



Clients NetScaler Gateway

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

Clients VPN NetScaler Gateway et fonctionnalités prises en charge	2
Citrix Secure Access pour macOS/iOS	5
Notes de publication	7
Configurer Citrix Secure Access pour les utilisateurs iOS	22
Envoyer l'identité du certificat utilisateur sous forme de pièce jointe à un e-mail aux utilisateurs iOS	30
Configurer le fichier PAC proxy pour l'application Citrix SSO pour les utilisateurs iOS ou le client Citrix Secure Access pour les utilisateurs de macOS	32
Configurer Citrix Secure Access pour les utilisateurs de macOS	33
Support de nFactor pour le client Citrix Secure Access sur macOS/iOS	41
Résolution des problèmes courants liés à Citrix Secure Access pour macOS/iOS	43
FAQ	45
Citrix Secure Access pour Android	46
Notes de publication	47
Configuration de Citrix Secure Access dans un environnement MDM	62
Configuration de Citrix Secure Access dans un environnement Intune Android Enterprise	62
Épinglage de certificats NetScaler Gateway avec Citrix Secure Access pour Android	83
Notes de mise à jour de Citrix Secure Access pour Windows	84
Support de Microsoft Edge WebView pour Windows Citrix Secure Access - Aperçu	107
Collecte de journaux améliorée pour le client Windows	110
Client Citrix Secure Access pour Linux	112
Notes de mise à jour de Citrix Secure Access pour Linux	115

Clients VPN NetScaler Gateway et fonctionnalités prises en charge

March 27, 2024

Important :

- Citrix SSO pour iOS/Android s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur de manière à refléter ce changement de nom.
- L'ancien client VPN a été créé à l'aide des API VPN privées d'Apple, qui sont désormais obsolètes. La prise en charge du VPN dans le client Citrix Secure Access pour macOS/iOS a été réécrite à l'aide du framework d'extension réseau public d'Apple. Le plug-in NetScaler Gateway et le VPN pour iOS et macOS ne sont plus pris en charge. Citrix Secure Access pour iOS/macOS est le client VPN recommandé.
- La disponibilité générale de la prise en charge de l'authentification nFactor pour les appareils Android sera disponible dans l'une des prochaines versions.

Le tableau suivant répertorie certaines des fonctionnalités couramment utilisées prises en charge pour chaque client VPN.

Fonctionnalité	Citrix Secure Access pour Windows	Citrix Secure Access pour Linux	Citrix Secure Access pour macOS	Citrix Secure Access pour iOS	Citrix Secure Access pour Android
Toujours activé (mode utilisateur)	Oui (11.1 et versions ultérieures)	Non	Non	Non	Oui (via MDM) Android 7.0 et versions ultérieures
fichier PAC	Oui (version 12.0 et ultérieure)	Non	Oui	Oui	Non
Prise en charge du proxy client	Oui	Oui	Non	Non	Oui. <i>Voir la note 1</i>
Limite maximale des applications Intranet	512	128	Durée illimitée	Durée illimitée	Durée illimitée

Clients NetScaler Gateway

Fonctionnalité	Citrix Secure Access pour Windows	Citrix Secure Access pour Linux	Citrix Secure Access pour macOS	Citrix Secure Access pour iOS	Citrix Secure Access pour Android
Prise en charge de l'IP Intranet (IIP)	Oui	Oui	Oui	Oui	Oui
Tunnel Split ON	Oui	Oui	Oui	Oui	Oui
Tunnel Split inverse	Oui	Oui	Oui	Oui	Oui. Voir la note 5
Split DNS DISTANT	Non	Oui	Oui	Oui	Oui. Voir la note 6
Split DNS DES DEUX CÔTÉS	Oui	Non	Oui	Oui	Oui. Voir la note 6
Split tunnel basé sur le nom de domaine complet	Oui uniquement ON (13.0 et versions ultérieures)	Non	Oui	Oui	Oui. Voir la note 5
Délai d'inactivité du client	Oui	Oui	Oui	Non	Non
Analyse des points de terminaison	Oui	Oui	Oui	Non	Non
Certificat de périphérique (classique)	Oui	Non	Oui	Non	Non
Authentification nFactor	Oui (12.1 et versions ultérieures)	Non	Oui	Oui	Oui. Voir la note 3
EPA (nFactor)	Oui (12.1 et versions ultérieures)	Non	Oui	Non	Non
Certificat de périphérique (NFactor)	Oui (12.1 et versions ultérieures)	Non	Oui	Non	Non

Fonctionnalité	Citrix Secure Access pour Windows	Citrix Secure Access pour Linux	Citrix Secure Access pour macOS	Citrix Secure Access pour iOS	Citrix Secure Access pour Android
Notification Push	Oui (12.1 et versions ultérieures)	Non	Non	Oui	Oui
Prise en charge de la saisie automatique des jetons OTP. <i>Voir la note 2</i>	Non	Non	Non	Oui	Oui
Prise en charge de TLS 1.3	Oui	Oui	Oui	Oui (Désactivé), par défaut. Disponible sur demande.)	Oui (Désactivé), par défaut. Disponible sur demande.)
Prise en charge de DTLS. <i>Voir la note 4</i>	Oui (version 13.0 et ultérieure)	Non	Oui	Oui	Non
Cookies HTTP uniquement	Oui	Oui	Oui	Oui	Oui
Équilibrage global de la charge des serveurs (GSLB)	Oui	Oui	Oui	Oui	Oui
Accès au réseau local	Oui	Non	Toujours activé	Toujours activé	Non

Remarque :

1. La définition d'un proxy dans la configuration du client sur le serveur virtuel VPN dans la configuration de passerelle pour Android 10 et versions ultérieures est prise en charge. Seule la configuration de base du proxy HTTP avec adresse IP et port est prise en charge.
2. Seuls les jetons scannés par code QR sont éligibles au remplissage automatique. Le remplissage automatique n'est pas pris en charge dans le flux d'authentification nFactor.

3. La prise en charge de l'authentification nFactor pour les appareils Android est en cours d'aperçu et la fonctionnalité est désactivée par défaut. Contactez le support NetScaler pour activer cette fonctionnalité. Les clients doivent fournir le nom de domaine complet de leur NetScaler Gateway à l'équipe de support pour activer l'authentification nFactor pour les appareils Android.
4. Pour plus de détails, consultez [Configurer le serveur virtuel VPN DTLS à l'aide du serveur virtuel VPN SSL](#).
5. La prise en charge du split tunnel basé sur le nom de domaine complet et le split tunnel inverse pour les appareils Android sont en cours d'aperçu et la fonctionnalité est désactivée par défaut. Contactez le support NetScaler pour activer cette fonctionnalité. Les clients doivent fournir le nom de domaine complet de leur NetScaler Gateway à l'équipe de support pour l'activer pour les appareils Android.
6. Pour le mode Split DNS DES DEUX CÔTÉS, les suffixes DNS doivent être configurés sur la passerelle et seules les requêtes d'enregistrement DNS A se terminant par ces suffixes sont envoyées à la passerelle. Les autres requêtes sont résolues localement. Citrix Secure Access pour Android prend également en charge le mode Split DNS LOCAL.

Référence

[Documentation d'aide pour l'utilisateur final](#)

Citrix Secure Access pour macOS/iOS

March 27, 2024

L'ancien client VPN a été créé à l'aide des API VPN privées d'Apple, qui sont désormais obsolètes. La prise en charge des VPN dans Citrix Secure Access pour macOS et iOS a été entièrement réécrite à l'aide du framework public d'extension réseau d'Apple.

Remarque

- Citrix SSO pour iOS s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur de manière à refléter ce changement de nom.
- Citrix Secure Access pour macOS est pris en charge sur 10.15 (Catalina), 11.x (Big Sur) et 12.x (Monterey). Il prend en charge les appareils équipés de puces Intel et de puces M1.
- Les utilisateurs dont le matériel ne peut pas être mis à niveau vers l'une des versions mentionnées précédemment (macOS 10.15 et macOS 11.0) ont accès à la dernière version com-

patible sur l'App Store, mais aucune autre mise à jour n'est disponible pour les anciennes versions.

- Si un utilisateur de macOS bascule entre l'application App Store et la version préliminaire de TestFlight ou inversement, il doit recréer le profil de connexion en effectuant les étapes suivantes :
 1. Cliquez sur le menu hamburger et cliquez sur **Configuration**.
 2. Supprimez le profil de la liste et ajoutez le même profil à nouveau.

Principales fonctionnalités du client Citrix Secure Access pour macOS/iOS

- **Jetons de mot de passe :** Un jeton de mot de passe est un code à 6 chiffres qui est une alternative aux services de mot de passe secondaires tels que VIP, OKTA. Ce code utilise le protocole T-OTP (Time-based One Time Password) pour générer le code OTP similaire à des services tels que Google Authenticator et Microsoft Authenticator. Les utilisateurs sont invités à saisir deux mots de passe lors de l'authentification auprès de NetScaler Gateway pour un utilisateur Active Directory donné. Le deuxième facteur est la modification du code à six chiffres que les utilisateurs copient à partir d'un service tiers enregistré tel que Google ou Microsoft Authenticator dans le navigateur de bureau. Les utilisateurs doivent d'abord s'inscrire à T-OTP sur l'appareil NetScaler. Pour connaître les étapes d'inscription, reportez-vous à <https://support.citrix.com/article/CTX228454>. Sur l'application, les utilisateurs peuvent ajouter la fonctionnalité OTP en scannant le code QR généré sur NetScaler ou en saisissant manuellement le secret TOTP. Les jetons OTP une fois ajoutés apparaissent dans le segment Jetons de mot de passe de l'interface utilisateur.

Pour améliorer l'expérience, l'ajout d'un OTP invite l'utilisateur à créer automatiquement un profil VPN. Les utilisateurs peuvent profiter de ce profil VPN pour se connecter au VPN directement depuis leurs appareils iOS.

Le client Citrix Secure Access pour macOS/iOS peut être utilisé pour scanner le code QR lors de l'inscription au support OTP natif.

La fonctionnalité de notification Push de NetScaler Gateway n'est disponible que pour les utilisateurs de Citrix Secure Access pour macOS/iOS.

- **Notification push :** NetScaler Gateway envoie une notification push sur votre appareil mobile enregistré pour une expérience d'authentification à deux facteurs simplifiée. Au lieu de lancer le client Citrix Secure Access pour macOS/iOS pour fournir le second facteur OTP sur la page de connexion NetScaler, vous pouvez valider votre identité en fournissant le code PIN de votre appareil/Touch ID/Face ID pour l'appareil enregistré.

Une fois que vous avez enregistré votre appareil pour la notification Push, vous pouvez également utiliser l'appareil pour la prise en charge OTP native à l'aide de Citrix Secure Access pour macOS/iOS.

L'inscription aux notifications push est transparente pour l'utilisateur. Lorsque les utilisateurs enregistrent TOTP, l'appareil est également enregistré pour les notifications push si NetScaler le prend en charge.

Notes de publication

March 27, 2024

Important :

Citrix SSO pour iOS est désormais renommé Citrix Secure Access. Nous mettons à jour les captures d'écran de l'interface utilisateur dans notre documentation pour refléter ce changement de nom. Vous remarquerez peut-être également les références Citrix SSO utilisées dans la documentation iOS pendant cette période de transition.

Les notes de publication décrivent les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes, les problèmes résolus et les problèmes connus disponibles dans une version révisée. Les notes de publication incluent une ou plusieurs des sections suivantes :

Nouveautés : les nouvelles fonctionnalités et améliorations disponibles dans la version actuelle.

Problèmes résolus : problèmes résolus dans la version actuelle.

Problèmes connus : problèmes qui existent dans la version actuelle et solutions de contournement, le cas échéant.

Remarques importantes concernant les clients de l'EPA :

- Les clients EPA sont pris en charge sur les versions macOS 10.13, 10.14, 10.15, 11.x, 12.x et 13.x.
- Les clients EPA sont pris en charge sur les versions NetScaler 12.1, 13.0, 13.1 et 14.1.

V24.03.1 (14 mars 2024)

Nouveautés

- Les bibliothèques EPA sont mises à jour vers la version 24.03.1.0 (bibliothèque OPSWAT OESIS V 4.3.3460.0).
- **Authentification unique automatique (SSO) à Citrix Secure Access via l'application Citrix Workspace - Aperçu**

Citrix Secure Access pour macOS prend désormais en charge l'authentification unique (SSO) automatique à Citrix Secure Access lorsque vous vous connectez à l'application Citrix Workspace.

Assurez-vous d'utiliser l'application Citrix Secure Access pour macOS 24.03.1/Citrix Workspace pour Mac 2402 et versions ultérieures afin de tirer parti de cette fonctionnalité. Cette fonctionnalité n'est prise en charge que sur les boutiques dans le cloud et non sur les boutiques sur site.

Actuellement, cette fonctionnalité est désactivée par défaut. Vous pouvez vous inscrire à l'aperçu en utilisant <https://podio.com/webforms/29383411/2410629>.

Pour plus de détails, consultez les [notes de mise à jour de l'application Citrix Workspace 2402 pour Mac](#).

[CSACLIENTS-6321]

- **Améliorations globales des performances et de la stabilité**

Le client Citrix Secure Access est doté des fonctionnalités suivantes pour améliorer les performances et la stabilité globales :

- Une augmentation du nombre de connexions simultanées pouvant être tunnelisées via un VPN. Cela ne s'applique qu'aux clients iOS.
- Une résilience de connexion VPN améliorée avec des passerelles IPv6. Cela s'applique à la fois aux clients macOS et iOS.

[NSHELP-36903]

V24.02.1 (15 février 2024)

Nouveautés

- **Support pour les opérateurs de scan EPA sur les clients Mac**

Le client Citrix Secure Access pour macOS prend désormais en charge tous les opérateurs, <> >=, <=, == et != sur l'éditeur EPA. L'option **Mac OS** est également disponible en tant qu'option distincte dans l'éditeur EPA (**Mac > Mac OS**). Vous pouvez effectuer une analyse de la version du produit sur vos appareils macOS à l'aide de ces opérateurs.

Pour plus de détails, consultez la section **Remarque** dans les [analyses avancées des terminaux](#).

[CSACLIENTS-6462]

- Les bibliothèques EPA sont mises à jour vers la version 24.1.2.1 (bibliothèque OPSWAT OESIS V 4.3.3405.0).

[CSACLIENTS-8520]

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

Client EPA 24.1.5 pour macOS (12 février 2024)

Nouveautés

- **Prise en charge de l'EPA pour les appareils Mac équipés d'un processeur Apple Silicon**

Le client Citrix EPA prend désormais en charge les appareils Mac qui utilisent le processeur Apple Silicon. Les appareils Mac ne nécessitent plus l'installation de Rosetta pour exécuter le client Citrix EPA.

[CSACLIENTS-8731]

- **Support pour les opérateurs de scan EPA sur les clients Mac**

Le client Citrix EPA pour Mac prend désormais en charge les opérateurs (<>>=, et <=) dans les expressions EPA. Les administrateurs peuvent configurer les analyses EPA pour autoriser un large éventail de versions de systèmes d'exploitation.

Par exemple, pour autoriser les versions du système d'exploitation de 12.4 à 13.0, sauf 12.8, les administrateurs peuvent configurer l'expression. `version >= 12.4 && version <= 13.0 && version != 12.8` Cela signifie que la version de macOS doit être comprise entre 12.4 et 13.0 mais ne peut pas être 12.8.

Pour plus de détails, voir [Analyses avancées des points de terminaison](#).

[CSACLIENTS-6462]

V23.12.2 (20 décembre 2023)

Nouveautés

Cette version résout des problèmes visant à améliorer les performances et la stabilité globales.

V23.12.1 (6 décembre 2023)

Nouveautés

- Les bibliothèques EPA sont mises à jour vers la version 23.11.1.5 (bibliothèque OPSWAT OESIS V 4.3.3318.0).

[CSACLIENTS-8516]

- Cette version résout d'autres problèmes afin d'améliorer les performances et la stabilité globales.

V23.11.2 (1er novembre 2023)

Nouveautés

Les bibliothèques EPA sont mises à jour vers la version 23.11.1.1 (bibliothèque OPSWAT OESIS V 4.3.3279.0).

[CSACLIENTS-8515]

V23.11.1 (27 octobre 2023)

Nouveautés

- Citrix SSO pour iOS est désormais renommé Citrix Secure Access. Nous mettons à jour les captures d'écran de l'interface utilisateur dans notre documentation pour refléter ce changement de nom.
- Les bibliothèques EPA sont mises à jour vers la version 23.10.1.1 (bibliothèque OPSWAT OESIS V 4.3.3246.0).
- Cette version aborde les points suivants :
 - Problèmes de connexion avec l'environnement Citrix Secure Private Access.
 - Autres problèmes pour améliorer les performances et la stabilité globales.

V23.10.2 (17 octobre 2023)

Cette version résout les problèmes de connexion IPv6.

V23.10.1 (09 octobre 2023)

Nouveautés

- Les bibliothèques EPA sont mises à jour vers la version 23.9.1.2 (bibliothèque OPSWAT OESIS V4.3.3221.0).

- **Prise en charge de l'accès au réseau local**

Citrix Secure Access pour macOS/Citrix SSO pour iOS prend désormais en charge la fonctionnalité d'accès au réseau local de NetScaler Gateway. Vous pouvez configurer l'accès au réseau local de telle sorte qu'une fois qu'une connexion VPN est établie, les utilisateurs finaux soient autorisés ou empêchés d'accéder aux ressources du réseau local sur leurs appareils clients. Pour plus d'informations, consultez les rubriques suivantes :

- [Configurations d'administration de NetScaler Gateway](#)
- [Configurations de l'utilisateur final - macOS](#)
- [Configurations de l'utilisateur final - iOS](#)

V23.09.1 (07 septembre 2023)

Important :

Si vous utilisez les dernières versions du système d'exploitation Apple, telles que macOS 14/iOS 17 et versions ultérieures, nous vous recommandons de passer à la version 23.09.1 ou ultérieure de Citrix Secure Access Client/Citrix SSO. Pour plus d'informations sur la configuration logicielle requise pour le client NetScaler Gateway, consultez la section Configuration système requise pour le client [Citrix Secure Access](#).

Nouveautés

- Les bibliothèques EPA sont mises à jour vers la version 1.3.9.9 (OPSWAT OESIS v4.3.3160).
[CSACLIENTS-6547]

- **Informations sur les connexions sécurisées sur l'interface utilisateur**

Sur l'écran « Connexions » de l'interface utilisateur du client Citrix Secure Access, vous pouvez consulter les détails de la connexion sécurisée. Les détails incluent l'adresse IP, le nom de domaine complet, le port de destination et la durée de la connexion. Pour plus d'informations, consultez la section Informations [sur les connexions sécurisées](#).

[SPA-2364]

- **Réauthentifiez-vous auprès de NetScaler Gateway après un échec de connexion VPN**

Le client Citrix Secure Access pour macOS et Citrix SSO pour iOS vous invitent désormais à vous authentifier à nouveau auprès de NetScaler Gateway en cas de perte de connexion VPN. L'interface utilisateur vous avertit que la connexion à NetScaler Gateway est perdue et que vous devez vous authentifier à nouveau pour reprendre la connexion. Pour plus d'informations, consultez :

- [Reconnectez-vous à NetScaler Gateway depuis macOS après un échec de connexion VPN](#)
- [Reconnectez-vous à NetScaler Gateway depuis iOS après un échec de connexion VPN](#).

[CSACLIENTS-6071]

V23.08.1 (24 août 2023)

Nouveautés

- Cette version résout certains problèmes afin d'améliorer la stabilité et les performances générales.
- Les bibliothèques EPA sont mises à jour vers la version 1.3.9.9 (OPSWAT OESIS v4.3.3122).

23.7.6 Client EPA pour macOS (10 août 2023)

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

V23.07.1 (17 juillet 2023)

Nouveautés

- **Différentes options pour partager des fichiers journaux**

L'option « Envoyer les journaux par e-mail » de Citrix SSO pour iOS est désormais remplacée par l'option « Partager les journaux ». Les fichiers journaux compressés peuvent désormais être partagés via des options telles que le courrier électronique, le chat, l'enregistrement dans des fichiers, etc.

Pour plus d'informations, consultez la section [Envoyer des journaux](#).

[CSACLIENTS-3834]

- **Améliorations apportées à la page Journaux**

La page Journaux de Citrix Secure Access pour macOS est améliorée avec les options suivantes :

- Nombre maximum de fichiers journaux : Spécifiez le nombre maximum de fichiers journaux que vous souhaitez ajouter pour la collecte de journaux.
- Journaux d'e-mails : envoyez les journaux par e-mail.

Pour plus d'informations, consultez la section [Envoyer des journaux](#).

[SPA-2365]

Problèmes résolus

Lorsque vous vous connectez à un VPN, si vous êtes invité à sélectionner un certificat pour l'authentification, l'écran de connexion à l'authentification apparaît derrière la page d'accueil du client Citrix Secure Access.

[CSACLIENTS-455]

V23.06.1 (07 juin 2023)

Nouveautés

- **Menu d'aide sur la barre de navigation**

Un menu d'aide est désormais ajouté à la barre de navigation du client Citrix Secure Access. Les options (Ouvrir les journaux, Exporter les journaux, les journaux des e-mails et Effacer les journaux) du menu Aide peuvent être utilisées pour le débogage des journaux.

Une option Journaux d'e-mails est introduite dans le menu Aide. Il peut être utilisé pour partager les journaux par e-mail. Pour plus d'informations, consultez la section [Envoyer des journaux](#).

[SPA-2361]

Problèmes résolus

Dans certains cas, la résolution des noms courts DNS échoue sur Citrix Secure Access pour macOS et Citrix SSO pour iOS.

[NSHELP-34568]

Problèmes connus

Dans certains cas, les routes exclues du split tunneling inversé sont tunnelisées.

[CGOP-24575]

V23.05.2 (11 mai 2023)

Problèmes résolus

Après une mise à niveau, le Citrix SSO pour les appareils clients iOS ne peut pas établir de connexions VPN par application.

[NSHELP-35224]

V23.05.1 (04 mai 2023)

Nouveautés

- Les bibliothèques EPA sont mises à jour vers la version 1.3.9.3 et les bibliothèques OPSWAT sont mises à jour vers la version 4.3.2987.

- **Support pour l'envoi d'événements à Citrix Analytics**

Citrix Secure Access pour macOS prend désormais en charge l'envoi d'événements tels que la création de session, la fermeture de session et la connexion d'applications au service Citrix Analytics. Ces événements sont ensuite enregistrés dans le tableau de bord du service Secure Private Access.

[SPA-2197]

Problèmes résolus

- Lorsque les utilisateurs sont connectés à Citrix Secure Access ou à Citrix SSO, le champ « Durée de connexion » n'affiche pas l'heure dans le format spécifique à la région.

[CGOP-23587]

V23.04.1 (04 avril 2023)

Nouveautés

- Les bibliothèques EPA sont mises à jour vers la version 1.3.9.1 et les bibliothèques OPSWAT sont mises à jour vers la version 4.3.2923.

V22.12.2 (27 février 2023)

Nouveautés

- Les bibliothèques EPA sont mises à jour vers la version 1.3.8.9 (OPSWAT OESIS v4.3.2892.0).

V22.12.1 (7 déc. 2022)

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

V22.11.1 (29 novembre 2022)

Problèmes résolus

- L'ouverture de session par transfert ne fonctionne pas pour l'authentification autre que NFactor avec des passerelles locales.

[CGOP-22729]

22.11.3 Plug-in EPA pour macOS (28 novembre 2022)

Problèmes résolus

- Le plug-in Citrix EPA pour macOS se bloque lorsque GSLB est activé sur NetScaler.

[CGOP-22722]

V22.10.1 (17 novembre 2022)

Nouveautés

- Le plug-in Citrix Endpoint Analysis prend désormais en charge une nouvelle expression de validation d'adresse MAC dans laquelle des ensembles de modèles peuvent être créés pour la liste des adresses IP autorisées.

[CGOP-22095]

Problèmes résolus

- Parfois, des paramètres de proxy vides dans NetScaler Gateway version 13.0 ou 13.1 amènent Citrix SSO à créer des paramètres de proxy incorrects.

[NSHELP-31970]

- Parfois, les clients VPN ne parviennent pas à se reconnecter après une panne réseau ou une fois que l'appareil sort du mode veille.

[NSHELP-32483]

- Parfois, les connexions de passerelle échouent lorsque les littéraux IPv6 sont utilisés comme destination.

[NSHELP-32876]

22.10.1 Plug-in EPA pour macOS (27 octobre 2022)

Nouveautés

- Le plug-in Citrix Endpoint Analysis prend désormais en charge une nouvelle expression de validation d'adresse MAC dans laquelle des ensembles de modèles peuvent être créés pour la liste des adresses IP autorisées.

[CGOP-22098]

- Le plug-in Citrix Endpoint Analysis envoie des alertes de consentement dupliquées lors du traitement des demandes de vérification préliminaire d'accès au réseau privé provenant de Google Chrome.

[CGOP-21751]

V22.06.1 (20 septembre 2022)

Nouveautés

- Les bibliothèques EPA sont mises à jour vers la version 4.3.2523.0 (1.3.7.5)

Problèmes résolus

- L'authentification nFactor avec scan EPA ne fonctionne pas sur les clients macOS.

[NSHELP-32182 - macOS]

- Sur la page d'accueil de Secure Access Agent pour macOS, un remplissage supplémentaire de couleur blanche ou noire apparaît à gauche et en haut du menu hamburger en fonction du thème sélectionné (clair ou foncé).

[CGOP-19353 - macOS]

- Lorsque vous vous connectez au VPN, la fenêtre WebView se réduit au premier essai si le certificat de l'appareil est configuré.

[CGOP-19354 - macOS]

- L'analyse des points de terminaison ne fonctionne pas pour l'application Citrix Secure Access sur le client macOS lorsque GSLB est activé sur l'appliance NetScaler.

[CGOP-21634 - macOS]

- S'il y a un espace dans le nom de l'application configurée et que vous essayez d'accéder à l'application, la fenêtre contextuelle Enhanced Security Enabled n'apparaît pas sur les clients macOS.

[ACS-2632 - macOS]

- L'authentification nFactor avec un certificat client facultatif échoue lorsqu'il n'existe aucun certificat client approprié sur l'appareil.

[NSHELP-32127 - iOS]

- Sur un appareil Mac utilisant Chrome, l'extension VPN se bloque lors de l'accès à deux noms de domaine complets.

[NSHELP-32144]

- Citrix Secure Access se bloque lorsqu'une valeur de localisation incorrecte est reçue de la passerelle. Cela peut se produire si l'administrateur définit une stratégie de répondeur pour rediriger vers un autre hôte.

[NSHELP-32312]

- Les connexions directes aux ressources situées en dehors du tunnel établi par Citrix Secure Access peuvent échouer en cas de retard ou de congestion important.

[NSHELP-31598]

V3.2.4.9 - Plug-in EPA pour macOS (01-août-2022)

Problèmes résolus

- Le plug-in Citrix Endpoint Analysis ne gère pas les demandes de vérification préliminaire d'accès au réseau privé provenant du navigateur Google Chrome version 104.

[CGOP-20709]

- Le plug-in Citrix Endpoint Analysis pour macOS ne prend pas en charge GSLB.

[CGOP-21543]

Problèmes connus

- Le plug-in Citrix Endpoint Analysis pour macOS affiche une boîte de dialogue de consentement en double lorsqu'il est démarré à partir du navigateur Google Chrome version 104. Les utilisateurs doivent accepter les deux invites.

[CGOP-21751]

V22.03.1 (14-Jun-2022)

Nouveautés

- Les bibliothèques EPA sont mises à jour vers la version 4.3.2393.0.

Problèmes résolus

- Un domaine DNS supplémentaire est ajouté à la liste de recherche. En effet, lorsque le split tunnel est défini sur « Split » ou « Both », seuls les domaines spécifiés et leurs sous-domaines ne sont PAS tunnelisés. Si le domaine spécifié est A.B.C, alors B.C est également apparié en plus de A.B.C et *.A.B.C.

[CGOP-21657]

- Les paramètres proxy HTTP/HTTPS qui n'utilisent pas de fichier PAC ne fonctionnent pas.

[CGOP-21660]

V22.02.3 (24-Mar-2022)

Nouveautés

- Citrix Secure Access pour macOS résout le nom de domaine complet d'un nœud de service sur chaque connexion de données TCP depuis le client pour les connexions de l'espace de travail cloud. La résolution du nom de domaine complet d'un nœud de service sur chaque connexion de données TCP ne s'applique pas aux connexions de passerelle sur site.

[ACS-1068]

Problèmes résolus

- Parfois, Citrix Secure Access pour macOS interrompt les connexions en raison de problèmes liés à certains protocoles non DNS utilisant le port 53, tels que STUN.

[NSHELP-31004]

- L'application Citrix Secure Access rompt certains protocoles lorsque le serveur envoie des données avant le client, immédiatement après l'établissement de la connexion.

[NSHELP-29374]

- Si l'utilisateur ferme la fenêtre d'authentification du client Citrix Secure Access pour macOS sans terminer l'authentification, les tentatives suivantes de connexion au serveur échouent jusqu'au redémarrage de l'application.

[ACS-2415]

- Le client Citrix Secure Access pour macOS est désormais fourni avec la version 4.3.2367.0 de la bibliothèque OPSWAT

[NSHELP-30802]

- Citrix Secure Access pour macOS prend plus de temps que prévu pour exécuter le contrôle EPA post-authentification.

[NSHELP-29118]

Problèmes connus

- L'application Citrix Secure Access pour macOS se déconnecte une minute après que la région du service Citrix Secure Private Access déjà connectée soit devenue inaccessible. Toutefois, cela n'affecte pas les connexions de passerelle sur site.

[ACS-2715]

V22.02.2 (15-Feb-2022)

Problèmes résolus

- Plusieurs fenêtres contextuelles s'affichent lorsqu'un utilisateur tente d'accéder à une application Web désabonnée à partir de Citrix Secure Access pour macOS.

[ACS-2406]

V22.01.1 (08-Feb-2022)

Problèmes résolus

- Les connexions VPN par application avec Citrix SSO pour appareils iOS ne parviennent pas à se connecter à NetScaler Gateway sur des ports autres que 443.

[NSHELP-30653]

V1.4.1 (28-Jan-2022)

Nouveautés

- L'application Citrix SSO pour macOS est désormais rebaptisée Citrix Secure Access.

[ACS-1092]

Problèmes résolus

- L'authentification du certificat client échoue si le serveur d'authentification demande le certificat client plusieurs fois au cours de la même session d'affichage Web.

[CGOP-20388]

- Citrix SSO ne parvient pas à établir une connexion VPN si le certificat de serveur possède uniquement une adresse IP pour le nom commun en raison d'un proxy entre le client et l'ADC.

[CGOP-20390]

- L'analyse EPA pour vérifier la dernière analyse complète du système antivirus échoue sur macOS.

[NSHELP-29571]

- Parfois, l'application Citrix SSO se bloque lors du traitement de gros paquets DNS.

[NSHELP-29133]

V1.4.0 (17-Nov-2021)

Problèmes résolus

- Parfois, le code de validation du serveur échoue lorsque le certificat du serveur est approuvé. Par conséquent, les utilisateurs finaux ne peuvent pas accéder à la passerelle.

[NSHELP-28942]

- Citrix SSO ne parvient pas à rétablir la connexion VPN après une interruption du réseau.

[CGOP-19988]

V1.3.13 (05-Nov-2021)

Problèmes résolus

- Vous pouvez rencontrer des échecs lors du filtrage des sessions pour les VPN gérés par rapport aux VPN non gérés. Les demandes initiales d'établissement de la session ne contiennent pas les informations « ManagedVpn » dans l'en-tête User-Agent.

[CGOP-19561]

V1.3.12 (21-Oct-2021)

Problèmes résolus

- L'authentification par certificat client échoue pour Citrix SSO pour macOS s'il n'existe aucun certificat client dans le trousseau macOS.
[NSHELP-28551]
- L'application Citrix SSO se bloque par intermittence lors de la réception de notifications.
[CGOP-19363]
- L'extension VPN peut se bloquer lorsque le paramètre « IsFeatureEnabled » est appelé pour vérifier un indicateur de fonctionnalité.
[CGOP-19360]
- L'extension VPN de passerelle se bloque si le protocole DTLS a une charge utile vide.
[CGOP-19361]
- L'application SSO se bloque par intermittence lorsque l'appareil sort du mode veille et que le VPN est connecté.
[CGOP-19362]

V1.3.11 (17-Sep-2021)

Problèmes résolus

- L'analyse EPA pour la vérification du pare-feu échoue pour les appareils macOS utilisant Citrix SSO.
[CGOP-19271]
- Citrix SSO se bloque sur un appareil iOS 12 lorsque l'authentification héritée ou la conformité d'accès réseau (NAC) Intune est configurée.
[CGOP-19261]

V1.3.10 (31-Aug-2021)

Nouveautés

- Citrix SSO pour macOS est désormais fourni avec la bibliothèque OPSWAT version 4.3.1977.0.
[NSHELP-28467]

V1.3.9 (13-Aug-2021)

Problèmes résolus

- Sur certains systèmes sur lesquels un logiciel proxy HTTP est installé, l'adresse IP de NetScaler Gateway s'affiche en interne sous la forme 127.0.0.1, empêchant ainsi l'établissement d'un tunnel.

[CGOP-18538]

- Le paramètre « Bloquer les serveurs non fiables » ne fonctionne pas sur les systèmes qui prennent en charge la localisation non anglaise de Citrix SSO pour iOS.

[CGOP-18539]

- Citrix SSO ne peut pas se connecter aux systèmes dont le nom DNS ne correspond pas au nom commun du certificat de serveur. Citrix SSO recherche désormais les noms alternatifs des sujets et se connecte correctement.

[NSHELP-28348]

V1.3.8 (07-Jul-2021)

Nouveautés

- Citrix SSO pour macOS est compatible avec les versions 10.15 (Catalina) et supérieures uniquement.

[CGOP-12555]

- À partir de la version 1.3.8 de Citrix SSO pour macOS, les bibliothèques EPA sont intégrées à l'application et ne sont pas téléchargées depuis le serveur NetScaler Gateway. La version actuelle de la bibliothèque EPA intégrée est 1.3.5.1.

[NSHELP-26838]

Configurer Citrix Secure Access pour les utilisateurs iOS

March 27, 2024

Important :

- Citrix SSO pour iOS est désormais renommé Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur pour refléter ce change-

ment de nom. Vous remarquerez peut-être les références Citrix SSO utilisées dans la documentation pendant cette période de transition.

- Le VPN ne peut pas être utilisé sur iOS 12 et versions ultérieures. Pour passer au VPN, utilisez Citrix Secure Access.

Pour obtenir la liste des fonctionnalités couramment utilisées prises en charge par Citrix Secure Access pour iOS, consultez la section [Clients VPN NetScaler Gateway et fonctionnalités prises en charge](#).

Compatibilité avec les produits MDM

Citrix Secure Access (macOS/iOS) est compatible avec la plupart des fournisseurs MDM tels que Citrix Endpoint Management (anciennement XenMobile), Microsoft Intune, etc.

Citrix Secure Access (macOS/iOS) prend également en charge une fonctionnalité appelée Network Access Control (NAC). Pour plus d'informations sur le NAC, voir [Configurer la vérification du périphérique de contrôle d'accès réseau pour le serveur virtuel NetScaler Gateway](#) pour une connexion à facteur unique. Grâce au NAC, les administrateurs MDM peuvent faire respecter la conformité des appareils des utilisateurs finaux avant de se connecter à l'appliance NetScaler. NAC sur Citrix Secure Access (macOS/iOS) nécessite un serveur MDM tel que Citrix Endpoint Management ou Intune and NetScaler.

Remarque :

Pour utiliser le client Citrix Secure Access sur macOS/iOS avec le VPN NetScaler Gateway sans MDM, vous devez ajouter une configuration VPN. Vous pouvez ajouter la configuration VPN sur iOS depuis la page d'accueil de Citrix Secure Access (macOS/iOS).

Configurer un profil VPN géré par MDM pour le client Citrix Secure Access (macOS/iOS)

La section suivante présente des instructions détaillées permettant de configurer des profils VPN à la fois pour l'ensemble de l'appareil et par application pour le client Citrix Secure Access (macOS/iOS) à l'aide de Citrix Endpoint Management (anciennement XenMobile) comme exemple. D'autres solutions MDM peuvent utiliser ce document comme référence lorsqu'elles travaillent avec Citrix Secure Access (macOS/iOS).

Remarque :

Cette section explique les étapes de configuration d'un profil VPN de base à l'échelle de l'appareil et par application. Vous pouvez également configurer les proxys On-Demand en suivant la documentation de Citrix Endpoint Management (anciennement XenMobile) ou la configuration de la charge utile du VPN MDM d'Apple.

Profils VPN au niveau de l'appareil

Les profils VPN au niveau de l'appareil sont utilisés pour configurer un VPN à l'échelle du système. Le trafic provenant de toutes les applications et de tous les services est canalisé vers NetScaler Gateway en fonction des stratégies VPN (telles que Full-tunnel, Split-tunnel, Reverse Split tunnel) définies dans NetScaler.

Pour configurer un VPN au niveau de l'appareil sur Citrix Endpoint Management Effectuez les étapes suivantes pour configurer un VPN au niveau de l'appareil sur Citrix Endpoint Management.

1. Sur la console Citrix Endpoint Management MDM, accédez à **Configurer > Stratégies d'appareil > Ajouter une nouvelle stratégie**.
2. Sélectionnez **iOS** dans le volet de gauche Policy Platform. Sélectionnez **VPN** dans le volet droit.
3. Sur la page **Informations sur la stratégie**, saisissez un nom de stratégie et une description valides, puis cliquez sur **Suivant**.
4. Sur la page **Stratégie VPN** pour iOS, saisissez un nom de connexion valide et choisissez **SSL personnalisé** dans **Type de connexion**.

Dans la charge utile VPN MDM, le nom de connexion correspond à la clé **UserDefinedName** et la **clé de type VPN** doit être définie sur **VPN**.

5. Dans **Identificateur SSL personnalisé (format DNS inverse)**, saisissez **com.citrix.netscalergateway.ios.a**. Il s'agit de l'identifiant du bundle pour Citrix Secure Access sur iOS.

Dans la charge utile VPN MDM, l'identificateur SSL personnalisé correspond à la clé **VPNSub-type**.

6. Dans l'**identifiant du bundle fournisseur**, entrez **com.citrix.netscalergateway.ios.app.vpnPlugin**. Il s'agit de l'identifiant du bundle de l'extension réseau contenue dans le fichier binaire de l'application iOS Citrix Secure Access.

Dans la charge utile VPN MDM, l'identificateur de bundle de fournisseur correspond à la clé **ProviderBundleIdentifier**.

7. Dans **Nom du serveur ou adresse IP**, entrez l'adresse IP ou le FQDN (nom de domaine complet) du NetScaler associé à cette instance Citrix Endpoint Management.

Les autres champs de la page de configuration sont facultatifs. Les configurations de ces champs sont disponibles dans la documentation Citrix Endpoint Management (anciennement XenMobile).

8. Cliquez sur **Suivant**.

9. Cliquez sur **Enregistrer**.

Profils VPN par application

Les profils VPN par application sont utilisés pour configurer le VPN pour une application spécifique. Le trafic provenant uniquement de l'application spécifique est canalisé vers NetScaler Gateway. La charge utile **VPN par application** prend en charge toutes les clés du VPN à l'échelle de l'appareil, ainsi que quelques autres clés.

Pour configurer un VPN au niveau de l'application sur Citrix Endpoint Management Effectuez les étapes suivantes pour configurer un VPN par application :

1. Terminez la configuration VPN au niveau de l'appareil sur Citrix Endpoint Management.
2. Activez le commutateur **Activer Per App VPN** dans la section Per App VPN.
3. Activez le **commutateur On-Demand Match App Enabled** si Citrix Secure Access (macOS/iOS) doit être démarré automatiquement lors du lancement de l'application Match. Cette option est recommandée pour la plupart des cas par application.

Dans la charge utile VPN MDM, ce champ correspond à la clé **OnDemandMatchAppEnabled**.

4. Dans **Type de fournisseur**, sélectionnez **Tunnel de paquets**.

Dans la charge utile VPN MDM, ce champ correspond au **type de fournisseur** clé.

5. La configuration du domaine Safari est facultative. Lorsqu'un domaine Safari est configuré, Citrix Secure Access (macOS/iOS) démarre automatiquement lorsque les utilisateurs lancent Safari et accèdent à une URL correspondant à celle du champ **Domaine**. Cette option n'est pas recommandée si vous souhaitez restreindre le VPN pour une application spécifique.

Dans la charge utile VPN MDM, ce champ correspond à la clé **SafariDomains**.

Les autres champs de la page de configuration sont facultatifs. Les configurations de ces champs sont disponibles dans la documentation Citrix Endpoint Management (anciennement XenMobile).

6. Cliquez sur **Suivant**.

7. Cliquez sur **Enregistrer**.

Pour associer ce profil VPN à une application spécifique sur l'appareil, vous devez créer une stratégie d'inventaire des applications et une stratégie de fournisseur d'informations d'identification en suivant ce guide - <https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/>.

Configuration du split tunnel dans un VPN par application

Les clients MDM peuvent configurer un tunnel partagé dans Per-App VPN pour Citrix Secure Access (macOS/iOS). La paire clé/valeur suivante doit être ajoutée à la section de configuration du fournisseur du profil VPN créé sur le serveur MDM.

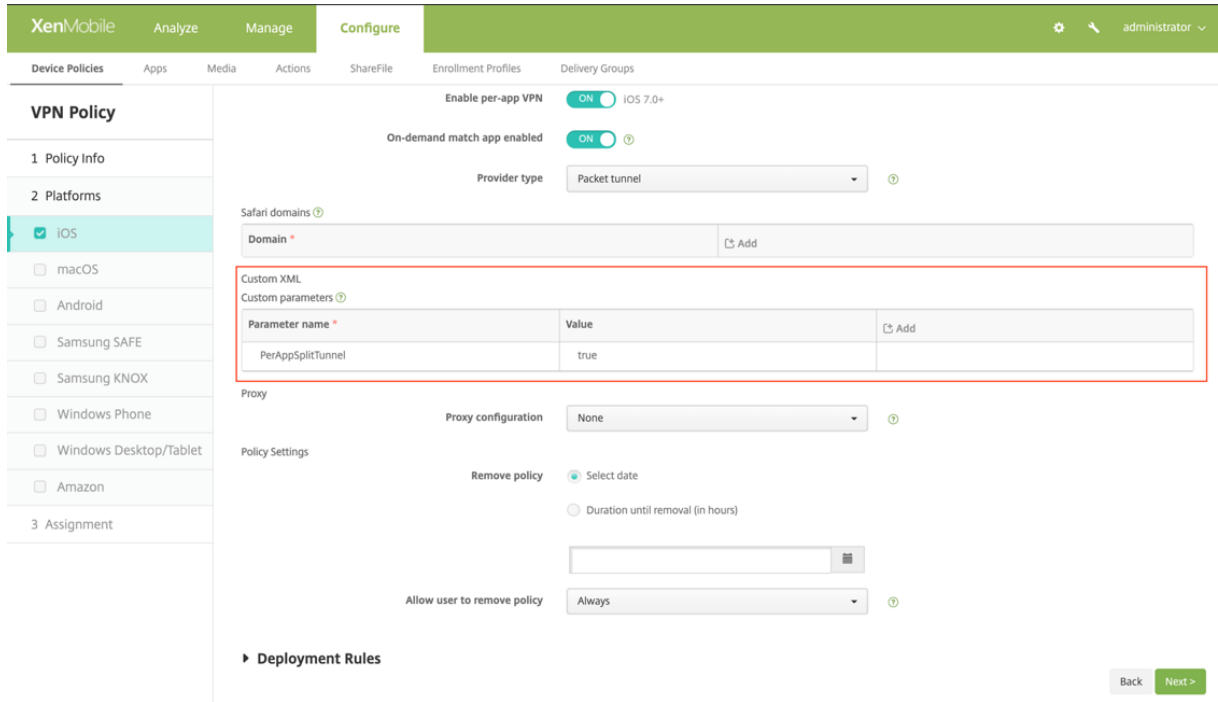
```
1 - Key = "PerAppSplitTunnel"  
2 - Value = "true or 1 or yes"  
3 <!--NeedCopy-->
```

La clé est sensible à la casse et doit correspondre exactement à la casse, tandis que la valeur n'est pas sensible à la casse.

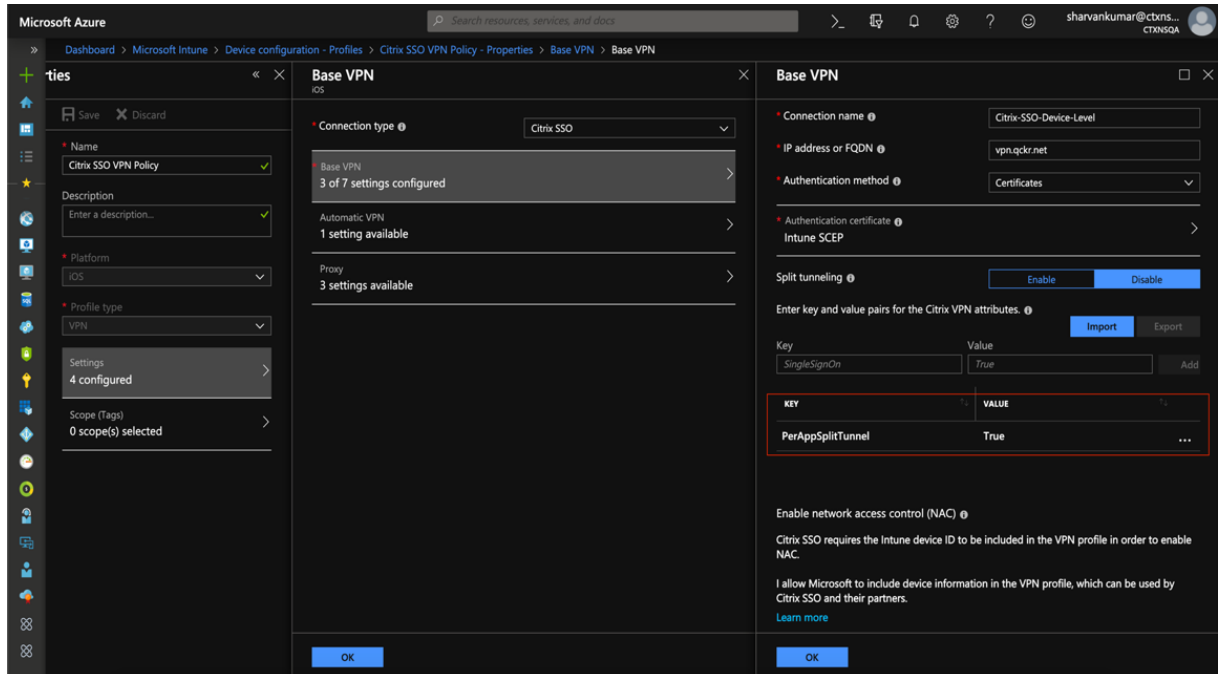
Remarque :

L'interface utilisateur permettant de configurer la configuration du fournisseur n'est pas standard parmi les fournisseurs MDM. Contactez le fournisseur MDM pour trouver la section de configuration du fournisseur sur votre console utilisateur MDM.

Voici un exemple de capture d'écran de la configuration (paramètres spécifiques au fournisseur) dans Citrix Endpoint Management.



Voici un exemple de capture d'écran de la configuration (paramètres spécifiques au fournisseur) dans Microsoft Intune.



Désactivation des profils VPN créés par les utilisateurs

Les clients MDM peuvent empêcher les utilisateurs de créer manuellement des profils VPN depuis Citrix Secure Access (macOS/iOS). Pour ce faire, la paire clé/valeur suivante doit être ajoutée à la section de configuration du fournisseur du profil VPN créé sur le serveur MDM.

```
1 - Key = "disableUserProfiles"  
2 - Value = "true or 1 or yes"  
3 <!--NeedCopy-->
```

La clé est sensible à la casse et doit correspondre exactement à la casse, tandis que la valeur n'est pas sensible à la casse.

Remarque :

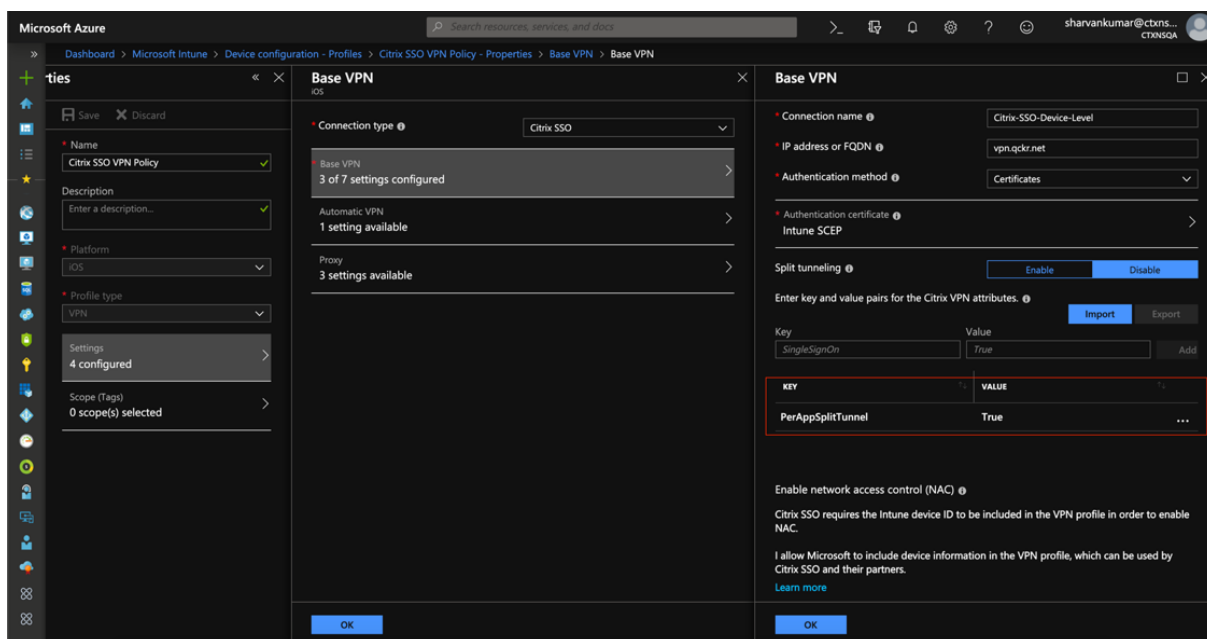
L'interface utilisateur permettant de configurer la configuration du fournisseur n'est pas standard parmi les fournisseurs MDM. Contactez le fournisseur MDM pour trouver la section de configuration du fournisseur sur votre console utilisateur MDM.

Voici un exemple de capture d'écran de la configuration (paramètres spécifiques au fournisseur) dans Citrix Endpoint Management.

The screenshot shows the configuration page for a VPN Policy in Citrix Endpoint Management. The left sidebar shows the policy is configured for iOS. The main area contains several sections:

- VPN Policy**: Enable per-app VPN (ON), On-demand match app enabled (ON), Provider type (Packet tunnel).
- Safari domains**: A table for adding domains.
- Custom XML**: A table for adding custom parameters. One parameter is visible: PerAppSplitTunnel with value true.
- Proxy**: Proxy configuration (None).
- Policy Settings**: Remove policy (Select date), Duration until removal (in hours) (empty field), Allow user to remove policy (Always).
- Deployment Rules**: A section for defining deployment rules.

Voici un exemple de capture d'écran de la configuration (paramètres spécifiques au fournisseur) dans Microsoft Intune.



Gestion DNS

Les paramètres DNS recommandés pour le client Citrix Secure Access sont les suivants :

- **Split DNS > REMOTE** si le split tunnel est réglé **sur OFF**.
- **Split DNS > BOTH** si le split tunnel est défini **sur ON**. Dans ce cas, les administrateurs doivent ajouter des suffixes DNS pour les domaines intranet. Les requêtes DNS pour les noms de domaine complets appartenant à des suffixes DNS sont acheminées vers l’appliance NetScaler et les requêtes restantes sont acheminées vers le routeur local.

Remarque :

- Il est recommandé que l’indicateur de **correction de troncature DNS** soit toujours **actif**. Pour plus de détails, consultez <https://support.citrix.com/article/CTX200243>.
- Lorsque le split tunnel est défini **sur ON** et que Split DNS est défini sur **REMOTE**, des problèmes peuvent survenir lors de la résolution des requêtes DNS après la connexion du VPN. Cela est lié au fait que le framework Network Extension n’intercepte pas toutes les requêtes DNS.

Problèmes connus

Description du problème : Tunneling pour les adresses de nom de domaine complet qui contiennent un domaine “.local” dans les configurations VPN par application ou VPN à la demande. Le framework Network Extension d’Apple présente un bogue qui empêche les adresses FQDN contenant

.local dans la partie domaine (par exemple <http://www.abc.local>) d'être tunnelisées via l'interface TUN du système. Au lieu de cela, le trafic pour les adresses FQDN est envoyé via l'interface physique de l'appareil client. Le problème est observé uniquement avec la configuration VPN par application ou VPN à la demande et n'est pas visible avec les configurations VPN à l'échelle du système. Citrix a déposé un rapport de bogue radar auprès d'Apple, et Apple a noté que, selon la RFC-6762 :,<https://tools.ietf.org/html/rfc6762> local est une requête DNS multicast (mDNS) et ne constitue donc pas un bogue. Cependant, Apple n'a pas encore résolu le bogue et il n'est pas clair si le problème sera résolu dans les prochaines versions d'iOS.

Solution : attribuez un nom de domaine non .local à ces adresses comme solution de contournement.

Limitations

- L'analyse des points de terminaison (EPA) n'est pas prise en charge sur iOS.
- Le split tunneling basé sur les ports/protocoles n'est pas pris en charge.

Envoyer l'identité du certificat utilisateur sous forme de pièce jointe à un e-mail aux utilisateurs iOS

March 27, 2024

Important :

Citrix SSO pour iOS s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur de manière à refléter ce changement de nom.

Citrix Secure Access sur iOS prend en charge l'authentification par certificat client avec NetScaler Gateway. Sur iOS, les certificats peuvent être fournis à Citrix Secure Access de l'une des manières suivantes :

- Serveur MDM : il s'agit de l'approche préférée des clients MDM. Les certificats sont configurés directement sur le profil VPN géré par MDM. Les profils VPN et les certificats sont ensuite poussés vers les appareils inscrits lorsque l'appareil s'inscrit dans le serveur MDM. Veuillez suivre les documents spécifiques au fournisseur MDM pour cette approche.
- E-mail - Approche uniquement pour les clients non-MDM. Dans cette approche, les administrateurs envoient un e-mail avec l'identité du certificat utilisateur (certificat et clé privée) jointe en tant que fichier PCKS #12 aux utilisateurs. Les utilisateurs doivent configurer leur compte

de messagerie sur leur appareil iOS pour recevoir l'e-mail avec pièce jointe. Le fichier peut ensuite être importé vers Citrix Secure Access sur iOS. La section suivante explique les étapes de configuration de cette approche.

Pré-requis

- Certificat utilisateur : fichier d'identité PKCS #12 avec une extension .pfx ou .p12 pour un utilisateur donné. Ce fichier contient à la fois le certificat et la clé privée.
- Compte de messagerie configuré sur l'appareil iOS.
- Citrix Secure Access est installé sur l'appareil iOS.

Étapes de configuration

1. Renommez le type d'extension/MIME du certificat utilisateur.

Les extensions de fichier les plus couramment utilisées pour le certificat utilisateur sont « .pfx », « .p12 », etc. Ces extensions de fichiers ne sont pas standard sur la plate-forme iOS, contrairement aux formats tels que .pdf, .doc. Les noms « .pfx » et « .p12 » sont tous deux revendiqués par le système iOS et ne peuvent pas être revendiqués par des applications tierces telles que Citrix Secure Access. Citrix Secure Access a donc défini un nouveau type d'extension/MIME appelé « .citrixsso-pfx » et « .citrixsso-p12 ». Les administrateurs doivent modifier le type d'extension/MIME du certificat utilisateur, de « .pfx » ou « .p12 » standard à « .citrixsso-pfx » ou « .citrixsso-p12 »

respectivement. Pour renommer l'extension, les administrateurs peuvent exécuter la commande suivante à partir de l'invite de commandes ou du terminal.

Windows 10

```
1 cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
2 rename <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.
   citrixsso-pfx
3 <!--NeedCopy-->
```

macOS

```
1 cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
2 mv <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-
   pfx
3 <!--NeedCopy-->
```

2. Envoyez le fichier sous forme de pièce jointe à un e-mail.

Le fichier de certificat utilisateur avec la nouvelle extension peut être envoyé sous forme de pièce jointe à l'utilisateur.

À la réception de l'e-mail, les utilisateurs doivent installer le certificat dans Citrix Secure Access.

Configurer le fichier PAC proxy pour l'application Citrix SSO pour les utilisateurs iOS ou le client Citrix Secure Access pour les utilisateurs de macOS

March 27, 2024

Important :

Citrix SSO pour iOS s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur de manière à refléter ce changement de nom.

L'application Citrix Secure pour iOS ou le client Citrix Secure Access pour macOS prennent en charge Auto Proxy Config (fichier PAC proxy) après l'établissement du tunnel VPN. Les administrateurs peuvent utiliser le fichier PAC du proxy pour autoriser tout le trafic HTTP du client à passer par un proxy, y compris la résolution des noms d'hôte.

Comment configurer un fichier PAC proxy

Disposer d'une machine interne pouvant héberger un fichier proxy. Par exemple, considérez que l'adresse IP de la machine est 172.16.111.43 et que le nom du fichier PAC est proxy.pac.

Si l'adresse IP du serveur proxy réel est 172.16.43.83 qui écoute sur le port 8080, alors un exemple de proxy.pac est le suivant :

```
function FindProxyForURL(url, host)
{
return "PROXY 172.16.43.83:8080";
}
```

L'URL du proxy PAC est <http://172.16.111.43/proxy.pac>. En supposant que le fichier soit hébergé sur le port HTTP 80.

Pour plus de détails, consultez <https://support.citrix.com/article/CTX224235> ou [Configuration automatique du proxy pour la prise en charge du proxy sortant pour NetScaler Gateway](#).

Remarque :

- Si Split Tunnel est activé, assurez-vous que l'adresse IP du serveur hébergeant le fichier PAC est incluse dans la liste des applications intranet afin qu'elle soit accessible via VPN.

- Une fois connectés à partir de Citrix Secure Access (macOS/iOS), les navigateurs commencent à utiliser les règles du fichier PAC proxy. Si une seule règle de proxy est fournie, comme dans l'exemple précédent, tout le trafic HTTP ou HTTPS est acheminé vers le serveur proxy interne.

Configurer Citrix Secure Access pour les utilisateurs de macOS

March 27, 2024

Important :

Citrix SSO pour iOS s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur pour refléter ce changement de nom.

Le client Citrix Secure Access pour macOS fournit la meilleure solution d'accès aux applications et de protection des données proposée par NetScaler Gateway. Vous pouvez désormais accéder en toute sécurité aux applications stratégiques, aux bureaux virtuels et aux données d'entreprise depuis n'importe où et à tout moment.

Citrix Secure Access est le client VPN de nouvelle génération pour NetScaler Gateway qui permet de créer et de gérer des connexions VPN à partir d'appareils macOS. Citrix Secure Access est conçu à l'aide du framework Network Extension (NE) d'Apple. NE Framework d'Apple est une bibliothèque moderne qui contient des API pouvant être utilisées pour personnaliser et étendre les fonctionnalités réseau principales de macOS. L'extension réseau prenant en charge le VPN SSL est disponible sur les appareils exécutant macOS 10.11+.

Citrix Secure Access fournit une prise en charge complète de la gestion des appareils mobiles (MDM) sur macOS. Avec un serveur MDM, un administrateur peut désormais configurer et gérer à distance les profils VPN au niveau de l'appareil et les profils VPN par application.

Citrix Secure Access pour macOS peut être installé à partir d'un Mac App Store.

Pour obtenir la liste des fonctionnalités couramment utilisées prises en charge par le client Citrix Secure Access pour macOS, consultez la section [Clients VPN NetScaler Gateway et fonctionnalités prises en charge](#).

Compatibilité avec les produits MDM

Citrix Secure Access pour macOS est compatible avec la plupart des fournisseurs MDM tels que Citrix XenMobile, Microsoft Intune, etc. Il prend en charge une fonctionnalité appelée contrôle d'accès réseau (NAC) grâce à laquelle les administrateurs MDM peuvent faire respecter la conformité des appareils des utilisateurs finaux avant de se connecter à NetScaler Gateway. Le NAC sur Citrix Secure Access nécessite un serveur MDM tel que XenMobile et NetScaler Gateway. Pour plus d'informations

sur le NAC, voir [Configurer la vérification du périphérique de contrôle d'accès réseau pour le serveur virtuel NetScaler Gateway](#) pour une connexion à facteur unique.

Remarque :

Pour utiliser le VPN Citrix Secure Access avec NetScaler Gateway sans MDM, vous devez ajouter une configuration VPN. Vous pouvez ajouter la configuration VPN sur macOS à partir de la page de configuration de Citrix Secure Access.

Configurer un profil VPN géré par MDM pour Citrix Secure Access

La section suivante présente des instructions détaillées pour configurer des profils VPN à la fois à l'échelle de l'appareil et par application pour Citrix Secure Access à l'aide de Citrix Endpoint Management (anciennement XenMobile) à titre d'exemple. D'autres solutions MDM peuvent utiliser ce document comme référence lors de l'utilisation de Citrix Secure Access.

Remarque :

Cette section explique les étapes de configuration d'un profil VPN de base à l'échelle de l'appareil et par application. Vous pouvez également configurer les proxys On-Demand en suivant la documentation de Citrix Endpoint Management (anciennement XenMobile) ou la configuration de la charge utile [du VPN MDM d'Apple](#).

Profils VPN au niveau de l'appareil

Les profils VPN au niveau de l'appareil sont utilisés pour configurer un VPN à l'échelle du système. Le trafic provenant de toutes les applications et de tous les services est canalisé vers NetScaler Gateway en fonction des stratégies VPN (telles que Full-tunnel, Split-tunnel, Reverse Split tunnel) définies dans NetScaler.

Pour configurer un VPN au niveau de l'appareil sur Citrix Endpoint Management Effectuez les étapes suivantes pour configurer un VPN au niveau de l'appareil.

1. Sur la console Citrix Endpoint Management MDM, accédez à **Configurer > Stratégies d'appareil > Ajouter une nouvelle stratégie**.
2. Sélectionnez **macOS** dans le volet de gauche Policy Platform. Sélectionnez **Stratégie VPN** dans le volet droit.
3. Sur la page **Informations sur la stratégie**, saisissez un nom de stratégie et une description valides, puis cliquez sur **Suivant**.
4. Sur la page **de détails de la stratégie** pour macOS, tapez un nom de connexion valide et choisissez **SSL personnalisé** dans **Type de connexion**.

Dans la charge utile VPN MDM, le nom de connexion correspond à la clé **UserDefinedName** et la **clé de type VPN** doit être définie sur **VPN**.

5. Dans **Identificateur SSL personnalisé (format DNS inverse)**, saisissez **com.citrix.netscalergateway.macOS**. Il s'agit de l'identifiant du bundle pour Citrix Secure Access sur macOS.

Dans la charge utile VPN MDM, l'identificateur SSL personnalisé correspond à la clé **VPNSub-type**.

6. Dans l'**identifiant du bundle fournisseur**, saisissez **com.citrix.NetScaler Gateway.macOS.App.VPNPlugin**. Il s'agit de l'identifiant de bundle de l'extension réseau contenue dans le fichier binaire du client Citrix Secure Access.

Dans la charge utile VPN MDM, l'identificateur de bundle de fournisseur correspond à la clé **ProviderBundleIdentifier**.

7. Dans **Nom du serveur ou adresse IP**, entrez l'adresse IP ou le nom de domaine complet du NetScaler associé à cette instance de Citrix Endpoint Management.

Les autres champs de la page de configuration sont facultatifs. Les configurations de ces champs sont disponibles dans la documentation Citrix Endpoint Management.

8. Cliquez sur **Suivant**.

The screenshot shows the 'Configure' page for a 'VPN Policy'. The left sidebar has 'macOS' selected under 'Platforms'. The main area contains the following configuration fields:

- Connection name:** SJC-UIGDEV-MACOS
- Connection type:** Custom SSL
- Custom SSL Identifier (reverse DNS format):** com.citrix.NetScalerGateway.macOS.app
- Server name or IP address:** sjc-ugdev.citrix.com
- User account:** (empty)
- Authentication type for the connection:** Password
- Auth Password:** (empty)
- Per-app VPN:** OFF (IOS 7.0+)
- Custom XML:** (empty table with 'Parameter name' and 'Value' columns)
- Proxy configuration:** None

9. Cliquez sur **Enregistrer**.

Profils VPN par application

Les profils VPN par application sont utilisés pour configurer un VPN pour une application spécifique. Le trafic provenant uniquement de l'application spécifique est canalisé vers NetScaler Gateway. La **charge utile VPN par application prend en charge toutes les clés du VPN** à l'échelle de l'appareil, ainsi que quelques autres clés.

Pour configurer un VPN au niveau de l'application sur Citrix Endpoint Management Effectuez les étapes suivantes pour configurer un VPN par application sur Citrix Endpoint Management :

1. Terminez la configuration VPN au niveau de l'appareil sur Citrix Endpoint Management.
2. **Activez le commutateur Activer le VPN par application** dans la section **VPN par application**.
3. Activez le **commutateur On-Demand Match App Enabled** si Citrix Secure Access doit être démarré automatiquement lors du lancement de l'application Match. Cette option est recommandée pour la plupart des cas par application.

Dans la charge utile VPN MDM, ce champ correspond à la clé **OnDemandMatchAppEnabled**.

4. La configuration du domaine Safari est facultative. Lorsqu'un domaine Safari est configuré, Citrix Secure Access démarre automatiquement lorsque les utilisateurs lancent Safari et accèdent à une URL correspondant à celle du champ **Domaine** . Cette option n'est pas recommandée si vous souhaitez restreindre le VPN pour une application spécifique.

Dans la charge utile VPN MDM, ce champ correspond à la clé **SafariDomains**.

Les autres champs de la page de configuration sont facultatifs. Les configurations de ces champs sont disponibles dans la documentation Citrix Endpoint Management (anciennement XenMobile).

The screenshot shows the 'Configure' tab for a 'VPN Policy'. On the left, a sidebar lists platforms, with 'macOS' selected. The main area contains the following configuration fields:

- Connection name:** SJC-UGDEV-MACOS
- Connection type:** Custom SSL
- Custom SSL Identifier (reverse DNS format):** com.citrix.NetScalerGateway.macos.app
- Server name or IP address:** sjcugdev.citrix.com
- User account:** (empty field)
- Authentication type for the connection:** Password
- Auth Password:** (empty field)
- Per-app VPN:** ON (IOS 7.0+)
- On-demand match app enabled:** ON
- Safari domains:** A table with one row containing 'Domain' and an 'Add' button.
- Custom XML:** A section for 'Custom parameters'.

At the bottom right, there are 'Back' and 'Next >' buttons.

5. Cliquez sur **Suivant**.
6. Cliquez sur **Enregistrer**.

Pour associer le profil VPN à une application spécifique sur l'appareil, vous devez créer une stratégie d'inventaire des applications et une stratégie de fournisseur d'informations d'identification en suivant ce guide : <https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/>

Configuration du split tunnel dans un VPN par application

Les clients MDM peuvent configurer le split tunnel dans le VPN par application pour Citrix Secure Access. La paire clé/valeur suivante doit être ajoutée à la section de configuration du fournisseur du profil VPN créé sur le serveur MDM.

- 1 - Key = "PerAppSplitTunnel"
- 2 - Value = "true or 1 or yes"

La clé est sensible à la casse et doit correspondre exactement à la casse, tandis que la valeur n'est pas sensible à la casse.

Remarque :

L'interface utilisateur permettant de configurer la configuration du fournisseur n'est pas standard parmi les fournisseurs MDM. Contactez le fournisseur MDM pour trouver la section de configuration du fournisseur sur votre console utilisateur MDM.

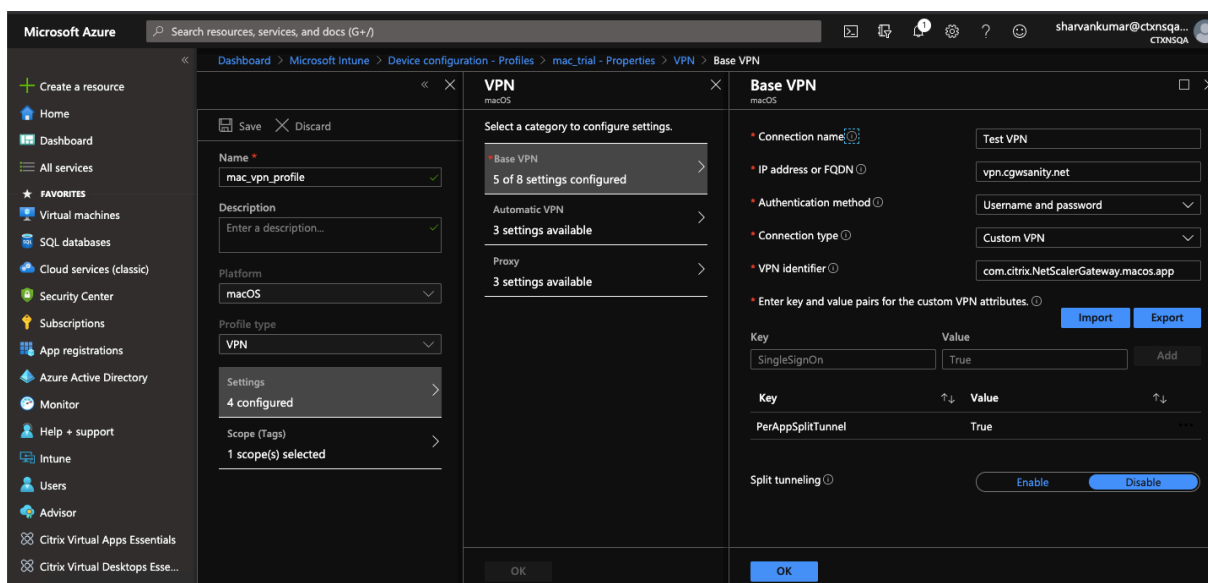
Voici un exemple de capture d'écran de la configuration (paramètres spécifiques au fournisseur) dans Citrix Endpoint Management.

The screenshot shows the 'Configure' page for a VPN Policy in Citrix Endpoint Management. The left sidebar shows 'VPN Policy' with 'iOS' selected under 'Platforms'. The main area shows configuration options for 'Enable per-app VPN' (ON), 'On-demand match app enabled' (ON), and 'Provider type' (Packet tunnel). A red box highlights the 'Custom XML' section, which contains a table of custom parameters:

Parameter name *	Value	Add
PerAppSplitTunnel	true	

Other visible settings include 'Proxy configuration' (None), 'Remove policy' (Select date), and 'Allow user to remove policy' (Always).

Voici un exemple de capture d'écran de la configuration (paramètres spécifiques au fournisseur) dans Microsoft Intune.



Désactivation des profils VPN créés par les utilisateurs

Les clients MDM peuvent empêcher les utilisateurs de créer manuellement des profils VPN à partir de Citrix Secure Access. Pour ce faire, la paire clé/valeur suivante doit être ajoutée à la section de configuration du fournisseur du profil VPN créé sur le serveur MDM.

- 1 - Key = "disableUserProfiles"
- 2 - Value = "true or 1 or yes"

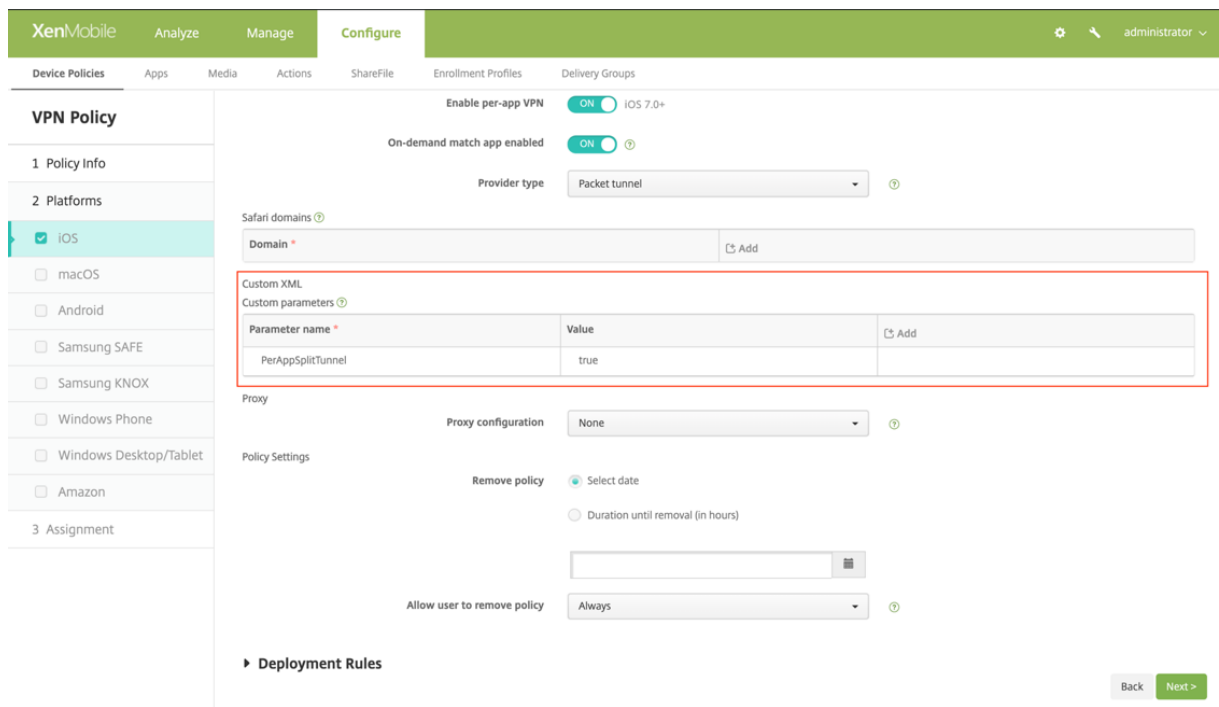
La clé est sensible à la casse et doit correspondre exactement à la casse, tandis que la valeur n'est pas sensible à la casse.

Remarque :

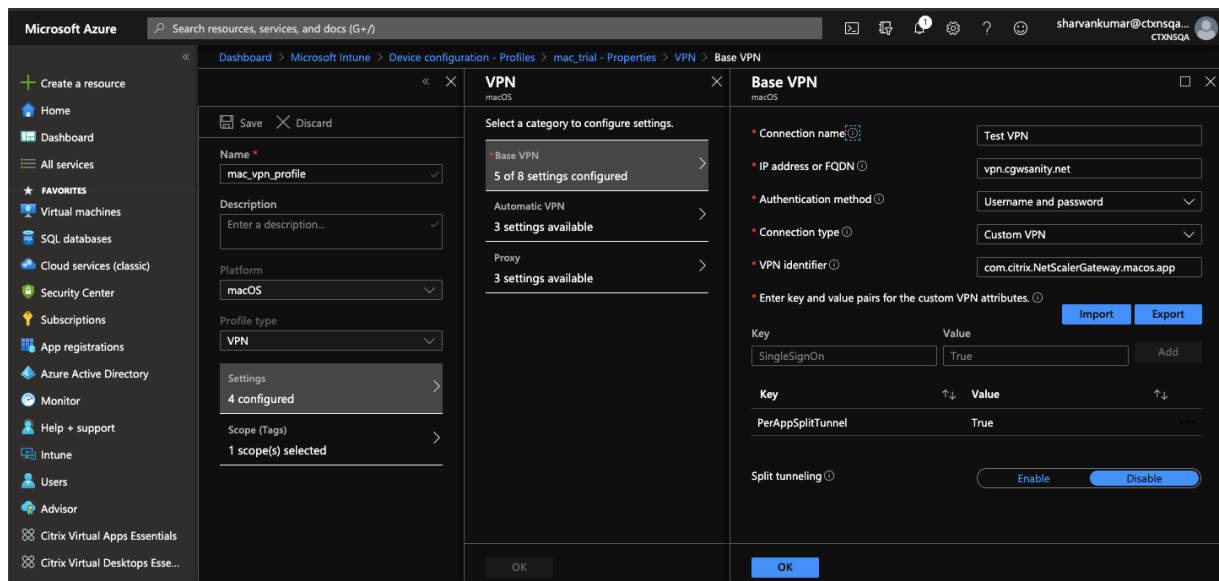
L'interface utilisateur permettant de configurer la configuration du fournisseur n'est pas standard parmi les fournisseurs MDM. Contactez le fournisseur MDM pour trouver la section de configuration du fournisseur sur votre console utilisateur MDM.

Voici un exemple de capture d'écran de la configuration (paramètres spécifiques au fournisseur) dans Citrix Endpoint Management.

Clients NetScaler Gateway



Voici un exemple de capture d'écran de la configuration (paramètres spécifiques au fournisseur) dans Microsoft Intune.



Gestion DNS

Les paramètres DNS recommandés pour Citrix Secure Access sont les suivants :

- **Split DNS > REMOTE** si le split tunnel est réglé **sur OFF**.
- **Split DNS > BOTH** si le split tunnel est défini **sur ON**. Dans ce cas, les administrateurs doivent

ajouter des suffixes DNS pour les domaines intranet. Les requêtes DNS pour les noms de domaine complets appartenant à des suffixes DNS sont acheminées vers l'appliance NetScaler et les requêtes restantes sont acheminées vers le routeur local.

Remarque :

- Il est recommandé que l'indicateur de **correction de troncature DNS** soit toujours **actif**. Pour plus de détails, consultez <https://support.citrix.com/article/CTX200243>.
- Lorsque le split tunnel est défini **sur ON** et que Split DNS est défini sur **REMOTE**, des problèmes peuvent survenir lors de la résolution des requêtes DNS après la connexion du VPN. Cela est lié au fait que le framework Network Extension n'intercepte pas toutes les requêtes DNS.

Analyses EPA prises en

Pour obtenir la liste complète des scans pris en charge, voir [Dernières bibliothèques EPA](#).

1. Dans la section **Matrice d'analyse prise en charge par OPSWAT v4**, cliquez sur **Liste des applications prises en charge** sous la colonne **Spécifique à MAC OS**.
2. Dans le fichier Excel, cliquez sur l'onglet **Analyses EPA classiques** pour afficher les détails.

Problèmes connus

Voici les problèmes connus actuellement.

- La connexion EPA échoue si l'utilisateur est placé dans le groupe de quarantaine.
- Le message d'avertissement de délai d'expiration forcé n'est pas affiché.
- Citrix Secure Access autorise la connexion si le split tunnel est activé et qu'aucune application intranet n'est configurée.

Limitations

Voici les limitations actuelles.

- Les analyses EPA suivantes peuvent échouer en raison de l'accès restreint à Secure Access dû au sandboxing.
 - « Type » et « chemin » de chiffrement du disque dur
 - Navigateur Web « par défaut » et « en cours d'exécution »
 - Gestion des correctifs « correctifs manquants »
 - Fonctionnement du processus d'élimination pendant l'EPA

- Le split tunneling basé sur les ports/protocoles n'est pas pris en charge.
- Assurez-vous que le trousseau de clés ne contient pas deux certificats portant le même nom et la même date d'expiration, car cela fait en sorte que le client n'affiche qu'un seul des certificats au lieu des deux.

Dépannage

Si le bouton **Télécharger le plug-in EPA est affiché aux utilisateurs finaux dans** la fenêtre d'authentification de Citrix Secure Access, cela signifie que la politique de sécurité du contenu de l'appliance NetScaler bloque l'invocation de l'URL `com.citrix.agmacepa://`. Les administrateurs doivent modifier la stratégie de sécurité du contenu de manière à ce que `com.citrix.agmacepa://` soit autorisé.

Support de nFactor pour le client Citrix Secure Access sur macOS/iOS

March 27, 2024

Important :

Citrix SSO pour iOS s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur de manière à refléter ce changement de nom.

L'authentification multi-facteurs (nFactor) améliore la sécurité d'une application en obligeant les utilisateurs à fournir plusieurs preuves d'identité pour y accéder. Les administrateurs peuvent configurer différents facteurs d'authentification, notamment le certificat client, LDAP, RADIUS, OAuth, SAML, etc. Ces facteurs d'authentification peuvent être configurés dans n'importe quel ordre en fonction des besoins de l'organisation.

Le client Citrix Secure Access sur macOS/iOS prend en charge les protocoles d'authentification suivants :

- **nFactor** — Le protocole nFactor est utilisé lorsqu'un serveur virtuel d'authentification est lié au serveur virtuel VPN sur la passerelle. Étant donné que l'ordre des facteurs d'authentification est dynamique, le client utilise une instance de navigateur rendue dans le contexte de l'application pour présenter l'interface graphique d'authentification.
- **Classique** : le protocole classique est le protocole de secours par défaut utilisé si les stratégies d'authentification classiques sont configurées sur le serveur virtuel VPN de la passerelle. Le protocole classique est le protocole de secours si nFactor échoue pour des méthodes d'authentification spécifiques telles que NAC.

- **Plateforme d'identité Citrix** : le protocole de plateforme d'identité Citrix est utilisé lors de l'authentification auprès de CloudGateway ou du service Citrix Gateway et nécessite une inscription MDM auprès de Citrix Cloud.

Le tableau suivant récapitule les différentes méthodes d'authentification prises en charge par chaque protocole.

Méthode d'authentification	nFactor	Classique	IdP Citrix
Cert Client	Pris en charge	Pris en charge	Non pris en charge
LDAP	Pris en charge	Pris en charge	Non pris en charge
Stockage local	Pris en charge	Pris en charge	Non pris en charge
RADIUS	Pris en charge	Non pris en charge	Non pris en charge
SAML	Pris en charge	Non pris en charge	Non pris en charge
OAuth	Pris en charge	Non pris en charge	Non pris en charge
TACACS	Pris en charge	Non pris en charge	Non pris en charge
WebAuth	Pris en charge	Non pris en charge	Non pris en charge
Négociateur	Pris en charge	Non pris en charge	Non pris en charge
EPA	Pris en charge	Pris en charge	Non pris en charge
NAC	Non pris en charge	Pris en charge	Non pris en charge
StoreFront	Non pris en charge	Non pris en charge	Non pris en charge
ADAL	Non pris en charge	Non pris en charge	Non pris en charge
DS-AUTH	Non pris en charge	Non pris en charge	Pris en charge

Configuration NFactor

Pour plus d'informations sur la configuration de NFactor, reportez-vous à la section [Configuration de l'authentification NFactor](#).

Important :

pour utiliser le protocole nFactor avec le client Citrix Secure Access sur macOS/iOS, la version locale recommandée de NetScaler Gateway est 12.1.50.xx et versions ultérieures.

Limitations

- Les stratégies d'authentification spécifiques aux appareils mobiles, telles que le NAC (contrôle d'accès réseau), exigent que le client envoie un identifiant d'appareil signé dans le cadre de l'authentification avec NetScaler Gateway. L'identificateur d'appareil signé est une clé secrète rotative qui identifie de manière unique un appareil mobile inscrit dans un environnement MDM. Cette clé est intégrée dans un profil VPN géré par un serveur MDM. Il n'est peut-être pas possible d'injecter cette clé dans le contexte WebView. Si le NAC est activé sur un profil VPN MDM, le client Citrix Secure Access sur macOS/iOS revient automatiquement au protocole d'authentification classique.
- Vous ne pouvez pas configurer la vérification NAC avec Intune pour macOS, car Intune ne fournit pas d'option permettant d'activer NAC pour macOS contrairement à iOS.

Résolution des problèmes courants liés à Citrix Secure Access pour macOS/iOS

March 27, 2024

Important :

Citrix SSO pour iOS s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur pour refléter ce changement de nom.

Problèmes de résolution DNS

- Si l'appareil se met en veille ou est inactif pendant une longue période, la reprise du VPN peut prendre environ 30 à 60 secondes. Pendant cette période, les utilisateurs peuvent voir certaines requêtes DNS échouer. Les demandes DNS sont résolues automatiquement après une courte période.
Si les requêtes DNS ne sont pas résolues, il est possible qu'une stratégie d'autorisation avancée bloque le trafic DNS. Reportez-vous <https://support.citrix.com/article/CTX232237> à la section pour résoudre ce problème.
- Vérifiez toujours la résolution DNS à partir des navigateurs. Les requêtes DNS utilisant la `nslookup` commande du terminal peuvent ne pas être exactes. Si vous devez utiliser la `nslookup` commande, vous devez inclure l'adresse IP du client dans la commande. Par exemple, `nslookup website_name 172.16.255.1`.

Problèmes EPA

- Gatekeeper est considéré comme un antivirus. S'il existe une analyse qui recherche « tout antivirus » (MAC-ANTIVIR_0_0), l'analyse est toujours effectuée même si l'utilisateur n'a pas installé d'antivirus d'autres fournisseurs.

Remarque :

- Activez la journalisation de sécurité du client pour obtenir les journaux de débogage pour EPA. Vous pouvez activer la journalisation de sécurité du client en définissant le paramètre `clientsecurityLog VPN` sur ON.
- Le logiciel de gestion des correctifs intégré d'Apple est « Software Update ». Il correspond à l'application « App Store » de l'appareil. La version de la « mise à jour logicielle » doit être similaire à "MAC-PATCH_100011_100076_VERSION_==_3.0[COMMENT: Software Update]"
- Maintenez toujours à jour les bibliothèques EPA sur NetScaler. Les dernières bibliothèques sont disponibles à l'adresse <https://www.citrix.com/downloads/citrix-gateway/epa-libraries/epa-libraries-for-netscaler-gateway.html>

Problèmes NFactor

- Citrix Secure Access ouvre la fenêtre d'authentification **Citrix SSO** pour l'authentification nFactor. Il est similaire à un navigateur. S'il y a des erreurs sur cette page, elles peuvent être vérifiées de manière croisée en essayant l'authentification sur un navigateur Web.
- Si l'ouverture de session de transfert échoue lorsque nFactor est activé, modifiez le thème du portail en « RFWebUI ».
- Si vous recevez le message d'erreur « Impossible d'établir une connexion sécurisée à NetScaler Gateway car la chaîne de certificats ne contient aucun des certificats requis. Veuillez contacter votre administrateur » ou « Passerelle inaccessible », puis le certificat du serveur de passerelle a expiré ou le certificat de serveur est lié au SNI activé. Citrix Secure Access ne prend pas encore en charge le SNI. Liez le certificat de serveur sans que le SNI soit activé. L'erreur peut également être due à l'épinglage des certificats configuré dans le profil VPN MDM et au fait que le certificat présenté par NetScaler Gateway ne correspond pas au certificat épinglé.
- Lorsque vous essayez de vous connecter à la passerelle, si la **fenêtre d'authentification Citrix SSO** s'ouvre mais est vide, vérifiez si la courbe ECC (ALL) est liée au groupe de chiffrement par défaut. La courbe ECC (ALL) doit être liée au groupe de chiffrement par défaut.

Vérification du contrôle d'accès réseau (NAC)

La stratégie d'authentification NAC est prise en charge uniquement dans l'authentification classique. Il n'est pas pris en charge dans le cadre de l'authentification NFactor.

FAQ

March 27, 2024

Important :

Citrix SSO pour iOS s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur de manière à refléter ce changement de nom.

Cette section présente la FAQ sur Citrix Secure Access pour macOS/iOS.

En quoi le client Citrix Secure Access pour macOS/iOS est-il différent de l'application VPN ?

Le client Citrix Secure Access pour macOS et le client Citrix Secure Access pour iOS (anciennement connu sous le nom de Citrix SSO pour iOS) constituent le client VPN SSL de nouvelle génération pour NetScaler. L'application utilise le cadre d'extension réseau d'Apple pour créer et gérer les connexions VPN sur les appareils iOS et macOS. Citrix VPN est l'ancien client VPN qui utilise les API VPN privées d'Apple, désormais obsolètes. Le support pour Citrix VPN n'est plus disponible sur l'App Store.

Qu'est-ce que NE ?

Le framework Network Extension (NE) d'Apple est une bibliothèque moderne qui contient des API pouvant être utilisées pour personnaliser et étendre les fonctionnalités réseau principales d'iOS et de macOS.

L'extension réseau prenant en charge le VPN SSL est disponible sur les appareils fonctionnant sous iOS 9+ et macOS 10.11+.

Pour quelles versions de NetScaler le client Citrix Secure Access pour macOS/iOS est-il compatible ?

Les fonctionnalités VPN du client Citrix Secure Access pour macOS/iOS sont prises en charge sur les versions 10.5 et supérieures de NetScaler. Le TOTP est disponible sur NetScaler version 12.0 et supérieure. La notification push sur NetScaler n'a pas encore été annoncée publiquement. L'application nécessite les versions iOS 9+ et macOS 10.11+.

Comment fonctionne l'authentification CERT pour les clients non-MDM ?

Les clients qui distribuaient auparavant des certificats par e-mail ou par navigateur pour effectuer l'authentification des certificats clients dans un VPN doivent prendre en compte cette modification lorsqu'ils utilisent le client Citrix Secure Access pour macOS/iOS. Cela est principalement vrai pour les clients non MDM qui n'utilisent pas de serveur MDM pour distribuer des certificats utilisateur.

Qu'est-ce que le contrôle d'accès réseau (NAC) ? Comment configurer NAC avec Citrix Secure Access pour iOS et NetScaler Gateway ?

Les clients MDM de Microsoft Intune et Citrix Endpoint Management (anciennement XenMobile) peuvent tirer parti de la fonctionnalité de contrôle d'accès réseau (NAC) de Citrix Secure Access pour iOS.

Avec le NAC, les administrateurs peuvent sécuriser le réseau interne de leur entreprise en ajoutant un niveau d'authentification supplémentaire pour les appareils mobiles gérés par un serveur MDM. Les administrateurs peuvent appliquer un contrôle de conformité des appareils au moment de l'authentification dans Citrix Secure Access pour iOS.

Pour utiliser le NAC avec Citrix Secure Access pour iOS, vous devez l'activer à la fois sur NetScaler Gateway et sur le serveur MDM.

- Pour activer le NAC sur NetScaler, voir [Configurer la vérification du périphérique de contrôle d'accès réseau pour le serveur virtuel NetScaler Gateway pour une connexion à facteur unique](#).
- Si Intune est un fournisseur MDM, consultez la section [Intégration du contrôle d'accès réseau \(NAC\) à Intune](#).
- Si un fournisseur MDM est Citrix Endpoint Management (anciennement XenMobile), consultez [Contrôle d'accès réseau](#).

Remarque :

La version minimale du client Citrix Secure Access pour macOS/iOS prise en charge est la version 1.1.6 et supérieure.

Citrix Secure Access pour Android

March 27, 2024

Citrix Secure Access (anciennement Citrix SSO) pour Android fournit la meilleure solution d'accès aux applications et de protection des données proposée par NetScaler Gateway. Vous pouvez désormais accéder en toute sécurité aux applications stratégiques, aux bureaux virtuels et aux données d'entreprise depuis n'importe où et à tout moment.

Important :

- Citrix SSO pour Android s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur de manière à refléter ce changement de nom.
- Le client Citrix Secure Access pour Android fonctionne dans le sous-système Android basé sur ChromeOS. Il fonctionne avec ChromeOS s'il est installé en tant qu'application Android depuis le Play Store et peut tunneler n'importe quelle application du sous-système Android.

Notes de publication

March 27, 2024

Important :

- Citrix SSO pour Android est désormais renommé Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur de manière à refléter ce changement de nom. Vous remarquerez peut-être les références Citrix SSO utilisées dans la documentation pendant cette période de transition.
- Le split tunneling basé sur FQDN et la prise en charge de l'authentification nFactor sont actuellement en préversion
- Citrix Secure Access n'est pas pris en charge pour Android 6.x et les versions antérieures après juin 2020.

Les notes de mise à jour de Citrix Secure Access décrivent les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes, les problèmes résolus et les problèmes connus disponibles dans une version de service. Les notes de publication incluent une ou plusieurs des sections suivantes :

Nouveautés : les nouvelles fonctionnalités et améliorations disponibles dans la version actuelle.

Problèmes résolus : problèmes résolus dans la version actuelle.

Problèmes connus : problèmes qui existent dans la version actuelle et solutions de contournement, le cas échéant.

V23.12.2 (15 décembre 2023)

Remarque :

Citrix Secure Access pour Android version 23.12.2 inclut le correctif pour CSACLIENTS-8799 et remplace la version 23.12.1.

[CSACLIENTS-8799]

Nouveautés

- **Citrix SSO pour Android renommé Citrix Secure Access**

Citrix SSO pour Android s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur de manière à refléter ce changement de nom.

[CSACLIENTS-6337]

- **Recevoir ou bloquer des notifications sur un appareil Android 13+**

Lors de l'installation ou de la réinstallation du client Citrix Secure Access sur un appareil Android 13, les utilisateurs finaux sont désormais invités à autoriser la réception de notifications de la part du client Citrix Secure Access. Si les utilisateurs finaux refusent l'autorisation, ils ne recevront aucun statut VPN ni aucune notification push de la part du client Citrix Secure Access sur leurs appareils Android. Il est conseillé aux administrateurs MDM d'accorder l'autorisation de notification à Citrix Secure Access (Package ID : `com.citrix.CitrixVPN`) dans leur solution.

Les utilisateurs finaux peuvent accéder à **Paramètres > Notifications** sur l'appareil Android pour modifier l'autorisation de notification pour le client Citrix Secure Access. Pour plus d'informations, consultez la section [Comment utiliser Citrix Secure Access depuis votre appareil Android](#).

[CSACLIENTS-8252]

- **Prise en charge de la connexion par transfert en mode VPN Always On**

Citrix Secure Access pour Android prend désormais en charge la fonctionnalité Transfer Logon en mode VPN Always On. Pour plus d'informations sur la configuration de l'ouverture de session de transfert, voir [Configuration de la page d'ouverture de session de transfert](#).

[CSACLIENTS-8305]

Problèmes résolus

Citrix Secure Access se bloque lorsque les utilisateurs copient le jeton OTP basé sur le temps (TOTP) sur l'appareil Android 13+.

[CSACLIENTS-8799]

V23.10.2 (19 décembre 2023)

Nouveautés

Remarques :

- La version 23.10.2 de Citrix SSO pour Android inclut le correctif pour CSACLIENTS-8314 et remplace la version 23.10.1.
- Citrix SSO pour Android 23.10.1 fonctionne avec Android 14.

- **Réauthentifiez-vous auprès de NetScaler Gateway après un échec de connexion VPN - Aperçu**

Citrix SSO pour Android vous invite désormais à vous authentifier à nouveau auprès de NetScaler Gateway en cas de perte de connexion VPN. L'interface utilisateur Citrix SSO et le panneau de notification de votre appareil Android vous indiquent que la connexion à NetScaler Gateway est perdue et que vous devez vous authentifier à nouveau pour reprendre la connexion. Cette fonctionnalité est disponible dans la Tech Preview.

Pour plus d'informations, voir [Reconnexion à NetScaler Gateway après un échec de connexion VPN](#).

Problèmes résolus

Le Citrix SSO se bloque par intermittence lors du redémarrage du service VPN dans certains scénarios Always On VPN.

[CSACLIENTS-8314]

V23.8.1 (31 août 2023)

Nouveautés

- **Redémarrage automatique du VPN Always On**

L'application Citrix SSO redémarre automatiquement le VPN Always On lorsqu'une application faisant partie de la liste d'autorisation ou de blocage est installée dans un profil professionnel ou un profil d'appareil. Le trafic provenant de cette application est automatiquement acheminé via une connexion VPN sans redémarrer le profil professionnel ni redémarrer l'appareil. Pour activer le redémarrage automatique du VPN Always On, les utilisateurs finaux doivent autoriser [tous les packages Query](#) à l'application Citrix SSO. Pour plus d'informations, consultez [Redémarrage automatique d'Always On VPN](#).

[CSACLIENTS-6158]

- **Activer la journalisation du débogage dans un profil VPN géré**

Les administrateurs MDM peuvent désormais activer la journalisation du débogage en tant que paramètre personnalisé dans le profil VPN géré de la console Endpoint Management. Pour activer la journalisation du débogage, la valeur de `EnableDebugLogging` doit être définie sur True. Si la journalisation de débogage est activée dans l'une des configurations VPN gérées, la fonctionnalité de journalisation du débogage prend effet lorsque les configurations sont analysées. Pour plus de détails, voir [Paramètres personnalisés pour la configuration d'Intune](#).

[CSACLIENTS-3746]

Problèmes résolus

- Parfois, l'application Citrix SSO ne parvient pas à canaliser le trafic vers certaines ressources. Ce problème se produit lorsque le split tunneling est défini sur OFF et que certains domaines ou adresses IP inaccessibles sont bloqués.

[NSHELP-35555]

V22.11.1 (30 novembre 2022)

Nouveautés

- **Citrix Secure Access est mis à jour pour cibler Android 12.1 (niveau d'API 32)**

Citrix Secure Access est désormais mis à jour pour cibler Android 12.1 (niveau d'API 32). Dans le cas d'un VPN par application, le service VPN risque de ne pas redémarrer automatiquement si l'un des packages de la liste des packages VPN par application est installé après la configuration du tunnel VPN. Cela est dû aux restrictions de visibilité des applications introduites dans Android 11. Pour plus de détails, consultez <https://developer.android.com/training/package-visibility>.

[CGOP-21409]

V22.10.1 (21 octobre 2022)

Nouveautés

- L'affichage du numéro de version de l'application est mis à jour au format YY.MM.Point-Release, où YY est l'année à 2 chiffres, MM est le mois à 2 chiffres et le point release est égal ou supérieur à 1+ en fonction du numéro de version du mois.
- La collecte de données Google Analytics/Crashlytics depuis la région de l'UE est désactivée pour les clients Android.

Problèmes résolus

- Les messages d'erreur qui apparaissent pour une entrée non valide dans les écrans Ajouter une connexion et Modifier une connexion ne sont pas localisés.

[CGOP-22060]

V2.5.3 (05 mai 2022)

Nouveautés

- Citrix SSO mis à jour vers le SDK cible Android 11 (API 30)

L'application Citrix SSO est désormais mise à jour vers le SDK cible Android 11 (API 30). Cette modification nécessite que les API Microsoft Intune NAC v2 soient utilisées par NetScaler Gateway pour vérifier la conformité des appareils. Pour plus de détails, consultez l'article de la base de connaissances <https://support.citrix.com/article/CTX331615>.

[CGOP-19774]

Problèmes résolus

- Il arrive parfois que Citrix SSO n'utilise pas de serveur DNS alternatif pour la résolution du nom d'hôte après une modification du réseau.

[NSHELP-29378]

V2.5.2 (21 octobre 2021)

Problèmes résolus

- Parfois, Citrix SSO se bloque lors de la gestion d'une erreur de non-conformité lors de la vérification NAC.

[CGOP-19198]

V2.5.1 (12 août 2021)

Problèmes résolus

- L'application Citrix SSO ne parvient pas à résoudre l'hôte lorsque la chaîne CNAME est supérieure à 6 sauts.

[CGOP-18475]

- Citrix SSO affiche une invite d'authentification lorsque NetScaler Gateway requiert uniquement l'authentification par contrôle NAC.

[CGOP-18348]

- Citrix SSO peut se bloquer lors du traitement de paquets ICMP exceptionnellement volumineux.

[CGOP-18286]

- Citrix SSO peut se bloquer lors de l'ajout d'un profil VPN sur certains appareils Android 8.0.
[CGOP-17607]
- Citrix SSO peut se bloquer lorsque vous redémarrez le VPN configuré pour Always On.
[CGOP-17580]
- Citrix SSO peut se bloquer lors de la gestion d'une erreur SSL dans le flux d'authentification nFactor.
[CGOP-17577]

V2.5.0 (8 juin 2021)

Nouveautés

- **Prise en charge du split tunneling basé sur le nom de domaine complet**
Citrix SSO pour Android prend désormais en charge le split tunneling basé sur le nom de domaine complet.
[CGOP-12079]

Problèmes résolus

- Citrix SSO Preview build 2.5.0 ne parvient pas (110) à se connecter aux versions 12.1 et antérieures de NetScaler Gateway.
[CGOP-17735]
- Le paramètre « DisableUserProfiles » n'est pas appliqué après le redémarrage de l'application SSO.
[CGOP-17454]

V2.4.16 (31-Mar-2021)

Problèmes résolus

- L'authentification NFactor est abandonnée si la navigation sécurisée n'est pas activée sur certains appareils.
[CGOP-17514]

V2.4.15 (17-Mar-2021)

Problèmes résolus

- Parfois, Citrix SSO ne reconnecte pas le VPN Always On lorsque le délai de session expire sur l'appliance NetScaler Gateway.

[CGOP-16800]

V2.4.14 (23-Feb-2021)

Problèmes résolus

- Citrix SSO nécessite une interaction de l'utilisateur lorsque le VPN Always-On avec authentification par certificat uniquement est utilisé avec l'authentification nFactor.

[CGOP-16805]

- Parfois, Citrix SSO peut se bloquer lors du redémarrage ou de la transition du service VPN.

[CGOP-16766]

V2.4.13 (04-Feb-2021)

Problèmes résolus

- Dans certains cas, la demande de connexion Citrix SSO expire avant que NetScaler Gateway ne réponde.

[CGOP-16759]

V2.4.12 (15 janvier 2021)

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

V2.4.11 (08-Jan-2021)

- L'authentification classique échoue car le Citrix SSO envoie un en-tête HTTP (X-Citrix-Gateway) à NetScaler Gateway qui est utilisé uniquement dans l'authentification nFactor.

[CGOP-16449]

V2.4.10 (09-Dec-2020)

Problèmes résolus

- Parfois, l'authentification classique peut échouer sur les appareils Android.
[CGOP-16219]
- Citrix SSO peut se bloquer lors de l'authentification classique.
[CGOP-16012]
- L'orientation de l'application Citrix SSO ne change pas lorsque vous faites pivoter l'appareil.
[CGOP-639]

V2.4.9 (20-Nov-2020)

Problèmes résolus

- L'application Citrix SSO se bloque lorsqu'un utilisateur tape sur la valeur du jeton TOTP sur l'appareil.
[CGOP-15886]

V2.4.8 (04-Nov-2020)

Problèmes résolus

- Citrix SSO peut se bloquer lors de la déconnexion du VPN après un délai d'expiration de session sur la passerelle.
[CGOP-15592]

V2.4.7 (12-Oct-2020)

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

V2.4.6 (28-Sep-2020)

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

V2.4.5 (16-Sep-2020)

Nouveautés

- Le nouveau logo NetScaler est introduit.

[CGOP-15327]

V2.4.4 (10-Sep-2020)

Problèmes résolus

- Parfois, Citrix SSO se bloque lors de la reconnexion de la session VPN.

[CGOP-15215]

V2.4.3

Problèmes connus

- Citrix SSO ne parvient pas à établir de session VPN vers NetScaler Gateway lorsque les ressources de l'appareil Android sont limitées.

[NSHELP-24647]

V2.4.2

Problèmes résolus

- L'application Citrix SSO se bloque lors du chargement de données de jeton corrompues précédemment enregistrées. Avec ce correctif, la valeur du jeton s'affiche sous la forme « Données de jeton corrompues » pour les jetons corrompus dans la liste des jetons. Supprimez les jetons corrompus et ajoutez-les à nouveau.

[CGOP-14546]

V2.4.1

Problèmes résolus

- L'application Citrix SSO n'est pas prise en charge pour Android 6.x et les versions antérieures après juin 2020.

[CGOP-13853]

V2.3.19

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

V2.3.18

Nouveautés

- La configuration du proxy est désormais prise en charge dans l'application Android Citrix SSO pour les appareils Android 10.

[CGOP-12007]

V2.3.17

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

V2.3.16

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

V2.3.15

Nouveautés

- L'application Citrix SSO prend désormais en charge l'épinglage des certificats NetScaler Gateway pour les profils VPN gérés.

[CGOP-12538]

- L'application Citrix SSO pour Android 10 détecte désormais le VPN Always On dans les paramètres système.

[CGOP-12656]

Problèmes résolus

- L'application Citrix SSO se bloque lors de la déconnexion du VPN si seuls des profils VPN MDM sont définis.

[CGOP-13825]

V2.3.14

Nouveautés

- L'application Citrix SSO peut désormais effectuer l'authentification des utilisateurs au nom de l'application Citrix Workspace pour l'authentification unique des applications natives.

[CGOP-12083]

- Le service VPN redémarre si l'un des packages de la liste des packages VPN par application est installé après la configuration du tunnel VPN.

[CGOP-11262]

Problèmes résolus

- Citrix SSO gère désormais correctement le message final d'établissement de la session VPN.

[CGOP-12488]

- L'adresse IP de NetScaler Gateway n'est désormais résolue qu'une seule fois. Auparavant, l'adresse IP de NetScaler Gateway avait été résolue à plusieurs reprises, ce qui entraînait parfois des échecs de connexion.

[CGOP-12101]

Problèmes connus

- L'état du VPN Always-On n'est pas toujours mis à jour correctement dans l'interface utilisateur de l'application.

[NSHELP-21709]

V2.3.13

Problèmes résolus

- L'adresse IP de NetScaler Gateway n'est désormais résolue qu'une seule fois.

Auparavant, l'adresse IP de NetScaler Gateway avait été résolue à plusieurs reprises, ce qui entraînait parfois des échecs de connexion.

[CGOP-12101]

Problèmes connus

- L'état du VPN Always-On n'est pas toujours mis à jour correctement dans l'interface utilisateur de l'application.

[NSHELP-21709]

V2.3.12

Problèmes résolus

- Citrix SSO peut se bloquer lors de l'enregistrement d'un profil VPN.

[CGOP-12137]

V2.3.11

Problèmes résolus

- Citrix SSO peut se bloquer lors de l'enregistrement d'un profil VPN.

[CGOP-12137]

- Le paramètre DisableUserProfile n'est pas correctement reflété dans l'interface utilisateur lorsqu'un nouveau profil VPN ou la mise à jour d'un profil existant entraîne la modification de la valeur DisableUserProfile.

[CGOP-11899]

- Citrix SSO pour Android ne traite pas les profils VPN en mode Propriétaire de l'appareil (DO).

[CGOP-11981]

- La connexion VPN n'est pas établie lorsqu'il existe uniquement des serveurs DNS locaux IPv6.

[CGOP-12053]

V2.3.10

Problèmes résolus

- La connexion VPN est perdue après un certain temps d'inactivité sur l'appareil.
[CGOP-11381]

V2.3.8

Nouveautés

- **Configuration de l'application Citrix SSO dans un environnement Intune Android Enterprise**

Vous pouvez désormais configurer l'application Citrix SSO dans un environnement Intune Android Enterprise. Pour plus d'informations, consultez la section [Configurer l'application Citrix SSO dans un environnement Intune Android Enterprise](#).

[CGOP-635]

- **Prise en charge du provisionnement de profils VPN via Android Enterprise**

Le provisionnement de profils VPN via Android Enterprise est désormais pris en charge.

[CGOP-631]

Problèmes résolus

- Si vous enregistrez un jeton déjà enregistré et que vous essayez de l'ouvrir, des caractères brouillés apparaissent dans le nom du jeton.

[CGOP-11696]

- L'application Citrix SSO ne parvient pas à établir de session VPN si aucun domaine de recherche DNS n'est configuré sur NetScaler Gateway.

[CGOP-11259]

V2.3.6

Nouveautés

- **Prise en charge Always On pour Citrix SSO**

La fonctionnalité Always On de Citrix SSO garantit que les utilisateurs sont toujours connectés au réseau de l'entreprise. Cette connectivité VPN persistante est obtenue par l'établissement automatique d'un tunnel VPN.

[CGOP-10015]

- **Une notification de reconnexion s'affiche si l'expiration du jeton Athena provoque une déconnexion**

Une notification invitant les utilisateurs à se reconnecter à Citrix Workspace s'affiche si les conditions suivantes sont remplies.

- La fonctionnalité Always On est activée dans le profil VPN provisionné Citrix Workspace
- L'authentification Athena est utilisée pour l'authentification unique
- L'utilisateur est déconnecté de l'application Citrix Workspace en raison de l'expiration du jeton Athena

[CGOP-10016]

- **L'inscription au service de notification Push s'effectue à l'aide de NetScaler Gateway**

Vous pouvez désormais vous inscrire au service de notification push à l'aide de l'appliance NetScaler Gateway. Auparavant, l'enregistrement était effectué sur l'appareil client.

[CGOP-10542]

Problèmes résolus

Parfois, Citrix SSO se bloque lorsqu'un nouveau jeton est analysé. Par exemple, Citrix SSO se bloque lorsqu'un jeton existant est supprimé et qu'un autre est analysé avec le même nom de jeton.

[CGOP-10818]

V2.3.1

Nouveautés

- **Les configurations gérées sont mises à jour pour inclure davantage de paramètres utilisateur**

Les configurations gérées sont mises à jour pour inclure les paramètres « BlockUntrusted-Servers », « DefaultProfileName » et « DisableUserProfiles » pour les environnements Android Enterprise.

[CGOP-10033]

- **Prise en charge améliorée des notifications Push**

Lors de la configuration de NetScaler Gateway pour les notifications push de type « OTP », aucun code PIN/empreinte digitale n'est demandé une fois que l'utilisateur a sélectionné « Autoriser » en réponse à la notification push demandant le consentement de l'utilisateur pour autoriser la poursuite de l'authentification.

[CGOP-9843]

- **Prise en charge de Firebase Analytics**

La prise en charge de Firebase Analytics de base est ajoutée pour fournir des informations d'utilisation sur l'application Citrix SSO. L'amélioration s'applique aux géolocalisations grossières, à l'utilisation de l'écran, aux différentes versions d'Android utilisées, etc.

[CGOP-7523]

- **Prise en charge de la configuration de profil VPN basée sur les configurations gérées Android**

L'application Citrix SSO peut être configurée dans l'environnement Android Enterprise à l'aide d'un fournisseur EMM/UEM tel que Citrix Endpoint Management. L'assistant de configuration gérée Android Enterprise de CEM peut être utilisé pour déployer des configurations VPN gérées dans l'application Citrix SSO. Pour plus d'informations sur la configuration de l'application Citrix SSO à l'aide des configurations gérées, consultez la stratégie relative aux [appareils VPN](#).

V2.2.9

Nouveautés

- **Prise en charge des notifications push**

NetScaler Gateway envoie une notification push sur votre appareil mobile enregistré pour une expérience d'authentification à deux facteurs simplifiée.

[CGOP-9592]

Problèmes résolus

- Les caractères autres que les URL sont autorisés dans le champ Serveur de l'écran Ajouter une connexion.

[CGOP-588]

Configuration de Citrix Secure Access dans un environnement MDM

March 27, 2024

Important :

Citrix SSO pour Android s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur de manière à refléter ce changement de nom.

Pour configurer Citrix Secure Access dans un environnement MDM, consultez la section [Configurer le protocole Citrix Secure Access pour Android](#).

Remarques :

- Dans un environnement non MDM, les utilisateurs créent manuellement des profils VPN.
- Vous pouvez également créer une configuration gérée par Android Enterprise pour Citrix Secure Access. Pour plus d'informations, consultez la section [Configurer les profils VPN pour Android Enterprise](#).
- Pour les utilisateurs d'Android 13+ utilisant Citrix Secure Access 23.12.1 et versions ultérieures, il est conseillé aux administrateurs MDM d'accorder l'autorisation de notification à Citrix Secure Access (Package ID : `com.citrix.CitrixVPN`) dans leur solution.

Configuration de Citrix Secure Access dans un environnement Intune Android Enterprise

March 27, 2024

Important :

Citrix SSO pour Android s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur pour refléter ce changement de nom.

Cette rubrique fournit des informations sur le déploiement et la configuration de Citrix Secure Access via Microsoft Intune. Ce document suppose qu'Intune est déjà configuré pour la prise en charge d'Android Enterprise et que l'inscription des appareils est déjà terminée.

Pré-requis

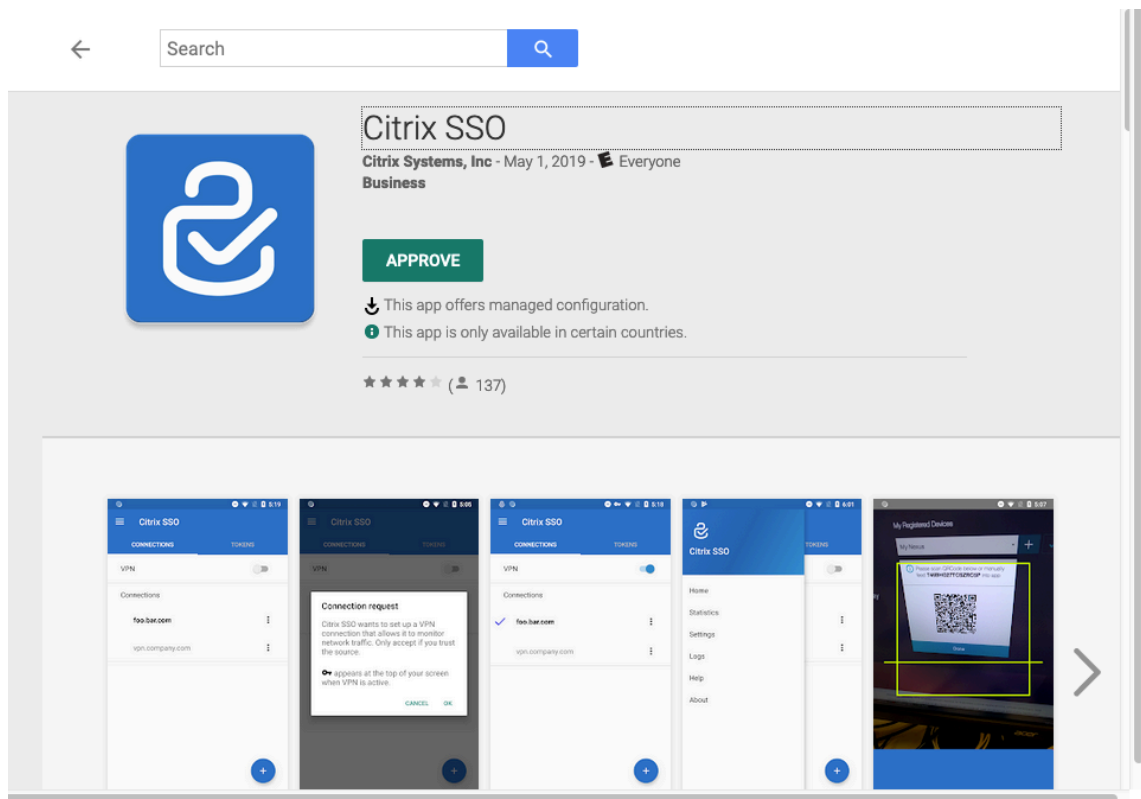
- Intune est configuré pour le support Android Enterprise
- L'inscription des appareils est terminée

Pour configurer Citrix Secure Access dans un environnement Intune Android Enterprise

- Ajouter Citrix Secure Access en tant qu'application gérée
- Configurer la stratégie des applications gérées pour Citrix Secure Access

Ajouter Citrix Secure Access en tant qu'application gérée

1. Connectez-vous à votre portail Azure.
2. Cliquez sur **Intune** dans le volet de navigation de gauche.
3. Cliquez sur **Applications clientes** dans la lame Microsoft Intune, puis cliquez sur Applications dans la lame Applications clientes.
4. Cliquez sur **Ajouter un lien** dans les options du menu en haut à droite. La lame Ajouter une configuration d'application apparaît.
5. Sélectionnez **Google Play géré** pour le type d'application.
Cela ajoute Gérer la recherche Google Play et approuver la lame si vous avez configuré Android Enterprise.
6. Recherchez Citrix Secure Access et sélectionnez-le dans la liste des applications.



Remarque : Si Citrix Secure Access n’apparaît pas dans la liste, cela signifie que l’application n’est pas disponible dans votre pays.

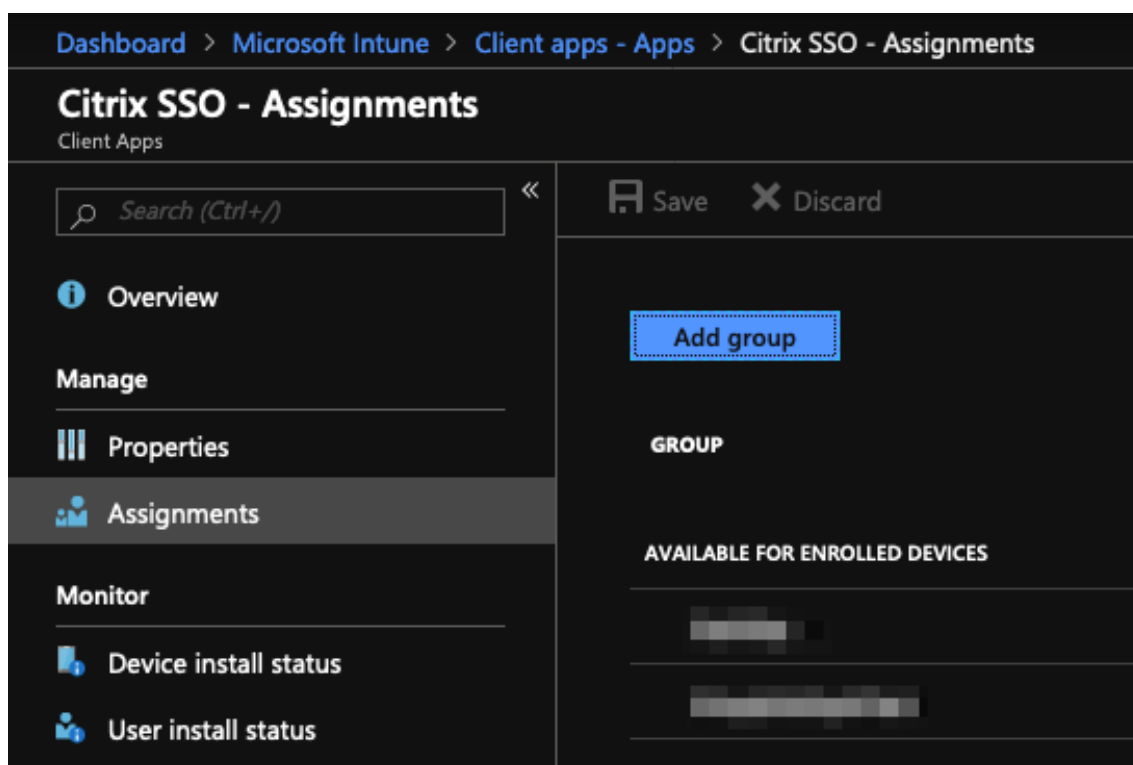
7. Cliquez sur **APPROUVER** pour approuver le déploiement de Citrix Secure Access via le Google Play Store géré.

Les autorisations requises par Citrix Secure Access sont répertoriées.

8. Cliquez sur **APPROUVER** pour approuver le déploiement de l’application.
9. Cliquez sur **Synchroniser** pour synchroniser cette sélection avec Intune.

Citrix Secure Access est ajouté à la liste des applications clientes. Vous devrez peut-être rechercher Citrix Secure Access si de nombreuses applications ont été ajoutées.

10. Cliquez sur l’application **Citrix Secure Access** pour ouvrir la fenêtre de détails de l’application.
11. Cliquez sur **Affectations** dans la lame de détails. **La lame Citrix Secure Access - Assignments** apparaît.



12. Cliquez sur **Ajouter un groupe** pour attribuer les groupes d'utilisateurs auxquels vous souhaitez autoriser l'installation de Citrix Secure Access, puis cliquez sur **Enregistrer**.
13. Fermez la fenêtre de détails de Citrix Secure Access.

Citrix Secure Access est ajouté et activé pour être déployé auprès de vos utilisateurs.

Configurer la stratégie des applications gérées pour Citrix Secure Access

Une fois Citrix Secure Access ajouté, vous devez créer une stratégie de configuration gérée pour Citrix Secure Access afin que le profil VPN puisse être déployé sur Citrix Secure Access sur l'appareil.

1. Ouvrez la lame **Intune** sur votre portail Azure.
2. Ouvrez la lame **Client Apps** à partir de la lame Intune.
3. Sélectionnez l'**élément Stratégies de configuration d'application** dans la lame Applications clientes et cliquez sur **Ajouter** pour ouvrir la lame **Ajouter une stratégie de configuration**.
4. Entrez le nom de la stratégie et ajoutez-en une description.
5. Dans **Type d'inscription des appareils**, sélectionnez **Appareils gérés**.
6. Dans **Platform**, sélectionnez **Android**.

Cela ajoute une autre option de configuration pour l'application associée.

7. Cliquez sur **Application associée** et sélectionnez l'application **Citrix Secure Access**.

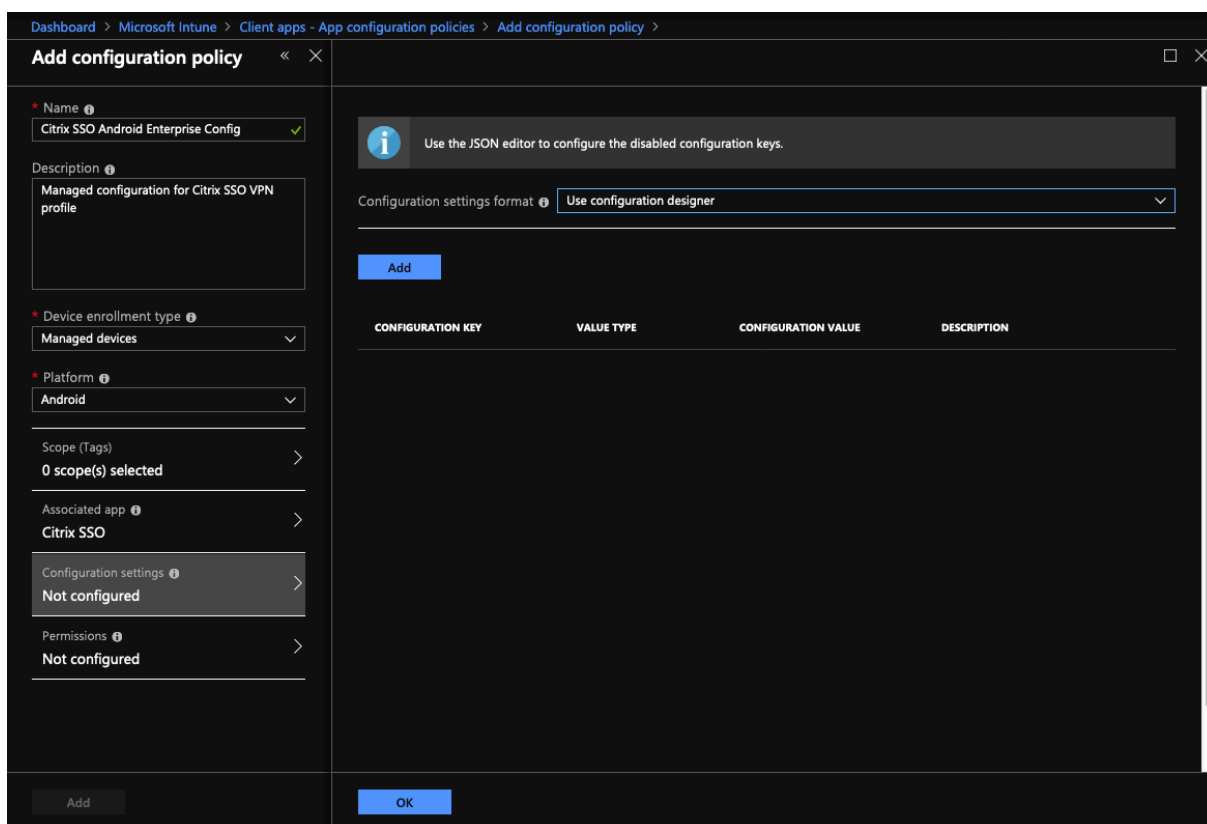
Vous devrez peut-être le rechercher si vous disposez de nombreuses applications.

8. Cliquez sur **OK**. Une option de paramètres de configuration est ajoutée dans la lame Ajouter une stratégie de configuration.

9. Cliquez sur Paramètres **de configuration**.

Une lame permettant de configurer Citrix Secure Access apparaît.

10. Dans Paramètres **de configuration**, sélectionnez **Utiliser le concepteur de configuration** ou **Entrez des données JSON** pour configurer Citrix Secure Access.



Remarque :

Pour les configurations VPN simples, il est recommandé d'utiliser le concepteur de configuration.

Configuration VPN à l'aide du concepteur de configuration

1. Dans **Paramètres de configuration**, sélectionnez **Utiliser le concepteur de configuration** et cliquez sur **Ajouter**.

Un écran de saisie des valeurs clés s'affiche pour configurer les différentes propriétés prises en charge par Citrix Secure Access. Au minimum, vous devez configurer les propriétés **Adresse du**

serveur et **Nom du profil VPN**. Vous pouvez survoler la section **DESCRIPTION** pour obtenir plus d'informations sur chaque propriété.

- Par exemple, sélectionnez les propriétés **Nom du profil VPN** et **Adresse du serveur (*)**, puis cliquez sur **OK**.

Les propriétés sont ajoutées au concepteur de configuration. Vous pouvez configurer les propriétés suivantes.

- **Nom du profil VPN**. saisissez un nom pour le profil VPN. Si vous créez plusieurs profils VPN, utilisez un nom unique pour chaque profil. Si vous ne fournissez pas de nom, l'adresse que vous entrez dans le champ Adresse du serveur est utilisée comme nom de profil VPN.
- **Adresse du serveur (*)**. Entrez le nom de domaine complet de base de NetScaler Gateway. Si votre port NetScaler Gateway n'est pas 443, saisissez également votre port. Utilisez le format URL. Par exemple, <https://vpn.mycompany.com:8443>.
- **Nom d'utilisateur (facultatif)**. Entrez le nom d'utilisateur que les utilisateurs finaux utilisent pour s'authentifier auprès de NetScaler Gateway. Vous pouvez utiliser le jeton de valeur de configuration Intune pour ce champ si la passerelle est configurée pour l'utiliser (voir jetons de valeur de configuration). Si vous ne fournissez pas de nom d'utilisateur, les utilisateurs sont invités à fournir un nom d'utilisateur lorsqu'ils se connectent à NetScaler Gateway.
- **Mot de passe (facultatif)**. Entrez le mot de passe que les utilisateurs finaux utilisent pour s'authentifier auprès de NetScaler Gateway. Si vous ne fournissez pas de mot de passe, les utilisateurs sont invités à fournir un mot de passe lorsqu'ils se connectent à NetScaler Gateway.
- **Alias de certificat (facultatif)**. Indiquez un alias de certificat dans le magasin de clés Android à utiliser pour l'authentification du certificat client. Ce certificat est présélectionné pour les utilisateurs si vous utilisez l'authentification basée sur des certificats.
- **Épingles de certificat Gateway (facultatif)**. Objet JSON décrivant les codes PIN de certificat utilisés pour NetScaler Gateway. Exemple de valeur : { "hash-alg": "sha256", "pinset": ["AA", "BB"] }. Pour plus de détails, consultez la section [Épinglage de certificats NetScaler Gateway avec Android Citrix Secure Access](#).
- **Type de VPN par application (facultatif)**. Si vous utilisez un VPN par application pour restreindre les applications qui utilisent ce VPN, vous pouvez configurer ce paramètre.
 - Si vous sélectionnez **Autoriser**, le trafic réseau pour les noms de packages d'applications répertoriés dans la liste des applications PerAppVPN est acheminé via le VPN. Le trafic réseau de toutes les autres applications est acheminé en dehors du VPN.

- Si vous sélectionnez **Interrompre**, le trafic réseau pour les noms de packages d'applications répertoriés dans la liste des applications PerAppVPN est acheminé en dehors du VPN. Le trafic réseau de toutes les autres applications est acheminé via le VPN. La valeur par défaut est Autoriser.
- **Liste des applications PerAppVPN.** liste des applications dont le trafic est autorisé ou interdit sur le VPN en fonction de la valeur définie pour Type de VPN par application. Répertoriez les noms de packages d'applications en les séparant par des virgules ou des points-virgules. Les noms de packages d'applications sont sensibles à la casse et doivent apparaître sur cette liste tels qu'ils figurent dans Google Play Store. Cette liste est facultative. Gardez cette liste vide pour le provisioning de VPN à l'échelle de l'appareil.
- **Profil VPN par défaut.** Le nom du profil VPN utilisé lorsque Always On VPN est configuré pour Citrix Secure Access. Si ce champ est vide, le profil principal est utilisé pour la connexion. Si un seul profil est configuré, il est marqué comme profil VPN par défaut.

i Use the JSON editor to configure the disabled configuration keys.

<input type="checkbox"/>	CONFIGURATION KEY	VALUE TYPE	DESCRIPTION
	Restrictions Version	hidden	
<input checked="" type="checkbox"/>	VPN Profile Name	string	Name of the VPN profile (if not ...
<input checked="" type="checkbox"/>	Server Address(*)	string	Url of the Citrix Gateway for the...
	Username (optional)	string	Username used for login to the ...
	Password (optional)	string	Password of the user for login t...
	Certificate Alias (optional)	string	Alias of the client certificate inst...
	Per-App VPN Type (optional)	choice	Are the listed apps allowed (whi...
	PerAppVPN app list	string	Comma (,) or semicolon (;) sepa...
	Default VPN profile	string	Name of VPN profile to use wh...
	Disable User Profiles	bool	Whether to allow users to manu...
<input checked="" type="checkbox"/>	Block Untrusted Servers	bool	Should the connection to untru...
	Custom Parameters	bundleArray	Custom Parameters (optional). ...
	List of additional VPN profiles	bundleArray	Additional VPN Profiles

OK

Remarque :

- Pour faire de Citrix Secure Access une application VPN Always On dans Intune, utilisez le fournisseur VPN de manière personnalisée et `com.citrix.CitrixVPN` comme nom du package de l'application.
- Seule l'authentification client basée sur des certificats est prise en charge pour le VPN Always On de Citrix Secure Access.
- Les administrateurs doivent sélectionner **l'authentification du client et définir le**

certificat client sur **Obligatoire** dans le **profilSSL ou dans les propriétés** SSL sur NetScaler Gateway pour Citrix Secure Access pour fonctionner comme prévu.

- **Désactiver les profils utilisateur**

- Si vous définissez cette valeur sur true, les utilisateurs ne peuvent pas ajouter de nouveaux profils VPN sur leurs appareils.
- Si vous définissez cette valeur sur false, les utilisateurs peuvent ajouter leur propre VPN sur leurs appareils.

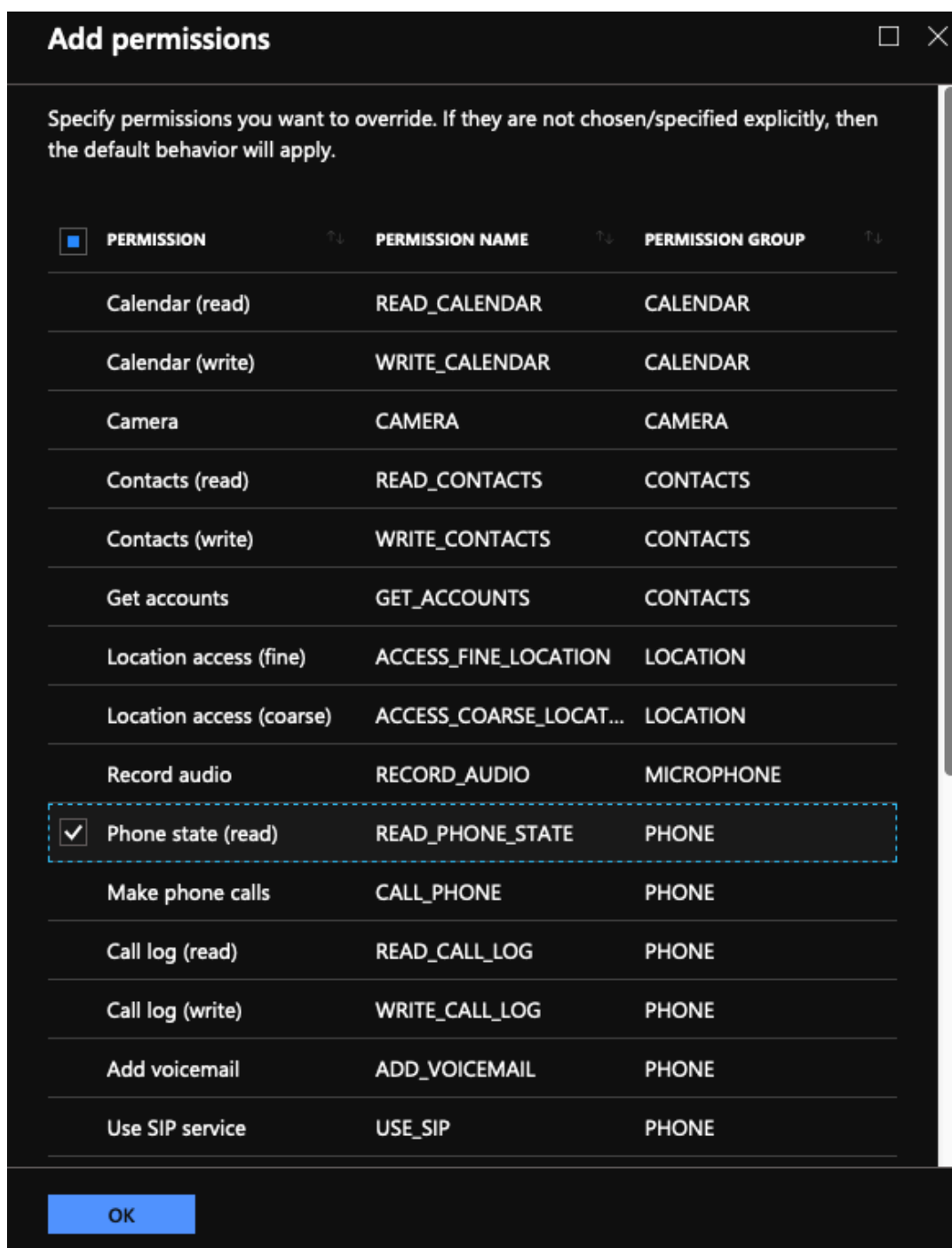
La valeur par défaut est false.

- **Bloquer les serveurs non fiables**

- Définissez cette valeur sur false lorsque vous utilisez un certificat autosigné pour NetScaler Gateway ou lorsque le certificat racine de l'autorité de certification qui émet le certificat NetScaler Gateway ne figure pas dans la liste des autorités de certification du système.
- Définissez cette valeur sur true pour permettre au système d'exploitation Android de valider le certificat NetScaler Gateway. Si la validation échoue, la connexion n'est pas autorisée.

La valeur par défaut est true.

3. Pour la propriété **Server Address (*)**, saisissez l'URL de base de votre passerelle VPN (par exemple, <https://vpn.mycompany.com>).
4. Dans le champ **Nom du profil VPN**, entrez un nom visible par l'utilisateur final sur l'écran principal du client Citrix Secure Access (par exemple, My Corporate VPN).
5. Vous pouvez ajouter et configurer d'autres propriétés en fonction de votre déploiement NetScaler Gateway. Cliquez sur **OK** lorsque vous avez terminé la configuration.
6. Cliquez sur la section **Autorisations**. Vous pouvez accorder les autorisations suivantes requises par Citrix Secure Access :
 - Si vous utilisez le check Intune NAC, Citrix Secure Access nécessite que vous accordiez l'autorisation d'**état (lecture) du téléphone**. Cliquez sur le bouton **Ajouter** pour ouvrir la lame d'autorisations. Actuellement, Intune affiche une liste importante des autorisations disponibles pour toutes les applications.
 - Si vous utilisez la vérification du NAC Intune, sélectionnez Autorisation **d'état du téléphone (lecture)** et cliquez sur **OK**. Cela l'ajoute à la liste des autorisations de l'application. Sélectionnez **Prompt** ou **Auto grant** pour que la vérification Intune NAC puisse fonctionner, puis cliquez sur **OK**.



- Il est conseillé d'accorder automatiquement des autorisations de notification à Citrix Secure Access.

Remarque :

Pour les utilisateurs d'Android 13+ utilisant Citrix Secure Access 23.12.1 et versions ultérieures, il est conseillé aux administrateurs MDM d'accorder l'autorisation de noti-

figuration à Citrix Secure Access (ID du package : `com.citrix.CitrixVPN`) dans leur solution.

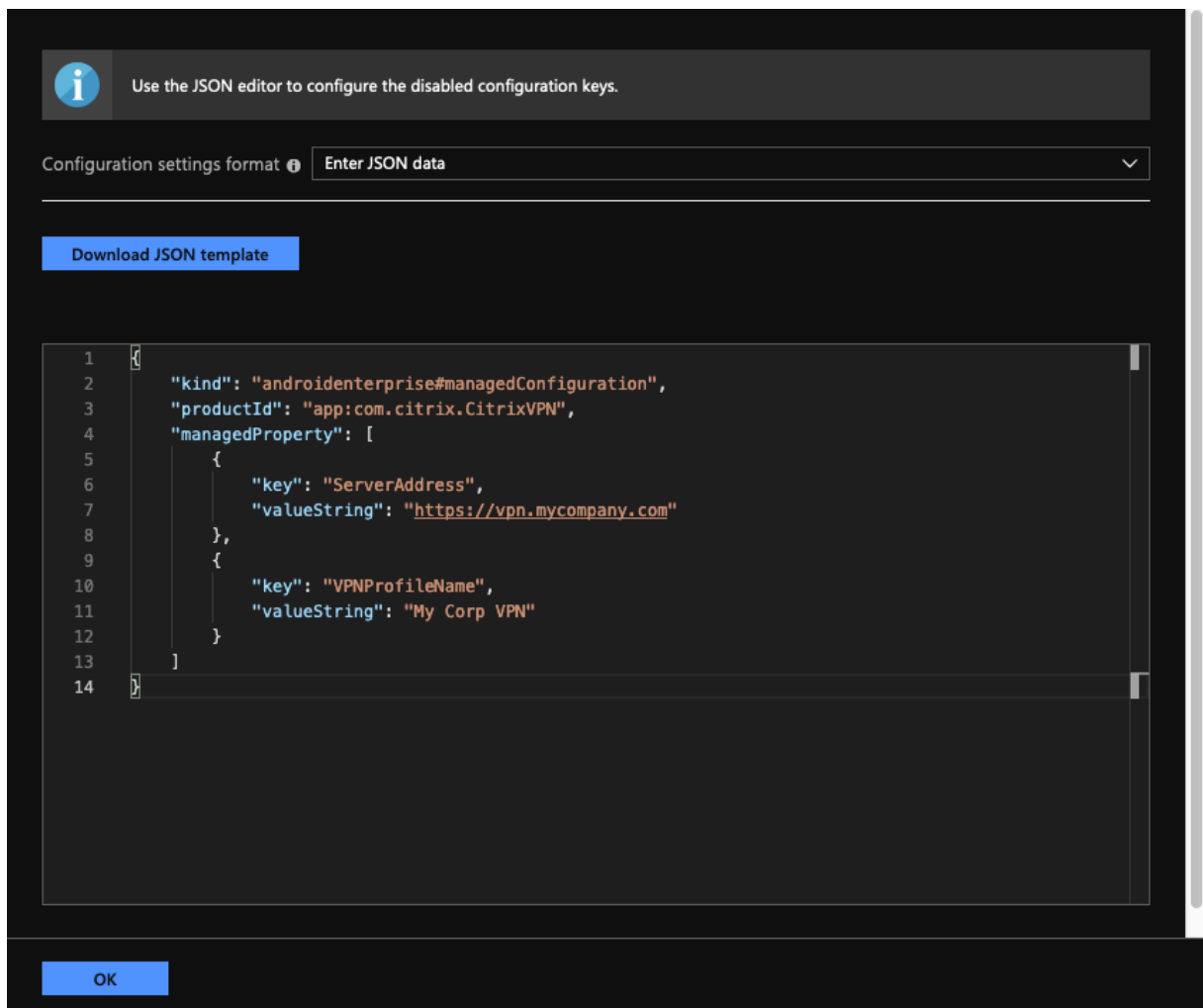
7. Cliquez sur **Ajouter** en bas du panneau de stratégie de configuration de l'application pour enregistrer la configuration gérée de Citrix Secure Access.
8. Cliquez sur **Attributions** dans la lame de stratégie de configuration des applications pour ouvrir la lame **Attributions**.
9. Sélectionnez les groupes d'utilisateurs pour lesquels vous souhaitez que cette configuration Citrix Secure Access soit fournie et appliquée.

Configuration VPN en entrant des données JSON

1. Dans Paramètres de **configuration**, sélectionnez **Entrer les données JSON** pour configurer Citrix Secure Access.
2. Cliquez sur le bouton Télécharger le modèle JSON pour télécharger un modèle permettant de fournir une configuration plus détaillée/complexes pour Citrix Secure Access. Ce modèle est un ensemble de paires clé-valeur JSON permettant de configurer toutes les propriétés possibles comprises par Citrix Secure Access.

Pour obtenir la liste de toutes les propriétés disponibles qui peuvent être configurées, consultez la section [Propriétés disponibles pour configurer le profil VPN dans l'application Citrix Secure Access](#).

3. Une fois que vous avez créé un fichier de configuration JSON, copiez et collez son contenu dans la zone d'édition. Par exemple, voici le modèle JSON pour la configuration de base créé précédemment à l'aide de l'option Concepteur de configuration.



Ceci termine la procédure de configuration et de déploiement de profils VPN pour Citrix Secure Access dans l'environnement Microsoft Intune Android Enterprise.

Important :

Le certificat utilisé pour l'authentification basée sur les certificats clients est déployé à l'aide d'un profil Intune SCEP. L'alias de ce certificat doit être configuré dans la propriété **Certificate Alias** de la configuration gérée pour Citrix Secure Access.

Propriétés disponibles pour configurer le profil VPN dans Citrix Secure Access

Clé de configuration	Nom du champ JSON	Type de valeur	Description
Nom du profil VPN	VPNProfileName	Texte	Nom du profil VPN (s'il n'est pas défini par défaut sur l'adresse du serveur).
Adresse du serveur (*)	ServerAddress	Adresse URL	URL de base de NetScaler Gateway pour la connexion (https://host[:port]). Il s'agit d'un champ obligatoire.
<code>Username</code> (facultatif)	Nom d'utilisateur	Texte	Nom d'utilisateur utilisé pour l'authentification auprès de NetScaler Gateway (facultatif).
Mot de passe (facultatif)	Mot de passe	Texte	Mot de passe de l'utilisateur pour s'authentifier auprès de NetScaler Gateway (facultatif).
Alias de certificat (facultatif)	ClientCertAlias	Texte	Alias du certificat client installé dans la banque d'informations d'identification Android à utiliser dans le cadre de l'authentification client basée sur les certificats (facultatif). L'alias de certificat est un champ obligatoire lors de l'utilisation de l'authentification basée sur des certificats sur NetScaler Gateway.

Clé de configuration	Nom du champ JSON	Type de valeur	Description
Épingles de certificat Gateway (facultatif)	ServerCertificatePins	Texte JSON	Objet JSON intégré décrivant les codes PIN de certificat utilisés pour NetScaler Gateway. Exemple de valeur: { "hash- alg": "sha256", "pinset": [" AAAAAAAAAAAAAAAAAAAAAAAAAAAAA =", " BBBBBBBBBBBBBBBBBBBBBBBBBBB ="] }. Assurez-vous d'échapper à ces données JSON intégrées lorsque vous utilisez le configurateur JSON.

Clé de configuration	Nom du champ JSON	Type de valeur	Description
Type de Per App VPN (facultatif)	PerAppVPN_Allow_Disallow	Enum (Allow, Disallow)	Les applications répertoriées sont-elles autorisées (liste d'autorisation) ou interdites (liste de blocage) à utiliser le tunnel VPN ? Si cette option est définie sur Autoriser , seules les applications répertoriées (dans la propriété Liste des applications PerAppVPN) sont autorisées à passer par tunnel via le VPN. Si cette option est définie sur Refuser , toutes les applications, à l'exception de celles répertoriées, sont autorisées à passer par tunnel via le VPN. Si aucune application n'est répertoriée, toutes les applications sont autorisées à passer par le VPN.

Clé de configuration	Nom du champ JSON	Type de valeur	Description
PerAppVPN app list	PerAppName_Appnames	Texte	Liste de noms de packages d'applications séparés par des virgules (,) ou des points-virgules (;) pour le Per App VPN. Les noms des packages doivent être identiques à ceux qui apparaissent sur l'URL de la page de liste des applications du Google Play Store. Les noms des packages distinguent les majuscules des minuscules.
Profil VPN par défaut	DefaultProfileName	Texte	Nom du profil VPN à utiliser lorsque le système démarre le service VPN. Ce paramètre est utilisé pour identifier le profil VPN à utiliser lorsque le VPN Always On est configuré sur l'appareil.
Désactiver les profils utilisateur	DisableUserProfiles	Booléen	Propriété permettant ou non aux utilisateurs finaux de créer manuellement des profils VPN. Définissez cette valeur sur true pour empêcher les utilisateurs de créer des profils VPN. La valeur par défaut est False .

Clé de configuration	Nom du champ JSON	Type de valeur	Description
Bloquer les serveurs non fiables	BlockUntrustedServers	Booléen	Propriété permettant de déterminer si la connexion à des passerelles non fiables (par exemple, à l'aide de certificats auto-signés ou lors de l'émission d'une autorité de certification n'est pas approuvée par le système d'exploitation Android) doit être bloquée ? La valeur par défaut est true (bloque les connexions à des passerelles non fiables).
Paramètres personnalisés (facultatif)	CustomParameters	Liste	Liste des paramètres personnalisés (facultatif) pris en charge par Citrix Secure Access. Pour plus de détails, voir Paramètres personnalisés . Consultez la documentation du produit NetScaler Gateway pour connaître les options disponibles.

Clé de configuration	Nom du champ JSON	Type de valeur	Description
Liste des autres profils VPN	bundle_profiles	Liste	Liste des autres profils VPN. La plupart des valeurs mentionnées précédemment pour chaque profil sont prises en charge. Pour plus de détails, consultez la section Propriétés prises en charge pour chaque VPN dans la liste des profils VPN .

Paramètres personnalisés Chaque paramètre personnalisé doit être défini à l'aide des noms de valeurs-clés suivants.

Clé	Type de valeur	Valeur
Nom du paramètre	Texte	Nom du paramètre personnalisé.
Valeur du paramètre	Texte	Valeur du paramètre personnalisé.

Paramètres personnalisés pour la configuration d'Intune

Nom du paramètre	Description	Valeur
UserAgent	Citrix Secure Access ajoute cette valeur de paramètre à l'en-tête HTTP de l'agent utilisateur, lors de la communication avec NetScaler Gateway, pour effectuer une vérification supplémentaire sur NetScaler Gateway.	Spécifiez le texte que vous devez ajouter à l'en-tête HTTP de l'agent utilisateur. Le texte doit être conforme aux spécifications de l'agent utilisateur HTTP.

Nom du paramètre	Description	Valeur
EnableDebugLogging	Activez la journalisation du débogage sur Citrix Secure Access pour résoudre les problèmes de connectivité VPN en cas d'Always On VPN. Vous pouvez l'activer dans toutes les configurations VPN gérées. La journalisation du débogage prend effet lorsque les configurations gérées sont traitées.	True : active la journalisation du débogage. Valeur par défaut : False .

Pour plus d'informations sur les paramètres personnalisés, voir [Créer une configuration gérée par Android Enterprise pour Citrix Secure Access](#).

Propriétés prises en charge pour chaque VPN dans la liste des profils VPN Les propriétés suivantes sont prises en charge pour chacun des profils VPN lors de la configuration de plusieurs profils VPN à l'aide du modèle JSON.

Clé de configuration	Nom du champ JSON	Type de valeur
Nom du profil VPN	bundle_VPNProfileName	Texte
Adresse du serveur (*)	bundle_ServerAddress	Adresse URL
Nom d'utilisateur	bundle_Username	Texte
Mot de passe	Bundle_Password	Texte
Alias de certificat client	bundle_ClientCertAlias	Texte
Épinglages de certificat Gateway	bundle_ServerCertificatePins	Texte
Type de VPN par application	bundle_PerAppVPN_Allow_Disallow	Enum (Allow, Disallow)
PerAppVPN app list	Bundle_PerAppVPN_AppNames	Texte
Paramètres personnalisés	bundle_CustomParameters	Liste

Définir Citrix Secure Access comme fournisseur VPN Always On dans Intune

En l'absence d'un support VPN à la demande dans un sous-système VPN Android, le VPN Always On peut être utilisé comme alternative pour fournir une option de connectivité VPN fluide ainsi qu'une authentification par certificat client avec Citrix Secure Access. Le VPN est démarré par le système d'exploitation lorsqu'il démarre ou lorsque le profil professionnel est activé.

Pour faire de Citrix Secure Access une application VPN Always On dans Intune, vous devez utiliser les paramètres suivants.

- Choisissez le type de configuration gérée à utiliser (propriété personnelle avec profil de travail OU profil de travail entièrement géré, dédié et appartenant à l'entreprise).
- Créez un profil de configuration d'appareil et sélectionnez **Restrictions d'appareil**, puis accédez à la section **Connectivité**. Sélectionnez Activer pour le paramètre VPN Always On.
- Choisissez **Citrix Secure Access** comme client VPN. Si Citrix Secure Access n'est pas disponible en tant qu'option, vous pouvez choisir **Personnaliser** en tant que client VPN et saisir **com.citrix.citrixvpn** dans le champ Package ID (le champ Package ID distingue les majuscules et minuscules)
- Laissez les autres options telles qu'elles sont. Il est recommandé de ne pas activer le mode Verrouillage. Lorsque cette option est activée, l'appareil risque de perdre la connectivité réseau complète si le VPN n'est pas disponible.
- En plus de ces paramètres, vous pouvez également définir le **type de VPN par application** et la **liste des applications PerAppVPN** dans la page **Stratégies de configuration** de l'application pour activer le VPN par application pour Android, comme décrit dans les sections précédentes.

Remarque :

Le VPN Always On est uniquement pris en charge avec l'authentification par certificat client dans Citrix Secure Access.

Références

Pour plus d'informations sur la configuration des options de connectivité dans Intune, reportez-vous aux rubriques suivantes.

- [Appareils d'entreprise dédiés entièrement gérés](#)
- [Appareils personnels](#)

Redémarrage automatique du VPN Always On

À partir de Citrix SSO pour Android 23.8.1, Citrix Secure Access redémarre automatiquement le VPN Always On lorsqu'une application faisant partie de la liste d'autorisation ou de blocage est installée dans un profil professionnel ou un profil d'appareil. Le trafic provenant de l'application récemment installée est automatiquement tunnelisé via une connexion VPN sans redémarrer le profil professionnel ni redémarrer l'appareil.

Pour activer le redémarrage automatique du VPN Always On, les utilisateurs finaux doivent autoriser Citrix Secure Access à [tous les packages Query](#). Une fois le consentement accordé, Citrix Secure Access :

- Reçoit la notification d'installation du package en provenance du système d'exploitation.
- Redémarre le VPN Always On.

Lorsqu'un utilisateur final se connecte à un profil VPN par application pour la première fois, il est invité à donner son consentement (requis par les règles de Google) pour collecter des informations sur le package installé. Si l'utilisateur final donne son consentement, la connexion VPN est initiée. Si l'utilisateur refuse son consentement, la connexion VPN est interrompue. L'écran d'autorisation ne réapparaît pas une fois que l'autorisation a été accordée. Pour plus d'informations sur les instructions destinées à l'utilisateur final, consultez la section [Comment utiliser Citrix Secure Access depuis votre appareil Android](#).

Limitations

Les limitations suivantes s'appliquent au Per App VPN dans l'environnement Android Enterprise sur les appareils Android 11+ en raison des [restrictions de visibilité des packages](#) introduites dans Android 11 :

- Si une application figurant dans la liste des applications autorisées/refusées est déployée sur un appareil après le démarrage de la session VPN, l'utilisateur final doit redémarrer la session VPN pour que l'application puisse acheminer son trafic via la session VPN.
- Si le VPN par application est utilisé via une session VPN Always On, après avoir installé une nouvelle application sur l'appareil, l'utilisateur final doit redémarrer le profil professionnel ou redémarrer l'appareil pour que le trafic de l'application soit routé via la session VPN.

Remarque :

Ces limitations ne s'appliquent pas si vous utilisez Citrix SSO pour Android 23.8.1 ou des versions ultérieures. Consultez [Redémarrage automatique d'Always On VPN](#) pour plus de détails.

Épinglage de certificats NetScaler Gateway avec Citrix Secure Access pour Android

March 27, 2024

Important :

Citrix SSO pour Android s'appelle désormais Citrix Secure Access. Nous mettons à jour notre documentation et les captures d'écran de l'interface utilisateur pour refléter ce changement de nom.

L'épinglage de certificats aide à prévenir les attaques de type « man-in-the-middle ». Citrix Secure Access prend en charge l'épinglage de certificats uniquement pour les configurations VPN gérées en mode Android Enterprise et en mode administrateur d'appareils existants. Il n'est pas pris en charge pour les profils VPN ajoutés par l'utilisateur final.

Configurer l'épinglage de certificats NetScaler Gateway avec Android Citrix Secure Access

Pour plus d'informations sur l'épinglage des certificats dans la configuration gérée (anciennement restrictions des applications) pour Citrix Secure Access, consultez la section [Certificats et authentification](#).

Une nouvelle paire clé-valeur est définie pour contenir les hachages du certificat NetScaler Gateway épinglé comme suit.

```
1 Key: ServerCertificatePins
2 Value: {
3
4   "hash-alg": "sha256",
5   "pinset": [
6     "cert1_base64_encoded_SHA-256_hash_of_the_X509_SubjectPublicKeyInfo
7     (SPKI)",
8     "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
9     "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB=",
10    ...
11  ]
12 }
13 <!--NeedCopy-->
```

La clé permettant de spécifier les détails d'épinglage de certificat dans la configuration gérée est **ServerCertificatePins**. La valeur est une charge utile JSON contenant les hachages SHA-256 codés en base64 du certificat NetScaler Gateway épinglé et de l'algorithme de hachage utilisé. Le certificat

Épinglé peut être n'importe lequel des certificats de la chaîne de confiance validés par le système d'exploitation. Dans ce cas, il s'agit d'Android.

L'épinglage du certificat est effectué uniquement après que le système d'exploitation a validé la chaîne de certificats lors de la prise de liaison TLS. Le code PIN du certificat est calculé en hachant les informations de clé publique d'objet du certificat (SPKI). Les deux champs (« **hash-alg** » et « **pinset** ») doivent être spécifiés dans la charge utile JSON.

Le « **hash-alg** » spécifie l'algorithme de hachage utilisé pour calculer le hachage SPKI.

Le « **pinset** » indique le tableau JSON contenant le hachage SHA-256 codé en base64 des données SPKI du certificat NetScaler Gateway.

Au moins une valeur doit être spécifiée pour le code PIN du certificat. D'autres valeurs de broche peuvent être spécifiées pour permettre la rotation ou l'expiration du certificat.

Vous pouvez calculer la valeur du code PIN d'un domaine (par exemple, gw.votredomain.com) à l'aide de la commande openssl suivante.

```
1 openssl s_client -servername gw.yourdomain.com -connect gw.yourdomain.com:443 | openssl x509 -pubkey -noout | openssl pkey -pubin -outform der | openssl dgst -sha256 -binary | openssl enc -base64
2 <!--NeedCopy-->
```

La commande affiche le hachage SHA-256 codé en base64 du certificat feuille présenté par une passerelle. N'importe quel certificat de la chaîne peut être utilisé pour l'épinglage de certificats. Par exemple, si une entreprise utilise sa propre autorité de certification intermédiaire pour générer des certificats pour plusieurs passerelles, le code PIN correspondant au certificat de signature intermédiaire peut être utilisé. Si aucune des broches ne correspond aux certificats de la chaîne de certificats validée, l'établissement de liaison TLS est interrompu et la connexion à la passerelle ne se poursuit pas.

Remarque :

En mode administrateur de périphérique, l'épinglage de certificat est pris en charge uniquement avec les solutions Citrix Endpoint Management et Microsoft Endpoint Management. L'épinglage de certificat doit être configuré dans les paramètres personnalisés utilisés dans le profil VPN hérité (configuration non gérée) avec le paramètre personnalisé ServerCertificatePins avec la même charge utile JSON pour l'épinglage.

Notes de mise à jour de Citrix Secure Access pour Windows

March 27, 2024

Le client Citrix Secure Access pour Windows est désormais disponible de manière autonome et est compatible avec toutes les versions de NetScaler. La version du client Citrix Secure Access suit le format YY.MM Release.Build.

Les notes de version décrivent les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes et les problèmes résolus.

Nouveautés : Les nouvelles fonctionnalités et améliorations disponibles dans la version actuelle.

Problèmes résolus : problèmes résolus dans la version actuelle.

Pour obtenir des informations détaillées sur les fonctionnalités prises en charge, consultez la documentation du [produit NetScaler Gateway](#).

Remarque :

- Le client Citrix Secure Access pour Windows versions 23.7.1.1 et ultérieures contient le correctif pour <https://support.citrix.com/article/CTX564833>.
- Le client Citrix Secure Access (anciennement connu sous le nom de plug-in NetScaler Gateway pour Windows) versions 21.9.1.2 et ultérieures contient le correctif pour <https://support.citrix.com/article/CTX341455>.

24.2.1.15 (4 mars 2024)

Nouveautés

- **Support pour SNI**

Dans un déploiement Citrix Secure Private Access, le client Citrix Secure Access prend désormais en charge l'extension d'indication du nom de serveur (SNI) sur toutes les demandes de pré-authentification.

[SPAHELP-236]

- **Support pour TLS 1.3**

Le client Citrix Secure Access prend désormais en charge le protocole TLS 1.3. Le protocole TLS 1.3 est pris en charge sur les plateformes suivantes :

- Windows 11 et versions ultérieures
- Windows Server 2022 et versions ultérieures

Pour plus de détails sur la configuration de TLS 1.3 sur NetScaler, [consultez la section Support](#) du protocole TLS 1.3.

[CSACLIENTS-6106]

- **Prise en charge des détails du système d'exploitation Windows dans l'en-tête HTTP**

Le client Citrix Secure Access inclut désormais les détails du système d'exploitation Windows dans la chaîne d'en-tête HTTP (agent utilisateur).

[NSHELP-36732]

Problèmes résolus

La résolution DNS échoue par intermittence si IPv6 est activé sur l'adaptateur réseau client.

[NSHELP-35708]

Les utilisateurs peuvent ne pas être en mesure de se connecter au client Citrix Secure Access en cas de tentatives de connexion simultanées à l'aide de la connexion automatique.

[NSHELP-35768]

L'installation de Citrix Secure Access échoue lorsque Smart App Control est activé sur des ordinateurs clients non anglophones.

[NSHELP-36126], [NSHELP-36907]

Les utilisateurs ne peuvent pas accéder à certaines applications via un VPN si le client Citrix Secure Access est configuré avec le pilote WFP. Ce problème se produit en raison de modifications apportées aux politiques de pare-feu.

[NSHELP-36254], [NSHELP-36312]

Une boîte de dialogue contextuelle apparaît lors d'un scan EPA. Cependant, lorsque l'utilisateur clique sur OK, le scan EPA fonctionne comme d'habitude. Ce problème se produit lorsque la langue suédoise est sélectionnée (**Configuration > Langue**) sur l'interface utilisateur du client Citrix Secure Access.

[NSHELP-36408]

En mode VPN Always On, le tunnel au niveau de la machine ne parvient pas à transférer la session lorsque l'authentification par certificat utilisateur est configurée sur NetScaler Gateway.

[NSHELP-36492]

L'accès aux ressources de l'intranet échoue par intermittence lorsque le pilote Windows Filtering Platform (WFP) est activé sur le client Citrix Secure Access.

[NSHELP-36568]

La page de l'interface utilisateur du client Citrix Secure Access se bloque par intermittence lorsque les utilisateurs cliquent sur le bouton Accueil.

[NSHELP-37046]

Les utilisateurs non administrateurs ne peuvent pas se connecter au tunnel VPN complet si les conditions suivantes sont remplies :

- L'EPA est configuré en tant que facteur dans un flux nFactor.
- Edge WebView est activé.
- Le paramètre de mise à niveau des contrôles du client Citrix EPA est défini sur **Always** on NetScaler Gateway et il existe une incohérence dans les versions du client Citrix EPA entre l'appareil client et NetScaler.

[NSHELP-37340]

L'analyse des certificats de périphérique EPA échoue si le magasin de certificats système de la machine cliente ne contient qu'un seul certificat de périphérique.

[NSHELP-37371]

La page de connexion du client Citrix Secure Access devient vide par intermittence lors de la connexion au service Citrix Secure Private Access.

[SPAHELP-202]

Les utilisateurs finaux peuvent ne pas être en mesure de connecter les machines clientes au domaine via un VPN si Windows Server 2019 ou une version ultérieure est utilisé.

[SPAHELP-219]

Lorsque le service Citrix Device Posture est activé, les entrées indésirables apparaissent dans la liste déroulante **Connection** de l'interface utilisateur du client Citrix Secure Access.

[SPAHELP-271]

Les utilisateurs finaux ne peuvent pas accéder aux ressources de l'intranet si la fonctionnalité d'authentification unique est activée sur le client Citrix Secure Access.

[CSACLIENTS-9940]

23.10.1.7 (29 novembre 2023)

Nouveautés

- **Configurer la plage de ports privés pour les connexions initiées par le serveur**

Vous pouvez désormais configurer un port privé compris entre 49152 et 64535 pour les connexions initiées par le serveur. La configuration des ports privés permet d'éviter les conflits qui peuvent survenir lorsque vous utilisez des ports pour créer des sockets entre le client Citrix Secure Access et des applications tierces sur les machines clientes. Vous pouvez configurer les

ports privés à l'aide du registre VPN Windows « SicBeginPort ». Vous pouvez également configurer la plage de ports privés à l'aide d'un fichier JSON de personnalisation du plug-in VPN sur NetScaler.

Pour plus d'informations, consultez la section [Configurer les connexions initiées par le serveur](#) et les [clés de registre du client VPN Windows NetScaler Gateway](#).

[NSHELP-36627]

- **Prise en charge de l'authentification Kerberos pour une connexion automatique fluide**

Le client Citrix Secure Access utilise désormais la méthode d'authentification Kerberos pour la connexion automatique. Dans le cadre de cette prise en charge, une clé de registre client VPN « EnableKerberosAuth » est introduite. Comme condition préalable, les administrateurs doivent configurer l'authentification Kerberos sur NetScaler et sur leurs machines clientes. Les utilisateurs finaux doivent installer Microsoft Edge WebView sur leurs machines pour activer la méthode d'authentification Kerberos. Pour plus d'informations, voir [Autologon avec authentification Kerberos](#).

[CSACLIENTS-3128]

- **Attribution automatique d'une plage d'adresses IP frauduleuses**

Le client Citrix Secure Access peut désormais détecter et appliquer une nouvelle plage d'adresses IP frauduleuses en cas de conflit entre la plage d'adresses IP usurpées configurée par l'administrateur et les applications basées sur IP ou le réseau de l'utilisateur final.

[CSACLIENTS-6132]

- **Notifications Microsoft**

Les notifications du client Citrix Secure Access apparaissent désormais sous forme de notifications Microsoft dans le panneau Notifications de votre machine Windows.

[CSACLIENTS-6136]

- **Collecte de journaux améliorée**

Le niveau de journalisation Verbose est désormais utilisé comme niveau de journalisation de débogage par défaut afin d'améliorer la collecte des journaux et la résolution des problèmes. Pour plus d'informations sur la journalisation, voir [Configurer la journalisation à l'aide de l'interface utilisateur du client](#).

[CSACLIENTS-8151]

Problèmes résolus

Le client Citrix Secure Access reste dans l'état « Connexion » si le tunnel machine du service Always On ne détecte pas l'emplacement de la machine cliente.

[CSACLIENTS-1174]

La fonctionnalité d'ouverture de session par transfert ne fonctionne pas lorsque Microsoft Edge Web-View est activé dans le client Citrix Secure Access.

[CSACLIENTS-6655]

En mode de service Always On, le client Citrix Secure Access ne parvient pas à établir de tunnel au niveau de la machine avec NetScaler Gateway si les stratégies d'authentification classiques basées sur les certificats de l'appareil sont liées à un serveur virtuel VPN.

[NSHELP-33766]

Les appels Webex entrants et sortants échouent lorsque les utilisateurs sont connectés au VPN. Ce problème se produit lorsque le pilote de la plateforme de filtrage Windows (WFP) est activé sur le client Citrix Secure Access au lieu du pilote DNE (Deterministic Network Enhancer).

[NSHELP-34651]

Le client Citrix Secure Access se bloque si les conditions suivantes sont remplies :

- Les connexions sont permutées lorsque les stratégies SAML sont liées à un serveur virtuel VPN.
- La prise en charge d'Internet Explorer WebView est activée.

[NSHELP-35366]

L'interface utilisateur du client Citrix Secure Access affiche le bouton Connect lors de la connexion automatique. Ce problème se produit si la méthode d'authentification UserCert est utilisée pour se connecter au VPN.

[NSHELP-36134]

La fonctionnalité d'accès au réseau local ne fonctionne pas avec le client Citrix Secure Access si un tunnel au niveau de la machine est configuré.

Dans cette version, la fonctionnalité d'accès au réseau local peut être définie avec une configuration de tunnel au niveau de la machine. Pour ce faire, vous devez configurer le paramètre d'accès au réseau local sur FORCED lorsque vous utilisez le mode tunnel de la machine. Pour plus de détails, voir [Appliquer l'accès au réseau local aux utilisateurs finaux en fonction de la configuration ADC](#).

[NSHELP-36214]

Lorsqu'un ordinateur client sort du mode veille plusieurs fois, le client Citrix Secure Access ne parvient pas à établir de connexion VPN avec les applications intranet.

[NSHELP-36221]

23.8.1.11 (19 octobre 2023)

Problèmes résolus

Le téléchargement du fichier epaPackage.exe peut échouer si la prise en charge du proxy de transfert est configurée sur NetScaler Gateway.

[CSACLIENTS-6917]

L'installation du client Citrix EPA échoue pour les utilisateurs non administrateurs ayant un accès restreint au lecteur C.

[NSHELP-36590]

23.8.1.5 (09 août 2023)

Problèmes résolus

L'authentification unique Kerberos échoue pour les applications lorsqu'elles sont connectées via le service Citrix Secure Private Access.

[CSACLIENTS-912]

L'accès aux applications avec le service Citrix Secure Private Access échoue par intermittence. Ce problème se produit lorsque le client Citrix Secure Access partage une adresse IP de destination incorrecte pour le trafic TCP ou UDP.

[CSACLIENTS-1151, CSACLIENTS-6326]

Le client Citrix Secure Access ne parvient pas à lancer les applications par intermittence en raison d'un problème de mise en cache DNS.

[CSACLIENTS-1170]

Le client Citrix Secure Access ne parvient pas à appliquer de suffixe DNS à Citrix Virtual Adapter. Ce problème se produit lorsque Citrix Virtual Adapter ne parvient pas à s'authentifier auprès d'Active Directory.

[NSHELP-33817]

Le client Citrix Secure Access se bloque si les conditions suivantes sont remplies :

- Le serveur virtuel NetScaler Gateway contient un certificat client comme facteur d'authentification nFactor.
- La prise en charge de Microsoft Edge WebView est activée.

[CSACLIENTS-6171]

Lorsque vous êtes connecté au VPN, il se peut que vous ne puissiez pas accéder aux ressources principales après avoir appliqué Microsoft KB5028166.

[NSHELP-35909]

Le client Citrix Secure Access ne parvient pas par intermittence à télécharger les configurations depuis NetScaler Gateway lorsque la personnalisation du portail dépasse la limite autorisée.

[NSHELP-35971]

Problèmes connus

La fonctionnalité d'ouverture de session par transfert ne fonctionne pas avec le client Citrix Secure Access. Ce problème se produit lorsque Microsoft Edge WebView est activé.

Solution : ouvrez une session à l'aide d'un navigateur Web pour transférer la session.

23.7.1.1 (14 juillet 2023)

Problèmes résolus

Dans certains cas, après une mise à niveau vers la version 23.x.x.x, le trafic ne passe pas par le tunnel VPN, ce qui bloque l'accès au VPN lorsqu'une plage d'adresses IP Intranet est configurée sur NetScaler. Cela se produit lorsque la règle de pare-feu multiprofil n'est pas appliquée aux applications VPN.

[NSHELP-35766]

23.5.1.3 (2 juin 2023)

Problèmes résolus

Le service Always On se bloque lorsque la collecte de journaux améliorée est activée à l'aide du registre « UseNewLogger » ci-dessous. `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client`

[CGOP-24462]

23.4.1.5 (14 avril-2023)

Nouveautés

- **Compatibilité avec Microsoft Edge WebView**

La prise en charge de Microsoft Edge WebView sur le client Citrix Secure Access pour Windows améliore l'expérience de l'utilisateur final. Cette fonctionnalité est désactivée par défaut. Pour plus de détails, consultez la section [Support de Microsoft Edge WebView pour Windows Citrix Secure Access](#).

[CGOP-22245]

- **Ajout de suffixes DNS pour résoudre les FQDN en adresses IP**

Les administrateurs peuvent désormais ajouter des suffixes aux applications au niveau du système d'exploitation. Cela permet aux clients Citrix Secure Access de résoudre un nom de domaine non entièrement qualifié lors de la résolution du nom.

Les administrateurs peuvent également configurer les applications à l'aide des adresses IP (CIDR/plage IP) afin que les utilisateurs finaux puissent accéder aux applications à l'aide des FQDN correspondants. Pour plus de détails, voir [Suffixes DNS pour résoudre les FQDN en adresses IP](#).

[ACS-2490]

- **Collecte de journaux améliorée**

La fonctionnalité de journalisation du client Windows Secure Access est désormais améliorée pour la collecte des journaux et le débogage. Les modifications suivantes sont apportées à la fonction de journalisation.

- Permettez aux utilisateurs de modifier la taille maximale du fichier journal à une valeur inférieure à 600 Mo.
- Permettez aux utilisateurs de mettre à jour le nombre de fichiers journaux à moins de 5.
- Augmentez les niveaux de journalisation à trois pour la nouvelle fonctionnalité de journalisation.

Grâce à ces modifications, les administrateurs et les utilisateurs finaux peuvent collecter les journaux de la session en cours et des sessions précédentes. Auparavant, la collecte des journaux était limitée aux sessions en cours uniquement. Pour plus de détails, consultez la section [Amélioration de la collecte des journaux pour le client Windows](#).

Remarque :

Pour activer la journalisation du débogage, sélectionnez **Journalisation > Verbose** dans la liste déroulante **Sélectionner le niveau de journalisation**. Avant la version 23.4.1.5 du client Citrix Secure Access pour Windows, la journalisation du débogage pouvait être activée à l'aide de la case à cocher **Configuration > Activer la journalisation du débogage**.

[CGOP-23537]

- **Prise en charge de l'envoi d'événements au service Citrix Analytics**

Le client Citrix Secure Access pour Windows prend désormais en charge l'envoi d'événements tels que la création de session, la fermeture de session et la connexion d'applications au service Citrix Analytics. Ces événements sont ensuite enregistrés dans le tableau de bord Citrix Secure Private Access.

[SPA-2197]

Problèmes résolus

- L'authentification unique du client Citrix Secure Access avec l'application Citrix Workspace vers le point de terminaison cloud échoue pour les utilisateurs Unicode.

[CGOP-22334]

- L'accès aux ressources échoue lorsque des applications basées sur le nom d'hôte sont configurées avec le suffixe DNS dans Citrix Secure Private Access.

[SPA-4430]

- La connexion VPN permanente échoue par intermittence au démarrage en raison d'un problème d'accessibilité du serveur virtuel de passerelle.

[NSHELP-33500]

- Les ressources de l'intranet qui se chevauchent avec une plage d'adresses IP usurpée ne sont pas accessibles lorsque le tunnel partagé est défini sur OFF sur le client Citrix Secure Access.

[NSHELP-34334]

- Le client Citrix Secure Access ne parvient pas à charger le schéma d'authentification, ce qui entraîne un échec de connexion au service Citrix Secure Private Access.

[SPAHELP-98]

23.1.1.11 (20-févr. 2023)

Cette version résout les problèmes qui contribuent à améliorer les performances globales et la stabilité du service Citrix Secure Private Access.

23.1.1.8 (8 février 2023)

Problèmes résolus

- Les échecs de résolution DNS se produisent lorsque Citrix Secure Access ne donne pas la priorité aux paquets IPv4 par rapport aux paquets IPv6.

[NSHELP-33617]

- Les règles de filtrage du système d'exploitation sont capturées lorsque le client Citrix Secure Access s'exécute en mode Windows Filtering Platform (WFP).

[NSHELP-33715]

- Une adresse IP usurpée est utilisée pour les applications intranet IP lorsque le client Citrix Secure Access s'exécute en mode Citrix Deterministic Network Enhancer (DNE).

[NSHELP-33722]

- Lorsque vous utilisez le pilote Windows Filtering Platform (WFP), l'accès à l'intranet ne fonctionne parfois pas une fois le VPN reconnecté.

[NSHELP-32978]

- L'analyse des terminaux (EPA) pour vérifier la version du système d'exploitation échoue sur les postes de travail multi-sessions Windows 10 et Windows 11 Enterprise.

[NSHELP-33534]

- Le client Windows prend en charge la taille du fichier de configuration de 64 Ko, par défaut, ce qui limite la possibilité pour les utilisateurs d'ajouter des entrées supplémentaires dans le fichier de configuration. Cette taille peut être augmentée en définissant la valeur de `ConfigSize` registre dans `HKEY_LOCAL_MACHINE \ SOFTWARE \ Citrix \ Secure Access Client`. Le type de clé de registre `ConfigSize` est `REG_DWORD` et les données clés sont `<Bytes size>`. Si la taille du fichier de configuration est supérieure à la valeur par défaut (64 Ko), la valeur de registre `ConfigSize` doit être définie sur $5 \times 64 \text{ Ko}$ (après conversion en octets) pour chaque ajout de 64 Ko. Par exemple, si vous ajoutez 64 Ko supplémentaires, vous devez définir la valeur du registre sur $64 \times 1024 \times 5 = 327680$. De même, si vous ajoutez 128 Ko, vous devez définir la valeur de registre sur $64 \times 1024 \times (5+5) = 655360$.

[SPA-2865]

- Lors de la fermeture de session VPN, les entrées de la liste de suffixes DNS dans le registre `Search-List` sont réécrites dans l'ordre inverse, séparées par une ou plusieurs virgules.

[NSHELP-33671]

- L'authentification par proxy échoue lorsque l'appliance NetScaler effectue une analyse EPA pour détecter la présence d'un antivirus.

[NSHELP-30876]

- Si les valeurs de registre associées à Citrix Secure Access sont supérieures à 1 500 caractères, le collecteur de journaux ne parvient pas à recueillir les journaux d'erreurs.

[NSHELP-33457]

22.10.1.9 (08-nov.-2022)

Nouveautés

- **Support de l'EPA pour la persistance du site de type proxy de connexion dans GSLB**

Le scan EPA de Windows prend désormais en charge la persistance du site de type proxy de connexion dans GSLB lorsque le scan est lancé depuis un navigateur. Auparavant, le scan EPA pour Windows ne prenait pas en charge le type de persistance du proxy de connexion pour le scan EPA lancé par le navigateur.

[CGOP-21545]

- **Authentification unique fluide pour l'URL Workspace (Cloud uniquement)**

Le client Citrix Secure Access prend désormais en charge l'authentification unique pour l'URL de Workspace (cloud uniquement) si l'utilisateur s'est déjà connecté via l'application Citrix Workspace. Pour plus de détails, consultez la section [Single sign-on support for the Workspace URL for users logged in via Citrix Workspace app](#).

[ACS-2427]

- **Gérer le client Citrix Secure Access et/ou la version du plug-in EPA via l'application Citrix Workspace (cloud uniquement)**

L'application Citrix Workspace peut désormais télécharger et installer la dernière version de Citrix Secure Access et/ou du plug-in EPA via le Global App Configuration Service. Pour plus de détails, consultez [Global App Configuration Service](#).

[ACS-2426]

- **Amélioration du contrôle de la journalisation de débogage**

Le contrôle de journalisation des débogues pour le client Citrix Secure Access est désormais indépendant de NetScaler Gateway et peut être activé ou désactivé depuis l'interface utilisateur du plug-in pour la machine et le tunnel utilisateur.

[NSHELP-31968]

- **Prise en charge des demandes de vérification préliminaire de Private Network Access**

Le client Citrix Secure Access pour Windows prend désormais en charge les demandes de vérification préliminaire de Private Network Access émises par le navigateur Chrome lors de l'accès aux ressources du réseau privé à partir de sites Web publics.

[CGOP-20544]

Problèmes résolus

- Le client Citrix Secure Access, version 21.7.1.1 et versions ultérieures, ne parvient pas à effectuer la mise à niveau vers des versions ultérieures pour les utilisateurs ne disposant pas de droits d'administration.

Cela s'applique uniquement si la mise à niveau du client Citrix Secure Access est effectuée à partir d'une appliance NetScaler. Pour plus de détails, consultez la section [Problème de mise à niveau ou de rétrogradation sur le client Citrix Secure Access](#).

[NSHELP-32793]

- Les utilisateurs ne peuvent pas se connecter au VPN en raison de défaillances intermittentes de l'EPA.

[NSHELP-32138]

- Parfois, le client Citrix Secure Access en mode tunnel machine uniquement n'établit pas automatiquement le tunnel machine une fois que la machine sort du mode veille.

[NSHELP-30110]

- En mode service Always on, le tunnel utilisateur essaie de démarrer même si seul le tunnel machine est configuré.

[NSHELP-31467]

- Le lien de la page d'accueil sur l'interface utilisateur de Citrix Secure Access ne fonctionne pas si Microsoft Edge est le navigateur par défaut.

[NSHELP-31894]

- Le message personnalisé du journal des défaillances de l'EPA ne s'affiche pas sur le portail NetScaler Gateway, mais le message « erreur interne » s'affiche.

[NSHELP-31434]

- Lorsque les utilisateurs cliquent sur l'onglet Page d'accueil de l'écran Citrix Secure Access pour Windows, la page affiche l'erreur de refus de connexion.

[NSHELP-32510]

- Sur certaines machines clientes, le client Citrix Secure Access ne parvient pas à détecter le paramètre proxy, ce qui entraîne un échec de connexion.

[SPAHELP-73]

Problèmes connus

- Le scan EPA basé sur des contrôles Windows Update ne fonctionne pas sur la version Windows 11 22H2. Pour plus de détails, voir [Echec du contrôle EPA pour Windows11 22H2](#).

[NSHELP-33068]

22.6.1.5 (17 juin-2022)

Nouveautés

- **Configuration des scripts de connexion et de déconnexion**

Le client Citrix Secure Access accède à la configuration du script de connexion et de déconnexion à partir des registres suivants lorsque le client Citrix Secure Access se connecte au service cloud Citrix Secure Private Access.

Chemin d'accès au registre : **HKEY_LOCAL_MACHINE>SOFTWARE > Citrix > Secure Access Client**

Valeurs du registre :

- SecureAccessLogInScript type REG_SZ - chemin d'accès au script de connexion
- SecureAccessLogOutScript type REG_SZ - chemin d'accès au script de déconnexion

[ACS-2776]

- **Client Windows Citrix Secure Access utilisant la plate-forme de filtrage Windows (WFP)**

WFP est un ensemble d'API et de services système qui fournit une plate-forme pour créer une application de filtrage de réseau. WFP est conçu pour remplacer les technologies de filtrage de paquets précédentes, le filtre NDIS (Network Driver Interface Specification) qui était utilisé avec le pilote DNE. Pour plus de détails, consultez la section [Client Windows Citrix Secure Access utilisant la plate-forme de filtrage Windows](#).

[CGOP-19787]

- **Prise en charge du split tunnel inversé basé sur le nom**

Le pilote WFP prend désormais en charge le split tunneling REVERSE basé sur le nom de domaine complet. Il n'est pas pris en charge par le pilote DNE. Pour plus de détails sur le split tunnel inversé, voir [Options de split tunneling](#).

[CGOP-16849]

Problèmes résolus

- Parfois, l'ouverture de session automatique Windows ne fonctionne pas lorsqu'un utilisateur se connecte à la machine Windows en mode de service Always On. Le tunnel machine ne passe pas au tunnel utilisateur et le message **Connexion** s'affiche dans l'interface utilisateur du plug-in VPN.

[NSHELP-31357]

- Lors de la fermeture de session VPN, les entrées de la liste de suffixes DNS dans le registre Search-List (Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client) sont réécrites dans l'ordre inverse, séparées par une ou plusieurs virgules.

[NSHELP-31346]

- L'adresse IP falsifiée est utilisée même après que la configuration de l'application intranet NetScaler est passée d'une application basée sur un FQDN à une application basée sur IP.

[NSHELP-31236]

- La page d'accueil de la passerelle ne s'affiche pas immédiatement après que le plug-in de passerelle a réussi à établir le tunnel VPN.

Avec ce correctif, la valeur de Registre suivante est introduite.

\HKLM\Software\Citrix\Secure Access Client\SecureChannelResetTimeoutSeconds

Type : DWORD

Par défaut, cette valeur de registre n'est ni définie ni ajoutée. Lorsque la valeur de « SecureChannelResetTimeoutSeconds » est 0 ou n'est pas ajoutée, le correctif pour gérer le délai ne fonctionne pas, ce qui est le comportement par défaut. L'administrateur doit définir ce registre sur le client pour activer le correctif (c'est-à-dire afficher la page d'accueil immédiatement après que le plug-in de passerelle ait établi le tunnel VPN avec succès).

[NSHELP-30189]

- Le registre de liste AlwaysOnAllow ne fonctionne pas comme prévu si la valeur du registre est supérieure à 2000 octets.

[NSHELP-31836]

- Le client Citrix Secure Access pour Windows ne crée pas de tunnel pour les nouvelles connexions TCP vers le serveur TCP principal si la région du service Citrix Secure Private Access déjà connectée devient inaccessible. Toutefois, cela n'affecte pas les connexions de passerelle sur site.

[ACS-2714]

22.3.1.5 (24-mars-2022)

Problèmes résolus

- Le nom du plug-in Windows EPA est rebaptisé Plug-in NetScaler Gateway EPA.

[CGOP-21061]

Problèmes connus

- Le client Citrix Secure Access pour Windows ne crée pas de tunnel pour les nouvelles connexions TCP vers le serveur TCP principal si la région du service Citrix Secure Private Access déjà connectée devient inaccessible. Toutefois, cela n'affecte pas les connexions de passerelle sur site.

[ACS-2714]

22.3.1.4 (10-mars-2022)

Nouveautés

- **Appliquer l'accès au réseau local aux utilisateurs finaux en fonction de la configuration ADC**

Les administrateurs peuvent empêcher les utilisateurs finaux de désactiver l'option d'accès au réseau local sur leurs machines clientes. Une nouvelle option, FORCED, est ajoutée aux valeurs des paramètres d'accès au réseau local existants. Lorsque la valeur Accès au réseau local est définie sur FORCED, l'accès au réseau local est toujours activé pour les utilisateurs finaux sur les machines clientes. Les utilisateurs finaux ne peuvent pas désactiver les paramètres du réseau local à l'aide de l'interface utilisateur du client Citrix Secure Access. Si les administrateurs souhaitent proposer une option permettant d'activer ou de désactiver l'accès au réseau local à l'utilisateur final, ils doivent reconfigurer le paramètre d'accès au réseau local sur ON.

Pour activer l'option **FORCED** à l'aide de l'interface graphique :

1. Accédez à **NetScaler Gateway > Paramètres globaux > Modifier les paramètres globaux**.
2. Cliquez sur l'onglet **Expérience client**, puis sur **Paramètres avancés**.
3. Dans **Accès au réseau local**, sélectionnez **FORCÉ**.

Pour activer l'option **FORCED** à l'aide de l'interface de ligne de commande, exécutez la commande suivante :

```
1 set vpn parameter -localLanAccess FORCED
2 <!--NeedCopy-->
```

[CGOP-19935]

- **Prise en charge de Windows Server 2019 et 2022 dans l'analyse du système d'exploitation EPA**

L'analyse du système d'exploitation EPA prend désormais en charge Windows Server 2019 et 2022.

Vous pouvez sélectionner les nouveaux serveurs à l'aide de l'interface graphique.

1. Accédez à **NetScaler Gateway > Stratégies > Préauthentification**.
2. Créez une nouvelle stratégie de préauthentification ou modifiez une stratégie existante.
3. Cliquez sur le lien **OPSWAT EPA Editor**.
4. Dans **Expression Editor**, sélectionnez **Windows > Windows Update** et cliquez sur l'icône **+**.
5. Dans **Nom du système d'exploitation**, sélectionnez le serveur selon vos besoins.

Vous pouvez mettre à niveau vers la version OPSWAT 4.3.2744.0 pour utiliser les serveurs Windows 2019 et 2022 dans l'analyse du système d'exploitation EPA.

[CGOP-20061]

- **Nouveaux types de classification d'analyse EPA pour les correctifs de sécurité manquants**

Les nouveaux types de classification suivants sont ajoutés à l'analyse EPA pour détecter les correctifs de sécurité manquants. L'analyse EPA échoue si l'un des correctifs de sécurité suivants est manquant sur le client.

- Application
- Connecteurs
- CriticalUpdates
- DefinitionUpdates
- DeveloperKits
- FeaturePacks
- Conseils
- SecurityUpdates
- ServicePacks
- Outils
- UpdateRollups
- Mises à jour

Vous pouvez configurer les types de classification à l'aide de l'interface graphique.

1. Accédez à **NetScaler Gateway > Stratégies > Préauthentification**.
2. Créez une nouvelle stratégie de préauthentification ou modifiez une stratégie existante.
3. Cliquez sur le lien ((OPSWAT EPA Editor)).
4. Dans Expression Editor, sélectionnez **Windows > Windows Update**.
5. Dans **Ne devrait pas avoir de correctif manquant du type de classification Windows Update suivant**, sélectionnez le type de classification pour les correctifs de sécurité manquants
6. Cliquez sur **OK**.

Vous pouvez effectuer une mise à niveau vers la version 4.3.2744.0 d'OPSWAT pour utiliser ces options.

- Pour plus d'informations sur les GUID de classification des services de mise à jour Windows Server, voir [https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803\(v=vs.85\)](https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85))
- Pour obtenir une description de la terminologie relative aux mises à jour logicielles Microsoft, voir <https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates>

Auparavant, les analyses EPA pour détecter les correctifs de sécurité manquants étaient effectuées sur les niveaux de gravité : Critique, Important, Modéré et Faible sur le client Windows.

[CGOP-19465]

- **Prise en charge de plusieurs certificats d'appareils pour l'analyse EPA**

Dans la configuration VPN Always on, si plusieurs certificats d'appareil sont configurés, le certificat dont la date d'expiration est la plus longue est essayé pour la connexion VPN. Si ce certificat autorise l'analyse EPA avec succès, la connexion VPN est établie. Si ce certificat échoue au cours du processus d'analyse, le certificat suivant est utilisé. Ce processus se poursuit jusqu'à ce que tous les certificats soient essayés.

Auparavant, si plusieurs certificats valides étaient configurés, si l'analyse EPA échouait pour un certificat, l'analyse n'avait pas été tentée sur les autres certificats.

[CGOP-19782]

Problèmes résolus

- Si le paramètre ClientCert est défini sur « Facultatif » dans le profil SSL lors de la configuration du serveur virtuel VPN, les utilisateurs sont invités à plusieurs reprises à sélectionner la carte à puce.

[NSHELP-30070]

- Les utilisateurs ne peuvent pas se connecter à l'appliance NetScaler Gateway après avoir modifié le paramètre de profil « networkAccessOnVPNFailure » de « fullAccess » à « onlyToGateway ».

[NSHELP-30236]

- Lorsque Always on est configuré, le tunnel utilisateur échoue en raison du numéro de version incorrect (1.1.1.1) dans le fichier aoservice.exe.

[NSHELP-30662]

- La résolution DNS des ressources internes et externes cesse de fonctionner pendant une session VPN prolongée.

[NSHELP-30458]

- Le client VPN Windows n'honore pas l'alerte « Notification de fermeture SSL » du serveur et envoie la demande de connexion de transfert sur la même connexion.

[NSHELP-29675]

- Vérification EPA du registre pour les « == » et « != » échoue pour certaines entrées de registre.

[NSHELP-29582]

22.2.1.103 (17-févr-2022)

Problèmes résolus

- Les utilisateurs ne peuvent pas lancer le plug-in EPA ou le plug-in VPN après une mise à niveau vers les versions de navigateur Chrome 98 ou Edge 98. Pour résoudre ce problème, effectuez les opérations suivantes :

1. Pour la mise à niveau du plug-in VPN, les utilisateurs finaux doivent se connecter à l'aide du client VPN pour la première fois afin d'obtenir le correctif sur leurs machines. Lors des tentatives de connexion suivantes, les utilisateurs peuvent choisir le navigateur ou le plug-in à connecter.
2. Pour le cas d'utilisation EPA uniquement, les utilisateurs finaux n'auront pas le client VPN pour se connecter à la passerelle. Dans ce cas, effectuez les opérations suivantes :
 - a) Connectez-vous à la passerelle à l'aide d'un navigateur.
 - b) Attendez que la page de téléchargement apparaisse et téléchargez le fichier nsepa_setup.exe.
 - c) Après le téléchargement, fermez le navigateur et installez le fichier nsepa_setup.exe.
 - d) Redémarrez le client.

[NSHELP-30641]

21.12.1.4 (17-déc-2021)

Nouveautés

- **Changements liés au rebranding**

Le plug-in NetScaler Gateway pour Windows est renommé client Citrix Secure Access.

[ACS-2044]

- **Prise en charge des applications privées TCP/HTTP (S)**

Le client Citrix Secure Access prend désormais en charge les applications privées TCP/HTTP (S) pour les utilisateurs distants via le service Citrix Workspace Secure Access.

[ACS-870]

- **Nouvelles langues prises en charge**

Les plug-ins VPN et EPA pour Windows pour NetScaler Gateway prennent désormais en charge les langues suivantes :

- Coréen
- Russe
- Chinois (traditionnel)

[CGOP-17721]

- **Prise en charge de Citrix Secure Access pour Windows 11**

Le client Citrix Secure Access est désormais pris en charge pour Windows 11.

[CGOP-18923]

- **Ouverture de session de transfert automatique lorsque l'utilisateur se connecte à partir de la même machine et que Always on est configuré**

Le transfert automatique de connexion se produit désormais sans aucune intervention de l'utilisateur lorsque Always on est configuré et que l'utilisateur se connecte à partir du même ordinateur. Auparavant, lorsque le client (utilisateur) devait se reconnecter dans des scénarios tels que le redémarrage du système ou des problèmes de connectivité réseau, un message contextuel apparaissait. L'utilisateur devait confirmer la connexion au transfert. Avec cette amélioration, la fenêtre contextuelle est désactivée.

[CGOP-14616]

- **Dérivation de l'adresse IP de la passerelle par défaut de Citrix Virtual Adapter à partir du masque réseau fourni par NetScaler**

L'adresse IP de la passerelle par défaut de Citrix Virtual Adapter est désormais dérivée du masque réseau fourni par NetScaler.

[CGOP-18487]

Problèmes résolus

- Parfois, les utilisateurs perdent l'accès à Internet après l'établissement d'un tunnel VPN en mode split tunnel ON. L'itinéraire par défaut erroné de l'adaptateur virtuel Citrix est à l'origine de ce problème réseau.

[NSHELP-26779]

- Lorsque Split Tunnel est réglé sur « Inverse », la résolution DNS pour les domaines intranet échoue.

[NSHELP-29371]

21.9.100.1 (30-déc-2021)

Nouveautés

- **Prise en charge de Citrix Secure Access pour Windows 11**

Le client Citrix Secure Access est désormais pris en charge pour Windows 11.

[CGOP-18923]

Problèmes résolus

- Parfois, les utilisateurs perdent l'accès à Internet après l'établissement d'un tunnel VPN en mode split tunnel ON. L'itinéraire par défaut erroné de l'adaptateur virtuel Citrix est à l'origine de ce problème réseau.

[NSHELP-26779]

- Lorsque Split Tunnel est réglé sur « Inverse », la résolution DNS pour les domaines intranet échoue.

[NSHELP-29371]

21.9.1.2 (04-oct-2021)

Problèmes résolus

- Parfois, après la déconnexion du VPN, le résolveur DNS ne parvient pas à résoudre les noms d'hôtes, car les suffixes DNS sont supprimés lors de la déconnexion du VPN.

[NSHELP-28848]

- Parfois, un utilisateur est déconnecté de NetScaler Gateway en quelques secondes lorsque le délai d'inactivité du client est défini.

[NSHELP-28404]

- Le plug-in Windows peut se bloquer pendant l'authentification.

[NSHELP-28394]

- En mode de service Always On, le plug-in VPN pour Windows ne parvient pas à établir automatiquement le tunnel utilisateur une fois que les utilisateurs se connectent à leurs machines Windows.

[NSHELP-27944]

- Après l'établissement du tunnel, au lieu d'ajouter des routes de serveur DNS avec l'adresse IP de la passerelle précédente, le plug-in Windows ajoute les routes avec l'adresse de passerelle par défaut.

[NSHELP-27850]

V21.7.1.1 (27-Aug-2021)

Nouveautés

- **Analyse des nouvelles adresses MAC**

La prise en charge des analyses d'adresses MAC plus récentes est ajoutée.

[CGOP-16842]

- **Analyse EPA pour vérifier le système d'exploitation Windows et sa version de compilation**

Ajout de l'analyse EPA pour vérifier le système d'exploitation Windows et sa version de compilation.

[CGOP-15770]

- **Analyse EPA pour vérifier l'existence d'une valeur particulière**

Une nouvelle méthode de l'analyse EPA du registre vérifie désormais l'existence d'une valeur particulière.

[CGOP-10123]

Problèmes résolus

- Si une erreur JavaScript se produit lors de la connexion en raison d'une erreur réseau, les tentatives de connexion suivantes échouent avec la même erreur JavaScript.

[NSHELP-27912]

- L'analyse EPA échoue pour la dernière vérification de l'heure de la dernière mise à jour de l'antivirus McAfee.

[NSHELP-26973]

- Parfois, les utilisateurs perdent leur accès à Internet après l'établissement d'un tunnel VPN.
[NSHELP-26779]
- Une erreur de script pour le plug-in VPN peut s'afficher pendant l'authentification nFactor.
[NSHELP-26775]
- En cas de perturbation du réseau, le flux de trafic UDP qui a démarré avant l'interruption du réseau ne s'interrompt pas avant 5 minutes maximum.
[NSHELP-26577]
- Vous risquez de subir un retard dans le démarrage du tunnel VPN si l'enregistrement DNS prend plus de temps que prévu.
[NSHELP-26066]

V21.3.1.2 (31-Mar-2021)

Nouveautés

- **Bibliothèques EPA mises à niveau**

Les bibliothèques EPA sont mises à niveau pour prendre en charge la dernière version des applications logicielles utilisées dans les analyses EPA.

[NSHELP-26274]

- **Compatibilité de l'adaptateur virtuel NetScaler Gateway**

L'adaptateur virtuel NetScaler Gateway est désormais compatible avec les adaptateurs virtuels directs Hyper-V et Microsoft Wi-Fi (utilisés avec les imprimantes).

[NSHELP-26366]

Problèmes résolus

- Le plug-in de passerelle VPN Windows bloque l'utilisation de « CTRL+P » et « CTRL+O » sur le tunnel VPN.
[NSHELP-26602]
- Le plug-in NetScaler Gateway pour Windows répond uniquement avec une adresse IP intranet enregistrée dans Active Directory lorsqu'une "nslookup" action est demandée pour le nom de la machine.
[NSHELP-26563]

- L'enregistrement et le désenregistrement IIP échouent par intermittence si le split DNS est défini sur « Local » ou « Des deux côtés ».

[NSHELP-26483]

- La connexion automatique au plug-in de passerelle VPN Windows échoue si Always On est configuré.

[NSHELP-26297]

- Le plug-in de passerelle VPN Windows ne parvient pas à supprimer les paquets DNS IPv6, ce qui entraîne des problèmes de résolution DNS.

[NSHELP-25684]

- Le plug-in de passerelle VPN Windows conserve la liste d'exceptions de proxy existante même si la liste déborde en raison de la limite du navigateur sur la liste des exceptions du proxy Internet Explorer.

[NSHELP-25578]

- Le plug-in de passerelle VPN Windows ne parvient pas à restaurer les paramètres du proxy lorsque le client VPN est déconnecté en mode Always On.

[NSHELP-25537]

- Le plug-in VPN pour Windows n'établit pas le tunnel après la connexion à Windows, si les conditions suivantes sont remplies :

- L'appliance NetScaler Gateway est configurée pour la fonctionnalité Always On.
- L'appliance est configurée pour l'authentification par certificat avec l'authentification à deux facteurs « désactivée ».

[NSHELP-23584]

Support de Microsoft Edge WebView pour Windows Citrix Secure Access - Aperçu

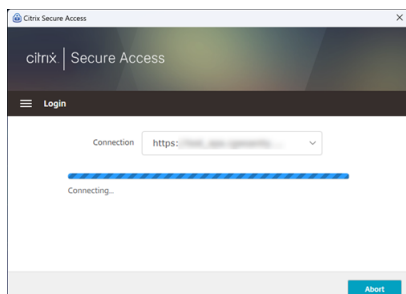
March 27, 2024

Microsoft Edge WebView est désormais le WebView recommandé par Microsoft car Internet Explorer WebView est obsolète. Nous vous recommandons d'utiliser le client Citrix Secure Access 23.8.1.5 ou une version ultérieure pour tirer parti des fonctionnalités de Microsoft Edge WebView.

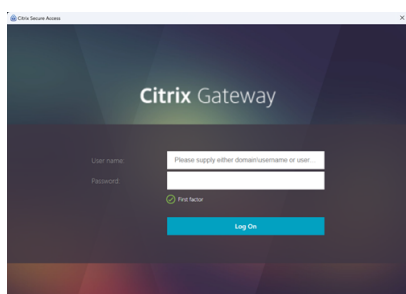
Microsoft Edge WebView est actuellement désactivé par défaut. Vous pouvez vous inscrire à l'aperçu en utilisant <https://podio.com/webforms/28291989/2245437>.

Changements concernant l'utilisateur final

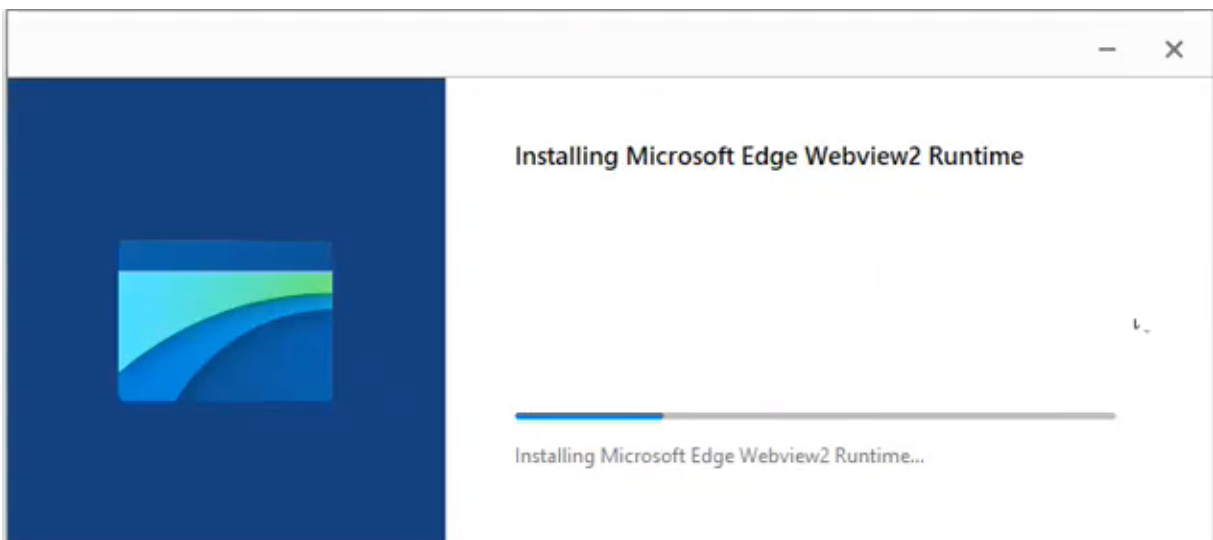
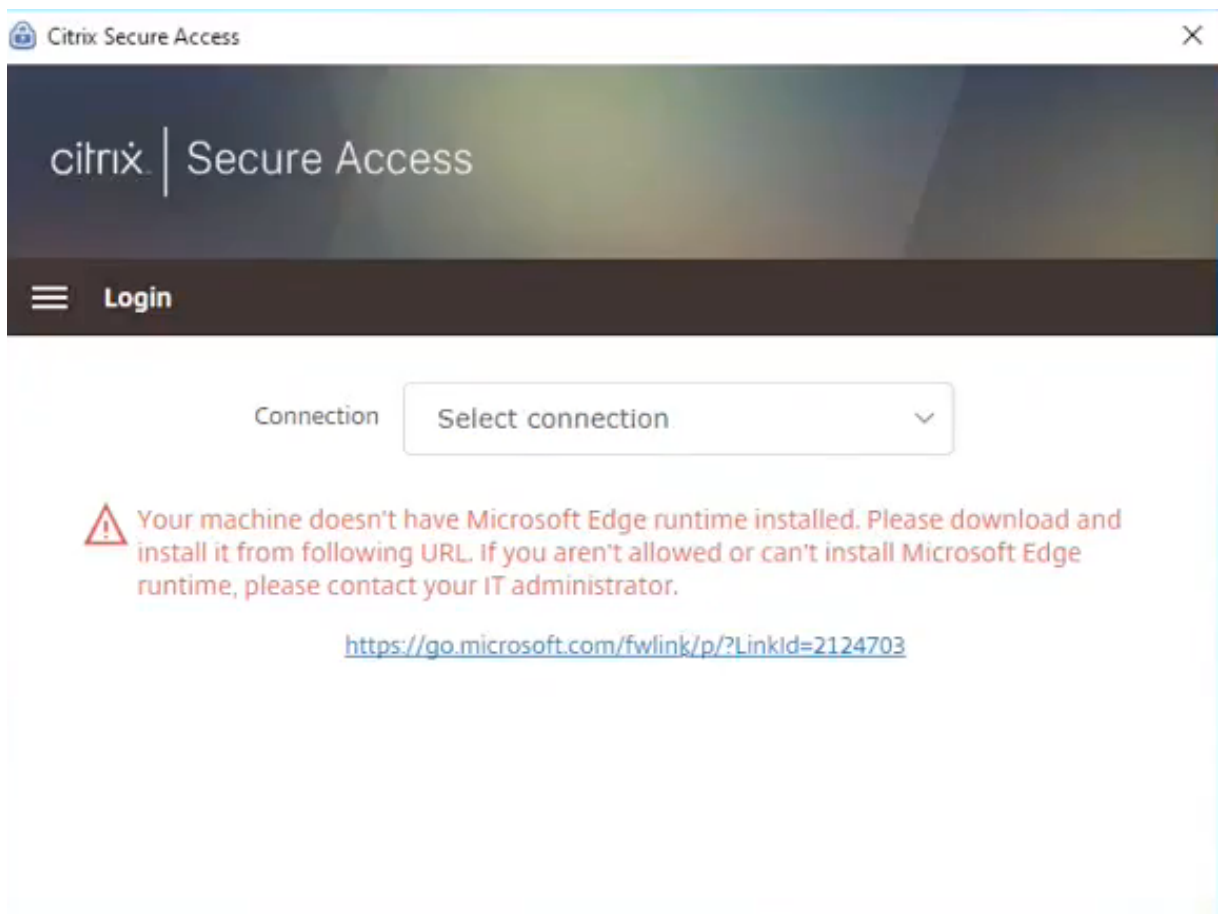
Les écrans d'authentification de l'interface utilisateur du client Citrix Secure Access apparaissent comme suit.



Une fois que les utilisateurs finaux ont sélectionné l'URL, le client Citrix Secure Access ouvre une nouvelle fenêtre les invitant à se connecter à NetScaler Gateway à l'aide de leurs informations d'identification.



Si le moteur d'exécution Microsoft Edge WebView n'est pas installé sur la machine cliente Windows, les utilisateurs finaux reçoivent un lien sur l'interface utilisateur du client Citrix Secure Access pour télécharger et installer le moteur d'exécution Microsoft Edge WebView. Les utilisateurs finaux peuvent télécharger et installer le moteur d'exécution Edge WebView de manière fluide lorsqu'ils sont connectés au VPN et l'authentification n'est pas interrompue pendant ce processus.



Remarques :

- La fonctionnalité Microsoft Edge WebView n'a aucune incidence sur les configurations spécifiques à l'administrateur.
- Nous vous recommandons d'activer la fonctionnalité de [cookie HttpOnly](#) lorsque vous

utilisez Edge WebView sur Citrix Secure Access. Cela améliore la durée de connexion à NetScaler Gateway lorsque l'EPA est utilisé comme facteur dans le flux nfactor.

Dépannage

- Si vous rencontrez des problèmes avec cette fonctionnalité, contactez le [support Citrix](#).
- Vous pouvez envoyer vos commentaires sur la fonctionnalité Edge WebView via citrixgatewaybetafeedback@cloud.com.

Collecte de journaux améliorée pour le client Windows

March 27, 2024

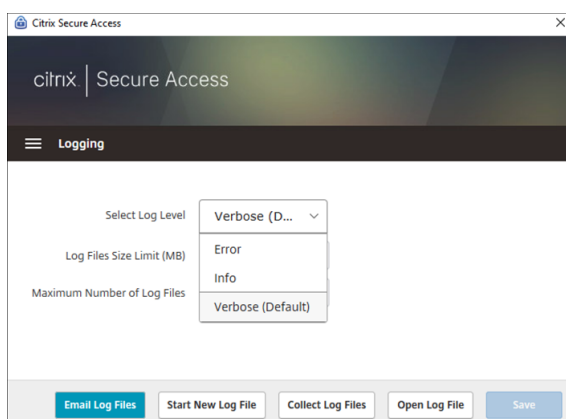
La fonctionnalité de journalisation du client Windows Secure Access est améliorée grâce à une meilleure collecte des journaux et à un débogage améliorés. Les nouveaux fichiers journaux sont préfixés par « csa_ ».

À partir du client Citrix Secure Access pour Windows 23.10.1.7, le niveau de journalisation par défaut est défini sur Verbose pour une collecte de journaux et un débogage améliorés.

Grâce à ces modifications, les administrateurs et les utilisateurs finaux peuvent collecter les journaux de la session en cours ainsi que des sessions passées. Auparavant, la collecte des journaux était limitée aux sessions en cours uniquement.

Configurer la journalisation à l'aide de l'interface utilisateur du client Citrix Secure Access

1. Installez le client Secure Access pour Windows.
2. Cliquez sur **Journalisation** dans le menu. Toutes les configurations relatives aux journaux peuvent être effectuées dans l'écran de journalisation.



- **Sélectionnez le niveau de journalisation :**

Lorsque le nouveau mécanisme de journalisation est activé, les trois niveaux de journalisation suivants sont disponibles.

- Erreur : seules les exceptions ou les défaillances signalées par l’application sont enregistrées.
- Info : Ce niveau inclut les messages d’information et les événements relatifs à l’exécution du programme. Il inclut également les erreurs et les exceptions.
- Verbose (par défaut) : ce niveau inclut tous les messages de journal signalés par les niveaux de journal des erreurs et des informations, ainsi que des messages supplémentaires susceptibles de faciliter le dépannage.

- **Limite de taille du fichier journal :** (Obligatoire) Entrez la taille du fichier journal de chaque fichier journal. La valeur maximale est de 600 Mo.
- **Nombre maximum de fichiers journaux :** (Obligatoire) Entrez le nombre de fichiers que vous souhaitez ajouter pour la collecte des journaux. La valeur maximale est 5.
- **Fichiers journaux par e-mail :** envoyez les fichiers journaux par e-mail à l’adresse e-mail enregistrée.
- **Démarrer un nouveau fichier journal :** lorsque vous sélectionnez cette option, un nouveau fichier journal est créé.
- **Collecter les fichiers journaux :** cliquez pour créer un fichier zip contenant tous les fichiers journaux de l’application. Ce fichier zip est enregistré sur le bureau du client.
- **Ouvrir les fichiers journaux :** lorsque vous sélectionnez cette option, le dernier fichier `csa_nssslvpn*.txts` ouvre.

Client Citrix Secure Access pour Linux

March 27, 2024

Le client Citrix Secure Access pour Linux est un logiciel client VPN géré par NetScaler Gateway qui permet aux utilisateurs d'accéder à distance aux données et aux applications de l'entreprise. Le client Citrix Secure Access protège les applications contre les accès non autorisés, les menaces au niveau des applications et les attaques basées sur les navigateurs.

Le client Citrix End Point Analysis (EPA) est un logiciel client géré par NetScaler Gateway. Il vérifie les critères des terminaux avant d'autoriser l'accès aux données de l'entreprise via NetScaler Gateway. Le client Citrix EPA et le client Citrix Secure Access sont indépendants l'un de l'autre.

Remarque :

Même si vous n'utilisez pas l'EPA, nous vous recommandons de mettre à jour simultanément les fichiers binaires des plug-ins EPA et VPN au cas où vous décideriez d'utiliser la fonctionnalité EPA ultérieurement.

Versions Linux prises en charge

Le client Citrix Secure Access et le client Citrix EPA sont compatibles avec les versions Ubuntu 18.04, Ubuntu 20.04 et Ubuntu 22.04. Pour plus d'informations sur les navigateurs pris en charge, consultez la section [Configuration logicielle requise pour les clients](#).

Remarque :

Pour qu'Ubuntu 22.04 fonctionne avec le client Citrix Secure Access et le client Citrix EPA, définissez le paramètre SSL `denySSLReneg` sur `NONSECURE` sur la CLI NetScaler.

Fonctionnalités prises en charge

Le client Citrix Secure Access pour Ubuntu prend en charge les fonctionnalités suivantes :

- Split tunneling et split tunneling inversé
- Tunnelisation d'applications TCP, UDP et ICMP
- Connexions initiées par le serveur via Intranet IP (IIP)
- Split DNS distant
- Proxy côté client
- Scans EPA classiques
- Authentification avancée (nFactor), y compris des scans EPA avancés (uniquement depuis le navigateur)

- Cookies HTTP uniquement
- Équilibrage global de la charge des serveurs (GSLB)

Remarque :

Split DNS BOTH n'est pas pris en charge avec le client Citrix Secure Access pour Ubuntu.

Mettre à niveau les clients Ubuntu sur NetScaler Gateway

Vous pouvez télécharger le client Citrix Secure Access et le client Citrix EPA pour Ubuntu depuis la page [Téléchargements](#).

Le client Citrix Secure Access et le client Citrix EPA sont nommés « nsgclient18_64.deb » et « nsepa18.deb », respectivement. Les clients sont compatibles avec Ubuntu 18.04 et 20.04.

Le client Citrix Secure Access et le client Citrix EPA qui prennent en charge Ubuntu 22.04 sont nommés « nsginstaller64.deb » et « nsepa.deb », respectivement.

Si vous souhaitez effectuer une mise à niveau vers la dernière version du client Citrix Secure Access de la version 1.0.0.x à la version 23.6.1, par exemple :

1. Remplacez les fichiers « nsgclient18_64.deb » et « nsginstaller64.deb » sur l'emplacement `/var/netscaler/gui/vpn/scripts/linux/` en utilisant l'invite shell.
2. Remplacez les fichiers « nsepa18.deb » et « nsepa.deb » sur l'emplacement `/var/netscaler/gui/epa/scripts/linux/` en utilisant l'invite shell.
3. Ouvrez le fichier `/var/netscaler/gui/vpn/scripts/linux/clientversions.xml`.

- a) Pour le client Citrix EPA, remplacez la version actuelle (1.0.0.x) dans les balises XML suivantes par la dernière version (23.6.1). Si les balises XML n'existent pas, ajoutez-les au fichier XML. Par exemple,

remplacer

```
<component pkgname="nsepa18"currentversion="1.0.0.x"minversion="1.0.0.x"ostype="ubuntu64"minkernelversion="0"maxkernelversion="100"updatetype="compatible"action="/epa/scripts/linux/nsepa18.deb"/>
```

avec

```
<component pkgname="nsepa18"currentversion="23.6.1"minversion="23.6.1"ostype="ubuntu64"minkernelversion="0"maxkernelversion="100"updatetype="compatible"action="/epa/scripts/linux/nsepa18.deb"/>
```

et remplacer

```
<component pkgname="nsepa22"currentversion="1.0.0.x"minversion="1.0.0.x"ostype="ubuntu64"minkernelversion="0"maxkernelversion="100"updatetype="compatible"action="/epa/scripts/linux/nsepa.deb"/>
```

avec

```
<component pkgname="nsepa22"currentversion="23.6.1"minversion="23.6.1"ostype="ubuntu64"minkernelversion="0"maxkernelversion="100"updatetype="compatible"action="/epa/scripts/linux/nsepa.deb"/>
```

- b) Pour le client Citrix Secure Access, remplacez la version actuelle (1.0.0.x) dans les balises XML suivantes par la dernière version (23.6.1). Si les balises XML n'existent pas, ajoutez-les au fichier XML. Par exemple,

remplacer

```
<component pkgname="nsgclient18"currentversion="1.0.0.x"minversion="1.0.0.x"ostype="ubuntu64"minkernelversion="3.0"maxkernelversion="5.16"updatetype="compatible"action="/vpn/scripts/linux/nsgclient18_64.deb"/>
```

sur

```
<component pkgname="nsgclient18"currentversion="23.6.1"minversion="23.6.1"ostype="ubuntu64"minkernelversion="3.0"maxkernelversion="5.16"updatetype="compatible"action="/vpn/scripts/linux/nsgclient18_64.deb"/>
```

et

```
<component pkgname="nsgclient22"currentversion="1.0.0.x"minversion="1.0.0.x"ostype="ubuntu64"minkernelversion="3.0"maxkernelversion="5.20"updatetype="compatible"action="/vpn/scripts/linux/nsginstaller64.deb"/>
```

sur

```
<component pkgname="nsgclient22"currentversion="23.6.1"minversion="23.6.1"ostype="ubuntu64"minkernelversion="3.0"maxkernelversion="5.20"updatetype="compatible"action="/vpn/scripts/linux/nsginstaller64.deb"/>
```

4. À l'invite du shell NetScaler, exécutez les commandes suivantes :

```
1 rm -rf /netscaler/ns_gui
2 ln -s /var/netscaler/gui /netscaler/ns_gui
```

5. Sur l'interface de ligne de commande NetScaler, exécutez les commandes suivantes :

```
1 set vpn parameter -clientversions all
2 flush cache contentgroup loginstaticobjects
```

Références

- [Clients VPN NetScaler Gateway et fonctionnalités prises en charge](#)
- [Analyses Endpoint Analysis prises en charge pour Ubuntu](#)
- [Documentation d'aide pour l'utilisateur final](#)

Notes de mise à jour de Citrix Secure Access pour Linux

March 27, 2024

Le client Citrix Secure Access et le client Citrix End Point Analysis (EPA) pour Linux sont désormais disponibles de manière autonome et sont compatibles avec toutes les versions de NetScaler. La version du client Citrix Secure Access suit le format YY.MM.Release.Build.

Les notes de mise à jour décrivent les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes, les problèmes résolus et les problèmes connus.

Nouveautés : Les nouvelles fonctionnalités et améliorations disponibles dans la version actuelle.

Problèmes résolus : problèmes résolus dans la version actuelle.

Problèmes connus : problèmes qui existent dans la version actuelle et solutions de contournement, le cas échéant.

Pour obtenir des informations détaillées sur les fonctionnalités prises en charge, consultez la documentation du [produit NetScaler Gateway](#).

23.10.3 (16 octobre 2023)

Problèmes résolus

Pour les utilisateurs français, la page Connexions de l'interface utilisateur Citrix Secure Access pour Linux affiche le taux de transfert de données en Ko et Mo au lieu de Ko et Mo, respectivement.

[NSOSLX-177]

23.9.1 (8 septembre 2023)

Nouveautés

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

[CGOP-25231]

23.6.2 (20 juin 2023)

Nouveautés

- **Prise en charge d'Ubuntu 22.04 pour le client Citrix Secure Access et le client Citrix EPA**

Ubuntu 22.04 est la dernière version de support à long terme d'Ubuntu. Les clients Citrix Secure Access et Citrix EPA sont compatibles avec Ubuntu 22.04. Pour plus d'informations, consultez la section [Configuration logicielle requise pour le client](#).

[CGOP-24312]

- **Support GSLB pour les clients Citrix Secure Access et Citrix EPA**

Le client Citrix Secure Access et le client Citrix EPA pour Ubuntu prennent en charge la fonctionnalité Global Server Load Balancing (GSLB) sur NetScaler Gateway. En configurant GSLB pour NetScaler Gateway, les administrateurs peuvent s'assurer que le réseau de l'entreprise (ressources intranet) est toujours accessible aux utilisateurs finaux, quel que soit leur emplacement géographique. Le GSLB répond également aux situations de catastrophe ou aux pannes de réseau dans lesquelles les utilisateurs d'un centre de données peuvent être redirigés vers un autre centre de données. Pour plus d'informations, consultez la section [Prise en charge des déploiements GSLB actifs-actifs sur NetScaler Gateway](#).

[CGOP-23506]

- **Prise en charge de HTTP/Only pour les clients Citrix Secure Access et Citrix EPA**

Les clients Citrix Secure Access et Citrix EPA prennent en charge l'indicateur HTTPOnly sur les cookies d'authentification. Les administrateurs de NetScaler Gateway configurent la fonctionnalité HTTPOnly sur les cookies d'authentification générés par les applications Web. Cette fonctionnalité permet d'empêcher le vol de cookies dû à l'utilisation de scripts intersites. Pour plus d'informations, voir [Appliquer l'indicateur HTTPOnly sur les cookies d'authentification](#).

[CGOP-23517]



© 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).
