cloud). Cliquez sur le lien **Connexion** de l'e-mail.
4. De retour dans Citrix Cloud, cliquez sur **Gérer** dans la vignette **Remote Browser Isolation**.



5. Sur la page **Bienvenue dans Remote Browser Isolation**, cliquez sur **Démarrer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. Sélectionnez le type de navigateur isolé distant à publier : code secret partagé, authentifié ou non authentifié. Puis cliquez sur **Continuer**.

   Par défaut, les utilisateurs doivent lancer des applications avec authentification par code secret partagé à l'aide de launch.cloud.com. Citrix Workspace et la bibliothèque Citrix Cloud ne prennent pas en charge les applications utilisant un code secret partagé.

   Pour utiliser Citrix Workspace, vous devez publier des applications authentifiées et attribuer explicitement des abonnés (utilisateurs) ou des groupes dans la bibliothèque Citrix Cloud. Les applications non authentifiées sont disponibles pour tous les abonnés de Workspace sans attribution d'utilisateur.

7. Configurez les paramètres suivants :

   - **Nom :** entrez un nom pour l'application que vous créez.
   - **URL de démarrage :** spécifiez l'URL qui s'ouvre lorsque les utilisateurs démarrent une application.
   - **Région :** choisissez l'emplacement/la région du serveur. Les régions disponibles sont les suivantes : Ouest des États-Unis, Est des États-Unis, Asie du Sud-Est, Est de l'Australie et Europe de l'Ouest.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Si vous sélectionnez **Auto**, votre navigateur isolé se connecte à la région la plus proche en fonction de votre géolocalisation.

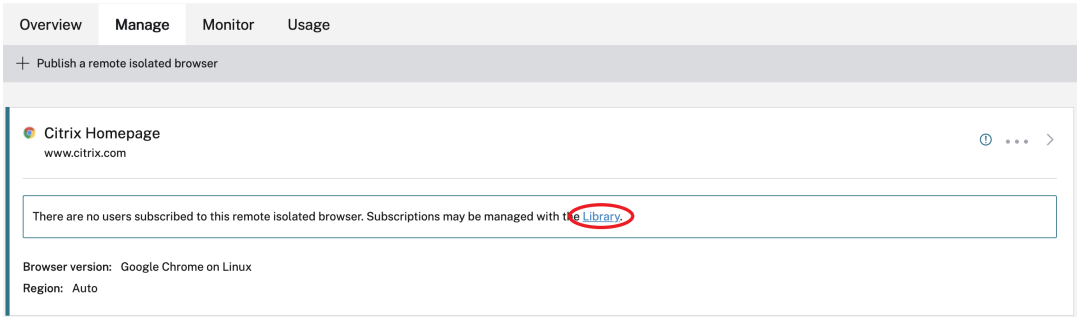
- **Code secret :** si vous avez sélectionné un navigateur doté d'une authentification par mot de passe partagé, saisissez le code secret pour fournir un accès sécurisé amélioré à votre application. Le code secret doit comporter au moins 10 caractères avec au moins 1 numéro et 1 symbole. Assurez-vous d'enregistrer le code secret et de le partager avec vos utilisateurs. Les utilisateurs doivent entrer le code secret lorsqu'ils lancent une application à l'aide de launch.cloud.com.
- **Icône :** par défaut, l'icône de l'exécutable de Google Chrome est utilisée lorsque vous publiez un navigateur isolé. Vous pouvez maintenant choisir votre propre icône pour représenter un navigateur publié.

  Cliquez sur **Changer icône > Sélectionner une icône** pour charger l'icône de votre choix ou choisissez **Utiliser icône par défaut** pour utiliser l'icône Google Chrome existante.

Cliquez sur **Publier**.

8. L'onglet **Gérer** répertorie le navigateur que vous avez publié. Pour lancer le navigateur que vous venez de créer, cliquez sur les points de suspension sur la vignette contenant le navigateur isolé, puis cliquez sur **Lancer navigateur publié**.

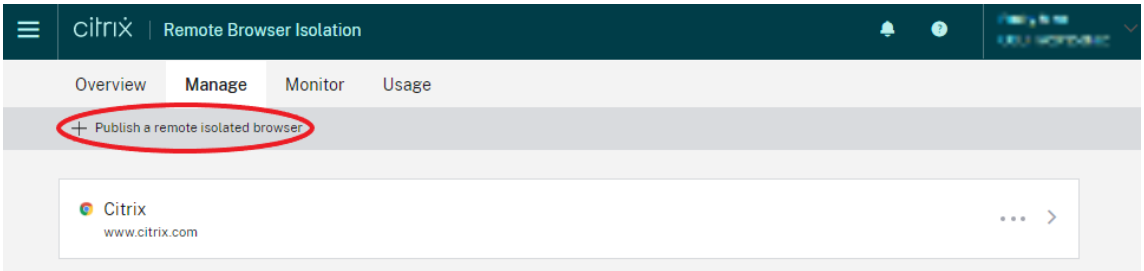
   - Si vous avez publié le navigateur isolé authentifié, vous devez utiliser la bibliothèque Citrix Cloud pour ajouter des utilisateurs ou des groupes. Cliquez sur la flèche droite à la fin de la ligne pour développer le volet d'informations contenant un lien vers la bibliothèque.

     Lorsque vous cliquez sur le lien fourni, vous êtes dirigé vers l'écran Bibliothèque qui contient votre navigateur isolé distant. Cliquez sur les points de suspension de la vignette contenant le navigateur isolé et cliquez sur **Gérer les abonnés**. Pour plus d'informations sur l'ajout d'abonnés, voir Attribuer des utilisateurs et des groupes à des offres de services à l'aide de la bibliothèque.

   Vous pouvez publier un autre navigateur isolé distant en cliquant sur **Publier un navigateur isolé distant** dans l'onglet **Gérer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Pour plus d'informations sur l'achat de Citrix Remote Browser Isolation Service (anciennement service Citrix Secure Browser), visitez https://www.citrix.com/products/citrix-remote-browser-isolation/.

Intégration avec Citrix Workspace

Remote Browser Isolation peut être intégré à Citrix Workspace. Pour s'assurer qu'il est intégré :

1. Connectez-vous à Citrix Cloud.
2. Dans le menu en haut à gauche, sélectionnez **Configuration de l'espace de travail**.
3. Sélectionnez l'onglet **Intégrations de services**.
4. Vérifiez que l'entrée de Remote Browser Isolation Service indique **Activé**. Si ce n'est pas le cas, cliquez sur le menu des points de suspension et sélectionnez **Activer**.

Si vous ne l'avez pas encore fait, configurez l'URL de Workspace, la connectivité externe et l'authentification de l'espace de travail pour votre Workspace, comme décrit dans la section Configuration de l'authentification aux espaces de travail.

Remote Browser Isolation prend en charge l'authentification avec Active Directory et Azure Active Directory. L'authentification avec Active Directory est configurée par défaut. Pour plus d'informations sur la configuration de l'authentification à l'aide de Azure Active Directory, consultez la section Connecter Azure Active Directory à Citrix Cloud.

Si vous configurez l'authentification à l'aide de Azure Active Directory, le domaine local contenant vos contrôleurs de domaine Active Directory doit contenir un (de préférence deux) Cloud Connector.

Intégration avec votre magasin StoreFront local

Les clients Citrix Virtual Apps and Desktops disposant d'un StoreFront local peuvent facilement s'intégrer à Remote Browser Isolation Service pour offrir les avantages suivants :

- Regroupez vos navigateurs isolés distants publiés avec vos applications Citrix Virtual Apps and Desktops existantes pour une expérience de magasin unifiée.
- Utilisez des Citrix Receiver natifs pour une expérience utilisateur optimisée.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Renforcez la sécurité des lancements de Remote Browser Isolation en utilisant votre solution d'authentification multifacteur existante intégrée à votre StoreFront.

Pour plus de détails, voir l'article CTX230272 et la documentation sur la configuration de StoreFront.

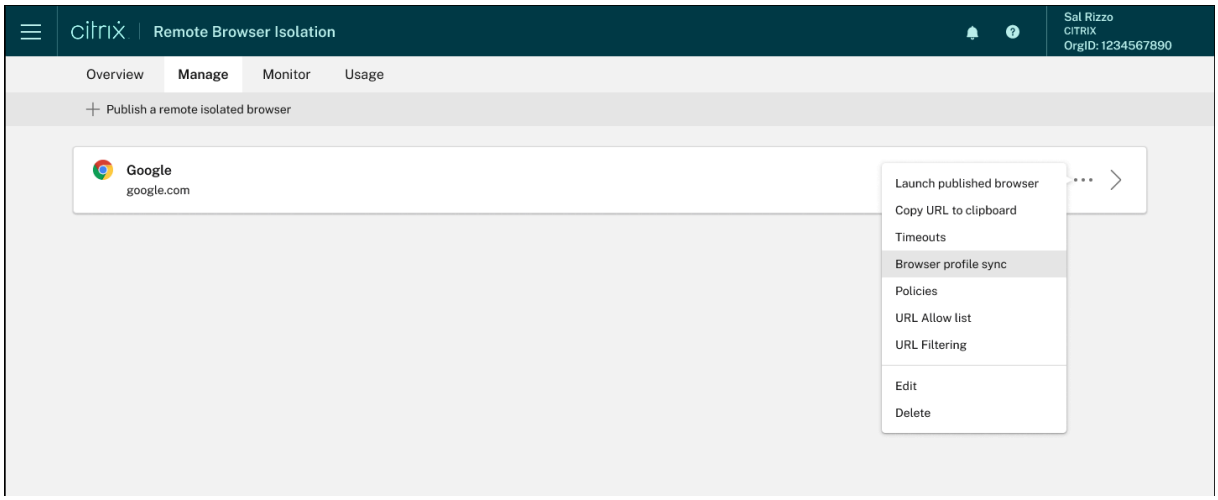
Gérer et surveiller les navigateurs isolés distants

April 5, 2024

Vous pouvez désormais gérer, surveiller et vérifier l'utilisation des navigateurs publiés dans Remote Browser Isolation.

Gérer

L'onglet **Gérer** répertorie les navigateurs publiés. Pour accéder aux tâches de gestion, cliquez sur les points de suspension situés à droite du navigateur publié, puis sélectionnez la tâche requise.



Si vous sélectionnez une entrée de menu, puis décidez de ne rien changer, annulez la sélection en cliquant sur le bouton **X** en dehors de la boîte de dialogue.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

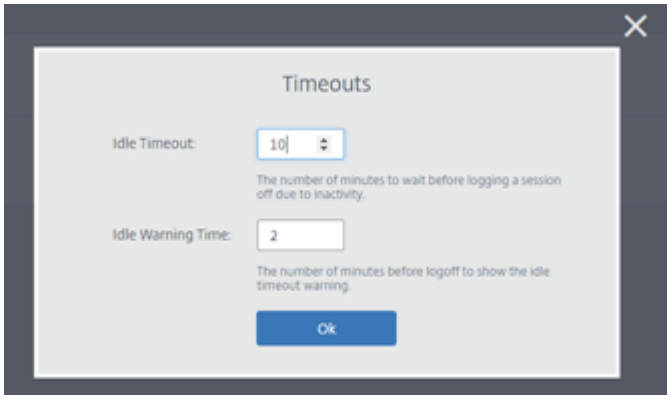
Vous pouvez gérer le navigateur isolé publié à l'aide des tâches suivantes :

- **Lancer navigateur publié :** ouvre la session de navigateur publié. Après avoir publié le navigateur, vous pouvez sélectionner cette tâche pour vérifier le lancement de la session de navigateur publié.
- **Copier URL dans le Presse-papiers :** copie l'URL du navigateur publié. Vous pouvez partager cette URL avec les utilisateurs finaux pour accéder aux navigateurs publiés.
- **Délais d'expiration :** vous pouvez définir le **Délai d'inactivité** et le **Délai d'avertissement d'inactivité** en sélectionnant la tâche **Délais d'expiration**.
  - **Délai d'inactivité :** nombre de minutes pendant lesquelles une session peut rester inactive avant d'être fermée pour cause d'inactivité.
  - **Délai d'avertissement d'inactivité :** nombre de minutes après lesquelles un message d'avertissement est envoyé à l'utilisateur avant la fermeture de la session.

  Par exemple, si vous définissez le délai d'inactivité sur 20 et le délai d'avertissement d'inactivité sur 5, le système affichera un message d'avertissement si aucune activité n'est détectée dans la session pendant 15 minutes. Si l'utilisateur ne répond pas, la session se termine cinq minutes plus tard.

  Pour définir le **Délai d'inactivité** et le **Délai d'avertissement d'inactivité** du navigateur isolé publié, sélectionnez la tâche **Délais d'expiration**, puis définissez la valeur du **Délai d'inactivité** et du **Délai d'avertissement d'inactivité** dans la boîte de dialogue **Délais d'expiration**. Cliquez ensuite sur **OK** pour enregistrer les modifications.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

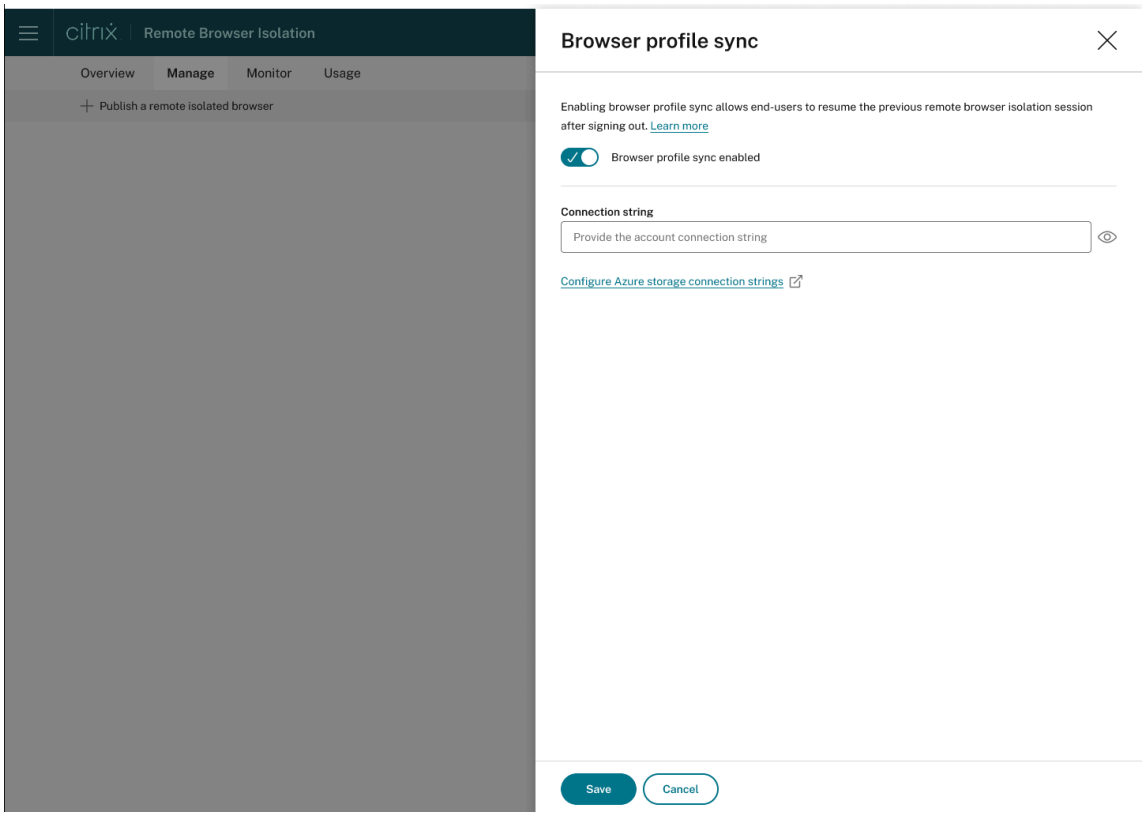


- **Synchronisation des profils de navigateur** : permet aux utilisateurs finaux de reprendre leur session de navigation précédente après leur déconnexion. Les administrateurs peuvent spécifier une chaîne de connexion pour leur stockage Azure afin de permettre le stockage du profil du navigateur. Lorsque l'utilisateur ouvre une autre session de navigateur avec le même profil, la session de navigateur précédente est rétablie là où l'utilisateur s'était arrêté. Si l'utilisateur s'est connecté à des sites Web, ces sites Web sont responsables de l'authentification. Bien que cette fonctionnalité puisse enregistrer des sessions, des cookies et d'autres informations, le site Web peut obliger l'utilisateur à se reconnecter. Actuellement, cette fonctionnalité ne prend en charge que la restauration des onglets.

  Pour activer la fonctionnalité **Synchronisation des profils de navigateur**, procédez comme suit :

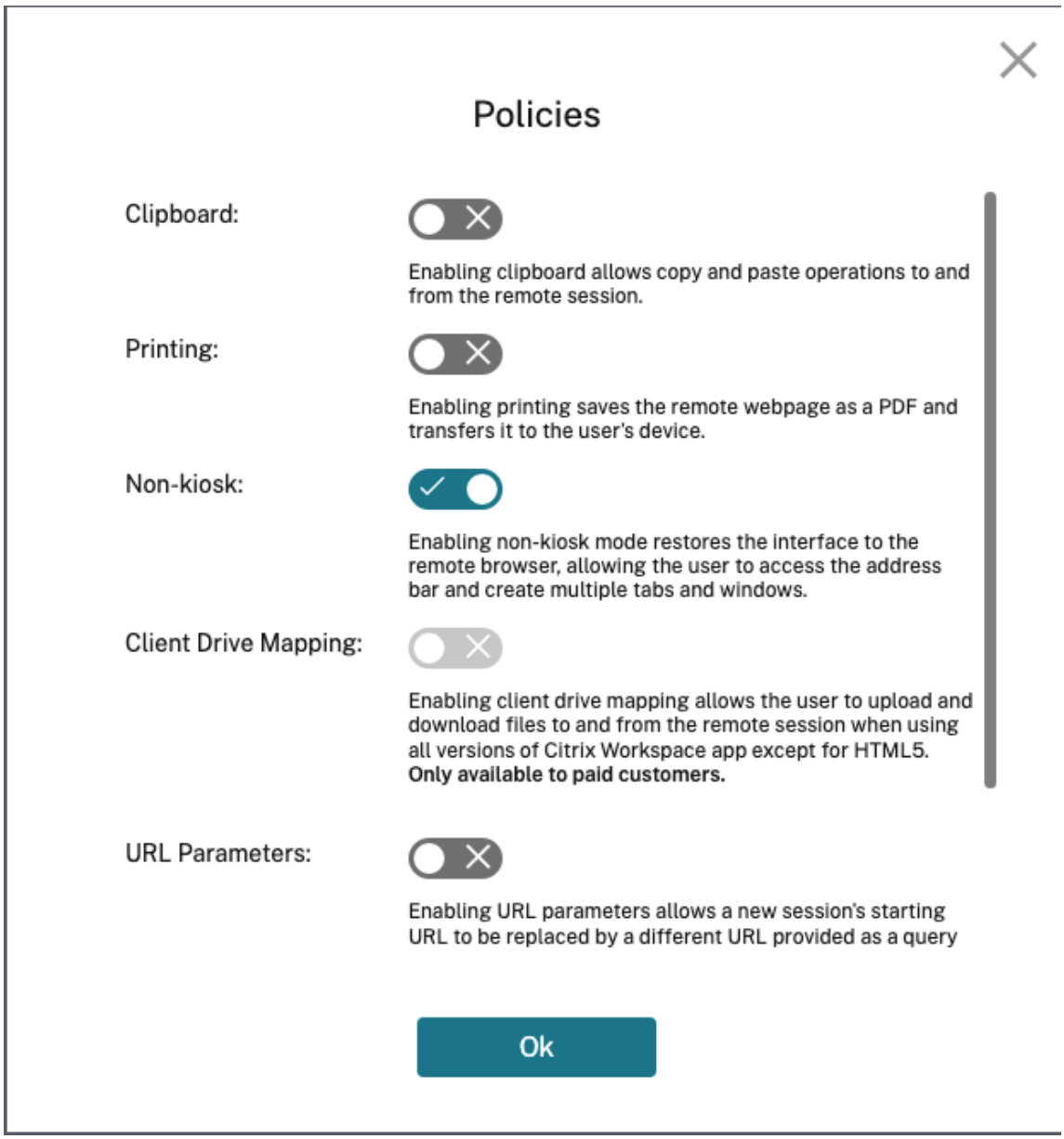
  1. Sélectionnez la tâche **Synchronisation des profils de navigateur** pour le navigateur publié requis.
  2. Dans la boîte de dialogue **Synchronisation des profils de navigateur**, activez la **Synchronisation des profils de navigateur**, puis entrez la **Chaîne de connexion**. Pour plus d'informations sur la configuration de la chaîne de connexion, consultez la section Configurer les chaînes de connexion de stockage Azure dans la documentation sur le stockage Blob Azure.
  3. Cliquez sur **Enregistrer**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- **Stratégies :** vous pouvez définir des stratégies pour les navigateurs publiés.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



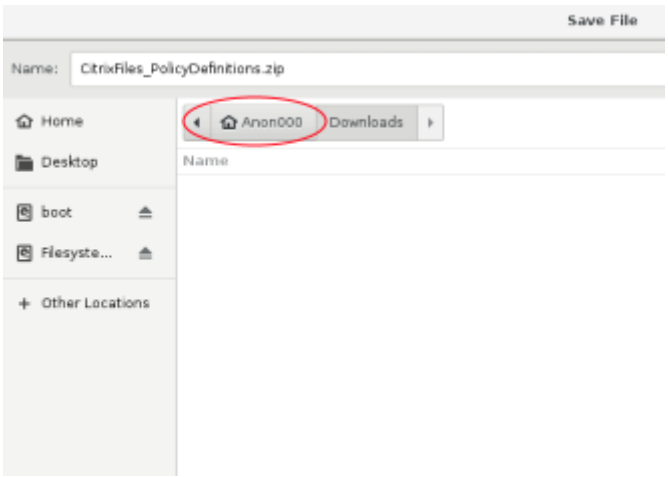
Les paramètres de la page des stratégies contrôlent ce qui suit :

- **Presse-papiers :** lorsque la stratégie Presse-papiers est activée, les opérations de copier-coller vers et depuis la session distante sont autorisées. (La désactivation de la stratégie du presse-papiers supprime le bouton Presse-papiers de la barre d'outils de l'application Citrix Workspace.) Par défaut, ce paramètre est désactivé.
- **Impression :** lorsque vous activez l'impression, la page Web distante peut être enregistrée au format PDF et transférée sur l'appareil de l'utilisateur. L'utilisateur peut ensuite appuyer sur Ctrl-P et sélectionner l'imprimante Citrix PDF. Par défaut, ce paramètre est désactivé.
- **Kiosque :** l'activation du mode non-kiosque restaure l'interface sur le navigateur distant.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

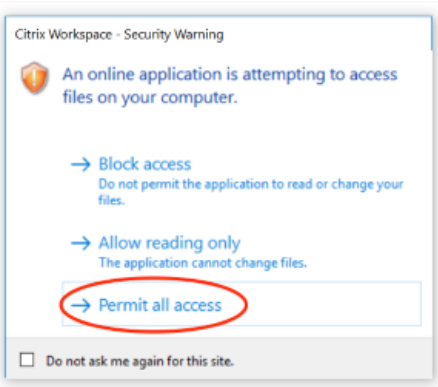
L'utilisateur peut alors accéder à la barre d'adresses et créer plusieurs onglets et fenêtres. (La désactivation du mode non-kiosque supprime les contrôles de navigation et la barre d'adresses du navigateur distant.) Par défaut, ce paramètre est activé (le mode non-kiosque est activé).

- **Basculement de région :** la stratégie de basculement de région permet de transférer automatiquement votre navigateur publié vers une autre région si votre région actuelle signale un problème. Si vous ne souhaitez pas utiliser cette fonctionnalité, désactivez la stratégie de basculement de région. Si vous avez publié le navigateur à l'aide de la sélection de région **Auto**, votre navigateur isolé reste inscrit à la stratégie. Ce paramètre est activé par défaut.
- **Mappage des lecteurs clients :** l'activation de la stratégie de mappage des lecteurs clients permet à l'utilisateur de charger et télécharger des fichiers vers et depuis la session distante. Cette fonctionnalité est disponible uniquement pour les sessions lancées avec l'application Citrix Workspace. Par défaut, cette stratégie est désactivée.
  - Les utilisateurs doivent enregistrer les fichiers téléchargés uniquement sur le disque `ctxmnt` du répertoire `Anonxxx`. Pour ce faire, les utilisateurs doivent naviguer jusqu'à l'emplacement souhaité pour stocker le fichier. Par exemple, **Anonxxx > ctxmnt > C > Utilisateurs > Nom d'utilisateur > Documents**.



  - La boîte de dialogue peut inviter l'utilisateur à accepter les autorisations **Permit all access** ou **Read and Write** pour accéder au dossier `ctxmnt`.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



  - **Paramètres d'URL :** l'activation des paramètres d'URL vous permet de modifier l'URL de démarrage d'une nouvelle session lorsque les utilisateurs lancent une application. Pour que cette stratégie prenne effet, configurez un serveur proxy local pour identifier les sites Web suspects et les rediriger vers Remote Browser Isolation. Par défaut, ce paramètre est désactivé. Pour plus d'informations, consultez le Guide de preuve de concept : Redirection d'URL vers Remote Browser Isolation avec Citrix ADC dans Azure.
  - **Suivi des noms d'hôte :** utilisez le suivi des noms d'hôte pour permettre à Remote Browser Isolation de consigner les noms d'hôte pendant la session d'un utilisateur. La stratégie est désactivée par défaut. Ces informations sont partagées avec Citrix Analytics. Pour plus d'informations, consultez Citrix Analytics.

  Lorsque vous avez terminé, cliquez sur **OK**.

- **Liste d'URL autorisées :** utilisez la tâche **Listes blanches** pour limiter l'accès des utilisateurs uniquement aux URL autorisées dans leur session Remote Browser Isolation publiée. Cette fonctionnalité est disponible pour les applications Web authentifiées externes.

  Saisissez les entrées de liste autorisée au format `hostname:port number`. Spécifiez chaque entrée sur une nouvelle ligne. Les astérisques sont pris en charge en tant que caractères génériques. Les demandes de navigateur doivent correspondre à au moins une entrée dans la liste d'autorisation.

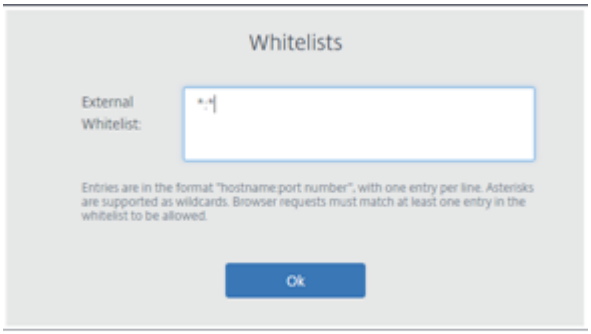
  Par exemple, pour définir `https://example.com` comme URL autorisée, procédez comme suit :

  - `example.com:*` permet de se connecter à cette URL depuis n'importe quel port.
  - `example.com:80` permet de se connecter à cette URL uniquement à partir du port 80.
  - `*:*` permet d'accéder à cette URL depuis n'importe quel port et depuis n'importe quel lien vers d'autres URL et ports. Le format `*.*` permet d'accéder à toutes les applications Web externes à partir de l'application publiée. Ce format est le paramètre par défaut pour le champ **Liste blanche externe** des applications Web.

  Lorsque vous avez terminé, cliquez sur **OK**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Des fonctionnalités avancées de filtrage Web sont disponibles via l'intégration au service Contrôle d'accès. En savoir plus sur Use case: Selective access to apps.



- **Filtrage d'URL :** vous pouvez configurer le filtrage d'URL pour contrôler les méthodes d'accès basées sur des catégories prédéfinies associées aux modèles de risque. Les options de filtrage d'URL incluent :
  - **Aucun** : autorise toutes les catégories.
  - **Minimal** : maximise l'accès tout en contrôlant les risques liés aux sites Web illégaux et malveillants. Comprend les catégories suivantes :
    - **Adulte :** contenu grotesque, éducation sexuelle, pornographie, nudité, services sexuels, recherche et liens pour adultes, maillots de bain et lingerie, magazines et actualités pour adultes, expression sexuelle (texte), fétiche et rencontres.
    - **Informatique et Internet :** proxys distants, adresses IP privées, partage de fichiers d'égal à égal et torrents.
    - **Jeux d'argent :** concours, prix, loteries et jeux d'argent en général.
    - **Contenu illégal et nuisible :** terrorisme, extrémisme, haine, diffamation, armes, violence, suicide, drogues illicites, médicaments, activités illégales, marijuana et défense d'intérêts en général.
    - **Malware et spam :** piratage, malware, spam, spyware, botnets, sites infectés, sites de phishing, keyloggers (enregistreurs de frappe), logiciels malware sur mobiles, robots téléphoniques, sites Web malveillants et dangereux.
  - **Modéré :** minimise les risques tout en autorisant des catégories supplémentaires affichant une faible probabilité d'exposition à des sites non sécurisés ou malveillants. Comprend les catégories suivantes :
    - **Adulte :** contenu grotesque, éducation sexuelle, pornographie, nudité, services sexuels, recherche et liens pour adultes, maillots de bain et lingerie, magazines et actualités pour adultes, expression sexuelle (texte), fétiche et rencontres.
    - **Commerce et industrie :** enchères.
    - **Informatique et Internet :** publicités, bannières, proxys distants, adresses IP privées, partage de fichiers d'égal à égal et torrents.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

    * **Téléchargements :** App Stores pour mobiles, services de stockage, téléchargements et téléchargements de programmes.
    * **E-mail :** messagerie Internet et abonnements par e-mail.
    * **Finance :** crypto-monnaie.
    * **Jeux d'argent :** concours, prix, loteries et jeux d'argent en général.
    * **Malware et spam :** piratage, malware, spam, spyware, botnets, sites infectés, sites de phishing, keyloggers (enregistreurs de frappe), logiciels malware sur mobiles, robots téléphoniques, sites Web malveillants et dangereux.
    * **Messagerie, chat et téléphonie :** messages instantanés et chat sur le Web.
    * **Actualités, divertissement et société :** Wordpress (publication et chargements), URL non prises en charge, occulte, aucun contenu, divers, horoscope, astrologie, divination, alcool, religions, pages Web personnelles, blogs et jeux en ligne.
    * **Réseaux sociaux :** sites de recherche et de partage de photos, bulletins informatiques et bulletins électroniques.

- **Strict :** minimise le risque d'accéder à des sites Web non sécurisés ou malveillants. Les utilisateurs peuvent toujours accéder aux sites Web qui présentent de faibles risques. Comprend les catégories suivantes :

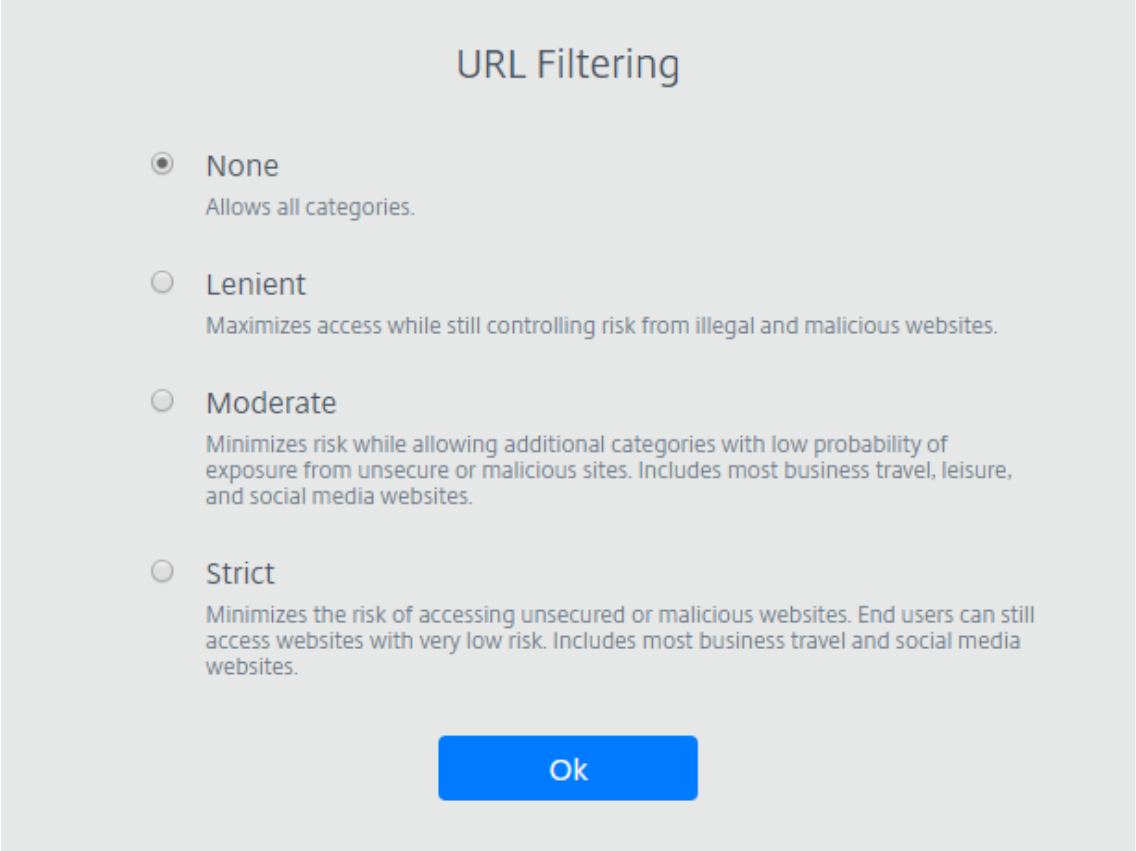
    * **Adulte :** contenu grotesque, éducation sexuelle, pornographie, nudité, services sexuels, recherche et liens pour adultes, maillots de bain et lingerie, magazines et actualités pour adultes, expression sexuelle (texte), fétiche et rencontres.
    * **Commerce et industrie :** enchères.
    * **Informatique et Internet :** publicités, bannières, DNS dynamique, applications mobiles, éditeurs, domaines parqués, proxys distants, adresses IP privées, partage de fichiers d'égal à égal et torrents.
    * **Téléchargements :** App Stores pour mobiles, services de stockage, téléchargements et téléchargements de programmes.
    * **E-mail :** messagerie Internet et abonnements par e-mail.
    * **Finance :** crypto-monnaie et produits financiers.
    * **Jeux d'argent :** concours, prix, loteries et jeux d'argent en général.
    * **Contenu illégal et nuisible :** terrorisme, extrémisme, haine, diffamation, armes, violence, suicide, drogues illicites, médicaments, activités illégales, marijuana et défense d'intérêts en général.
    * **Emplois et CV :** emploi, avancement professionnel et LinkedIn (mises à jour, messages, connexions et emplois).
    * **Malware et spam :** piratage, malware, spam, spyware, botnets, sites infectés, sites de phishing, keyloggers (enregistreurs de frappe), logiciels malware sur mobiles, robots téléphoniques, sites Web malveillants et dangereux.
    * **Messagerie, chat et téléphonie :** messages instantanés et chat sur le Web.
    * **Actualités, divertissement et société :** Wordpress (publication et chargements),

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

hébergement, voyage et tourisme, URL non prises en charge, politique, mode et beauté, événements artistiques et culturels, référence, loisirs et hobbies, communautés locales, divers, boissons, sujets populaires, événements spéciaux, actualités, société et culture, magazines en ligne, jeux en ligne, événements de la vie, occulte, aucun contenu, horoscope, astrologie, divination, célébrités, streaming de multimédia, divertissement, lieux, activités, pages Web personnelles et blogs, et religions.

* **Réseaux sociaux :** réseaux sociaux en général, YikYak (publication), Twitter (publication, messages et suivre), Vine (charger, commenter et messages), Google+ (charger des photos et des vidéos, messages, chat vidéo et commenter), Instagram (charger et commenter), YouTube (partages et commenter), Facebook (groupes, jeux, questions, charger des vidéos, charger des photos, événements, chat, applications, publication, commenter et amis), Tumblr (publication, commenter, charger des photos et des vidéos), Pinterest (épingles et commenter), bulletins informatiques et bulletins électroniques.

Lorsque vous avez terminé, cliquez sur **OK**.



- **Modifier :** utilisez la tâche **Modifier** pour modifier le nom, l'URL de démarrage, la région d'un navigateur publié ou le code secret. Une fois terminé, cliquez sur **Publier**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

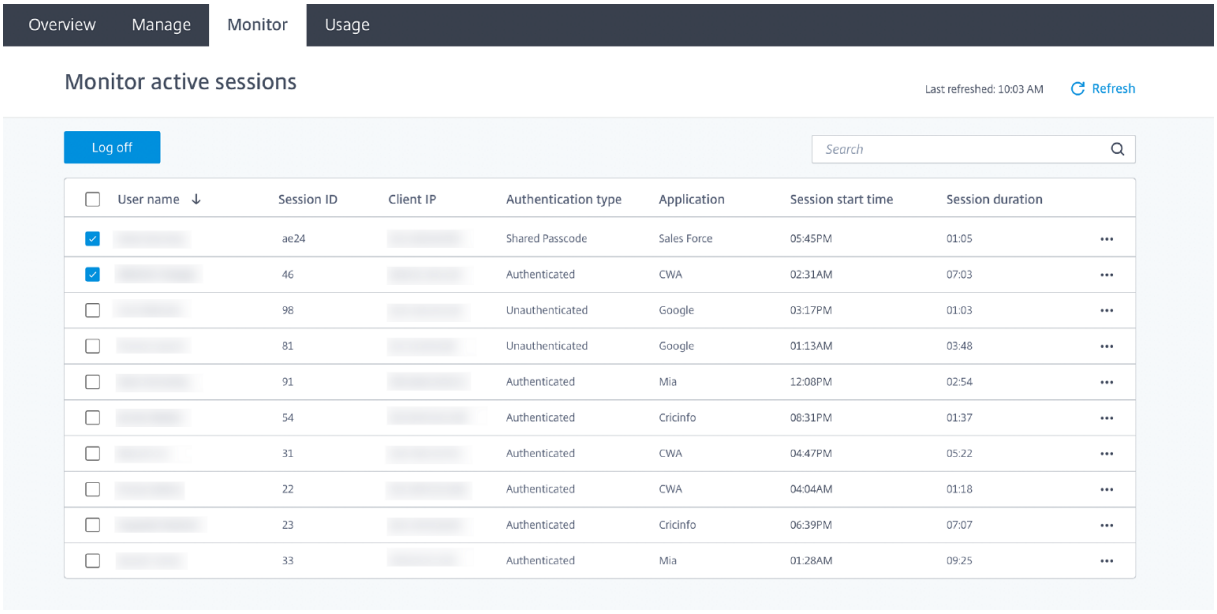
- **Supprimer :** utilisez la tâche **Supprimer** pour supprimer un navigateur isolé publié. Lorsque vous sélectionnez cette tâche, vous êtes invité à confirmer la suppression.

Surveiller

L'onglet **Surveiller** fournit des informations sur les sessions des utilisateurs en temps réel. Vous pouvez surveiller et déconnecter une ou plusieurs sessions actives.

Pour déconnecter une session unique, sélectionnez-la et cliquez sur le menu des points de suspension à la fin de la ligne d'une entrée. Cliquez sur **Fermer session** et confirmez vos modifications.

Pour déconnecter plusieurs sessions, sélectionnez les sessions actives dans la liste et cliquez sur le bouton **Fermer session** en haut de la page. Une fois vos modifications confirmées, Remote Browser Isolation déconnecte immédiatement toutes les sessions sélectionnées.

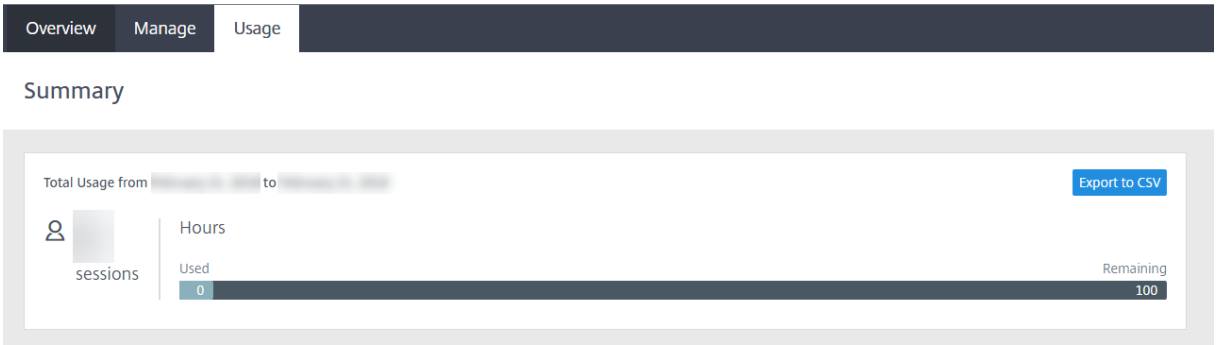


Utilisation

L'onglet **Utilisation** indique le nombre de sessions démarrées et le nombre d'heures utilisées.

Pour créer une feuille de calcul contenant des détails d'utilisation, cliquez sur **Exporter au format CSV** et sélectionnez une période.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Vue d'ensemble de la sécurité technique de Remote Browser Isolation

October 13, 2022

Remote Browser Isolation (anciennement Secure Browser Service) est un produit SaaS géré et exploité par Citrix. Il permet d'accéder aux applications Web via un navigateur Web intermédiaire hébergé dans le cloud.

Service de cloud

Citrix Remote Browser Isolation Service se compose de navigateurs Web exécutés sur des VDA (Virtual Delivery Agents) et de la console de gestion qui est utilisée pour gérer et connecter les utilisateurs à ces VDA. Citrix Cloud gère le fonctionnement de ces composants, y compris la sécurité et l'application de correctifs aux systèmes d'exploitation, navigateurs Web et composants Citrix.

Lors de l'utilisation de Remote Browser Isolation Service, les navigateurs Web hébergés suivent l'historique de navigation de l'utilisateur et effectuent la mise en cache des requêtes HTTP. Citrix utilise des profils obligatoires et garantit que ces données sont supprimées à la fin de la session de navigation.

Remote Browser Isolation Service est accessible via un navigateur Web compatible HTML5. Le service ne fournit aucun client téléchargeable. Tout le trafic entre le navigateur utilisé et le service cloud est crypté à l'aide du cryptage TLS standard. Remote Browser Isolation prend uniquement en charge TLS 1.2

Le trafic de sortie pour Remote Browser Isolation utilise des adresses IP spécifiques pour protéger le réseau interne. Pour obtenir la liste des adresses IP acceptées, consultez l'article du Centre de connaissances CTX286379.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Applications Web

Citrix Remote Browser Isolation est utilisé pour fournir des applications Web appartenant au client ou à un tiers. Le propriétaire de l'application Web est responsable de sa sécurité, y compris de l'application de correctifs au serveur Web et à l'application afin de les protéger contre toute vulnérabilité.

La sécurité du trafic entre Remote Browser Isolation et l'application Web dépend des paramètres de cryptage du serveur Web. Pour protéger ce trafic pendant son transit sur Internet, les administrateurs publient des URL HTTPS.

Informations supplémentaires

Consultez les ressources suivantes pour de plus amples informations sur la sécurité :

- Site de sécurité de Citrix : https://www.citrix.com/security
- Documentation Citrix Cloud : Guide de déploiement sécurisé pour la plate-forme Citrix Cloud

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).