NetScaler

Citrix SSO

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

Citrix SSO pour appareils iOS/macOS

March 13, 2020

Le client VPN Citrix hérité a été construit à l'aide des API VPN privées d'Apple qui sont désormais obsolètes. La prise en charge VPN dans Citrix SSO est réécrite à partir de zéro à l'aide du framework public Network Extension d'Apple.

Voici quelques-unes des principales fonctionnalités introduites avec l'application Citrix SSO :

- **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, etc. Ce code utilise le protocole T-OTP (Mot de passe à usage unique basé sur le temps) pour générer le code OTP similaire à des services tels que Google Authenticator, Microsoft Authenticator, etc. Les utilisateurs sont invités à entrer deux mots de passe lors de l'authentification à Citrix Gateway pour un utilisateur Active Directory donné. Le deuxième facteur est un code à six chiffres évolutif 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'appliance Citrix ADC. Pour les étapes d'inscription, reportez-vous à la section https://support.citrix.com/article/CTX228454. Sur l'application, les utilisateurs peuvent ajouter la fonctionnalité OTP en scannant le code QR généré sur Citrix ADC ou en saisissant manuellement le secret TOTP. Les jetons OTP une fois ajoutés apparaissent sur le segment de 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 directement à VPN à partir de leurs appareils iOS.

L'application Citrix SSO peut être utilisée pour scanner le code QR lors de l'inscription à la prise en charge Native OTP.La fonctionnalité de notification Push
Citrix Gateway est disponible uniquement pour les utilisateurs de l'application Citrix SSO.

- **Notification push :** Citrix Gateway envoie une notification push sur votre appareil mobile enregistré pour une expérience d'authentification simplifiée à deux facteurs. Au lieu d'ouvrir l'application Citrix SSO pour taper le deuxième facteur OTP sur la page d'ouverture de session Citrix ADC, vous pouvez valider votre identité en fournissant votre code PIN de périphérique/Touch ID pour le périphérique enregistré.

Une fois que vous avez enregistré votre appareil pour la notification Push, vous pouvez également l'utiliser pour prendre en charge Native OTP à l'aide de l'application Citrix SSO. 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 Citrix ADC le prend en charge.

Notes de publication

March 13, 2020

Les notes de publication de Citrix SSO décrivent les nouvelles fonctionnalités, les améliorations apportées aux fonctionnalités existantes, les problèmes résolus et les problèmes connus disponibles dans une Service Release. Les notes de publication comprennent une ou plusieurs des sections suivantes :

Nouveautés : 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.

V1.2.6

Problèmes connus

- Le VPN est parfois bloqué après le réveil de macOS.

  [NSHELP-20656 - macOS]

V1.2.5

Problèmes connus

- Le VPN est parfois bloqué après le réveil de macOS.

  [NSHELP-20656 - macOS]

V1.2.4

Problèmes connus

- Parfois, la session VPN ne répond pas après le réveil du Mac du mode veille.

  [NSHELP-20656 - macOS]

V1.2.3

Nouveautés

- Schéma d'URL d'SSO Citrix — Citrix SSO enregistre désormais un schéma d'URL afin que d'autres applications puissent déterminer si Citrix SSO est installé sur un périphérique iOS. Le

schéma d'URL est "citrixsso."

[CGOP-11979 - iOS]

Problèmes résolus

- L'application Citrix SSO se bloque lors de l'envoi d'un trafic UDP important.

  [CGOP-11603 - macOS]

- Citrix SSO pour iPad se bloque lorsque l'application est démarrée à partir d'une notification sur iOS 13.

  [NSHELP-21087 - iOS]

V1.2.2

Problèmes résolus

- Dans certains déploiements GSLB, Citrix SSO résout le nom de la Gateway plusieurs fois, ce qui entraîne des échecs de connexion.

  [CGOP-12013]

- Citrix SSO pour iOS ne parvient pas à analyser OTPSecret supérieur à 16 octets.

  [CGOP-11978 - iOS]

- Les utilisateurs dont les profils sont configurés pour l'authentification par certificat uniquement et une vérification NAC sont invités à entrer les informations d'identification d'ouverture de session et ne sont pas en mesure de créer les connexions VPN.

  [CGOP-11925 - iOS]

- Bien que l'indicateur Tunnel Split par application soit vérifié uniquement pour le trafic TCP, le trafic ICMP est tunnelé même dans les cas où le trafic ICMP doit être envoyé directement.

  [CGOP-11614 - iOS]

Problèmes connus

- Le plug-in Citrix Gateway pour macOS ne prend pas en charge la fonctionnalité qui ouvre la page de destination sur l'application Citrix Workspace.

  [NSHELP-7047]

V1.2.0

Nouveautés

- **Prise en charge de l'authentification nFactor.**L'authentification nFactor est désormais prise en charge sur iOS et macOS.

  [CGOP-11251]

- **Prise en charge de l'application Citrix SSO.** L'application Citrix SSO est désormais prise en charge sur iOS 13 et macOS Catalina.

  [CGOP-11714]

Problèmes résolus

- L'adresse IP du client est affichée à l'envers dans la page Connexions de l'application SSO.

  [CGOP-11596]

- Citrix SSO n'honore pas le bit tronqué DNS dans l'indicateur DNS dans Citrix ADC version 13.0.

  [CGOP-11777]

- Le tunnel fractionné par application n'est pas compatible avec Citrix ADC version 13.0.

  [CGOP-11464]

- Citrix SSO ignore certains messages de délai d'expiration de Citrix Gateway.

  [CGOP-11310]

- Lorsque les utilisateurs se connectent à l'application pour la première fois, la dernière ligne de la description de l'application n'apparaît pas sur l'écran de l'utilisateur.

  [CGOP-11595 - macOS]

- La taille de la fenêtre d'ouverture de session de l'application Citrix SSO continue d'augmenter lorsque vous cliquez plusieurs fois sur le bouton d'ouverture de session.

  [CGOP-11594 - macOS]

- Lorsque la limite maximale d'utilisateurs sous licence est dépassée, un message d'erreur s'affiche au niveau du système et non dans la fenêtre de l'application.

  [CGOP-11600 - macOS]

V1.1.12

Nouveautés

- **Collecte de données de télémétrie pour macOS.** Citrix SSO collecte des événements d'analyse personnalisés liés à l'utilisation du VPN dans l'application.

  [CGOP-9789 - macOS]

- **Prise en charge du split tunneling par application.** Les administrateurs peuvent configurer un split tunneling par application. Le trafic par application correspondant aux routes intranet de Citrix Gateway est acheminé en tunnelage vers l'appliance Citrix Gateway.

  [CGOP-657]

- **FQDN Split Tunnel trafic basé sur le nom de domaine complet du système.** FQDN Split Tunnel tunnel le trafic basé sur le nom de domaine complet du système plutôt que sur l'adresse IP résolue par les serveurs DNS.

  [CGOP-316]

Problèmes résolus

- Les éléments de l'interface utilisateur tels que les boutons, les champs de texte, les étiquettes, etc. sont mal alignés sur les écrans de l'iPad.

  [CGOP-10141 - iOS]

- Les utilisateurs ne sont pas avertis pour une connexion à distance s'ils n'ont pas de profil VPN ajouté.

  [CGOP-9731 - iOS]

V1.1.10

Problèmes résolus

- L'application Citrix SSO n'affiche pas le message d'erreur approprié lors de l'atteinte du lorsque le nombre maximal d'utilisateurs.

  [CGOP-231]

- La case CLUF n'est pas désactivée par défaut.

  [CGOP-245]

- Ajout de fonctionnalité n'est pas pris en charge pour l'analyse anti-hameçonnage « activée » dans EndPoint Analysis.

  [CGOP-249]

- La sélection automatique du certificat client/périphérique pour l'authentification ne se produit pas même si un seul client/périphérique est présent dans le trousseau.

  [CGOP-251]

- Impossible d'ajouter un « enregistrement de connexion » après avoir modifié un dans l'application Citrix SSO.

  [CGOP-7256]

Configurer Citrix SSO pour les utilisateurs iOS

April 18, 2023

> **IMPORTANT :** Citrix VPN ne peut pas être utilisé sur iOS 12 et versions ultérieures. Pour continuer au VPN, utilisez l'application Citrix SSO.

Le tableau suivant compare la disponibilité de diverses fonctionnalités entre Citrix VPN et Citrix SSO.

Fonctionnalité	Citrix VPN	Citrix SSO
VPN au niveau de l'appareil	Pris en charge	Pris en charge
VPN par application (MDM uniquement)	Pris en charge	Pris en charge
Split tunneling par application	Non pris en charge	Pris en charge
Profils VPN configurés MDM	Pris en charge	Pris en charge
VPN à la demande	Pris en charge	Pris en charge
Jetons de mot de passe (basés sur T-OTP)	Non pris en charge	Pris en charge
Connexion basée sur les notifications push (second facteur à partir du téléphone enregistré)	Non pris en charge	Pris en charge
Authentification basée sur le certificat	Pris en charge	Pris en charge
Authentification du nom d'utilisateur/mot de passe	Pris en charge	Pris en charge

Fonctionnalité	Citrix VPN	Citrix SSO
Vérification du contrôle d'accès réseau avec Citrix Endpoint Management (anciennement XenMobile)	Non pris en charge	Pris en charge
Vérification du contrôle d'accès réseau avec Microsoft Intune	Pris en charge	Pris en charge
Prise en charge de DTLS	Non pris en charge	Pris en charge
Bloquer les profils VPN créés par l'utilisateur	Pris en charge	Pris en charge
Authentification unique pour les applications natives gérées par Citrix Cloud	Non pris en charge	Pris en charge
Version de système d'exploitation prise en charge	iOS 9, 10, 11 (ne fonctionne pas à partir d'iOS 12+)	iOS 9+

Compatibilité avec les produits MDM

Citrix SSO est compatible avec la plupart des fournisseurs MDM tels que Citrix Endpoint Management (anciennement XenMobile), Microsoft Intune, etc.

Citrix SSO prend également en charge une fonctionnalité appelée Contrôle d'accès réseau (NAC). Pour en savoir plus sur NAC, cliquez ici. Avec NAC, les administrateurs MDM peuvent appliquer la conformité des machines de l'utilisateur final avant de se connecter à Citrix ADC. NAC sur Citrix SSO nécessite un serveur MDM tel que Citrix Endpoint Management ou Intune et Citrix ADC.

Configurer un profil VPN géré par MDM pour Citrix SSO

La section suivante capture les instructions étape par étape pour configurer les profils VPN à l'échelle du périphérique et par application pour Citrix SSO à l'aide de Citrix Endpoint Management (anciennement XenMobile) à titre d'exemple. D'autres solutions MDM peuvent utiliser ce document comme référence lorsque vous travaillez avec Citrix SSO.

> **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 serveurs proxy à la demande, en continu et en suivant la documentation Citrix Endpoint Management (anciennement

> XenMobile) ou la configuration de charge utile VPN MDM d'Apple.

Profils VPN au niveau du périphérique

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

Pour configurer un VPN au niveau du périphérique sur Citrix Endpoint Management

Procédez comme suit pour configurer un VPN au niveau du périphérique sur Citrix Endpoint Management.

1. Sur la console Citrix Endpoint Management MDM, accédez à **Configurer** > **Stratégies de périphérique** > **Ajouter une nouvelle stratégie**.

2. Sélectionnez **iOS** dans le volet de gauche de la Plateforme de stratégie. Sélectionnez **VPN** dans le volet droit.

3. Dans la page **Informations sur la stratégie**, entrez un nom et une description de stratégie valides, puis cliquez sur **Suivant**.

4. Sur la page **Stratégie VPN** pour iOS, tapez un nom de connexion valide et choisissez **SSL personnalisé** dans **Type de connexion**.

Remarque : 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 l'**identifiant SSL personnalisé (format DNS inverse)**, entrez **com.citrix.netscalerGateway.ios.app**. Il s'agit de l'identificateur de bundle pour l'application Citrix SSO sur iOS.

Remarque : Dans la charge utile VPN MDM, l'identificateur SSL personnalisé correspond à la clé **VPNSubType**.

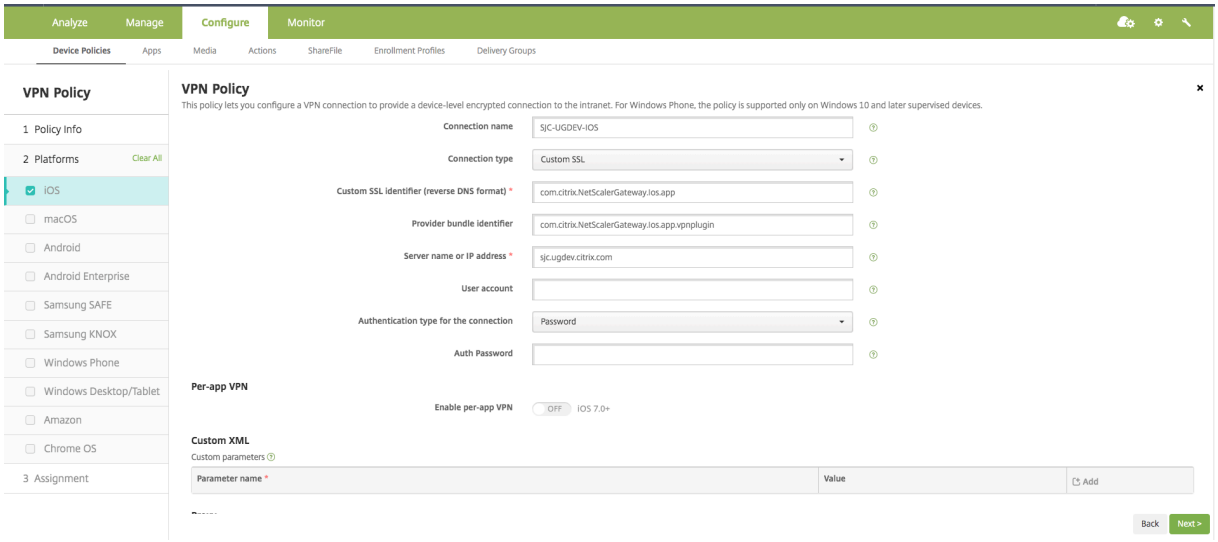
6. Dans l'**identifiant du bundle fournisseur**, entrez **com.citrix.NetScalerGateway.ios.app.vpnPlugin** . Il s'agit de l'identificateur de bundle de l'extension réseau contenue dans le binaire de l'application Citrix SSO iOS.

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

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

Les champs restants de la page de configuration sont facultatifs. Les configurations de ces champs se trouvent 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 VPN pour une application spécifique. Le trafic provenant uniquement de l'application spécifique est acheminé vers Citrix Gateway. La charge utile VPN par application prend en charge toutes les clés pour VPN à l'échelle de l'appareil ainsi que quelques clés supplémentaires.

Pour configurer un VPN par application sur Citrix Endpoint Management

Procédez comme suit pour configurer un VPN par application :

1. Terminez la configuration VPN au niveau du périphérique sur Citrix Endpoint Management.
2. Activez le commutateur **Activer Per App VPN** dans la section Per App VPN.
3. Activez le commutateur **Correspondance d'application à la demande activée** si Citrix SSO doit être démarré automatiquement lorsque l'application Match est lancée. Ceci est recommandé pour la plupart des cas par application.

Remarque : Dans la charge utile VPN MDM, ce champ correspond à la clé **OnDemandMatchAppenabled**.

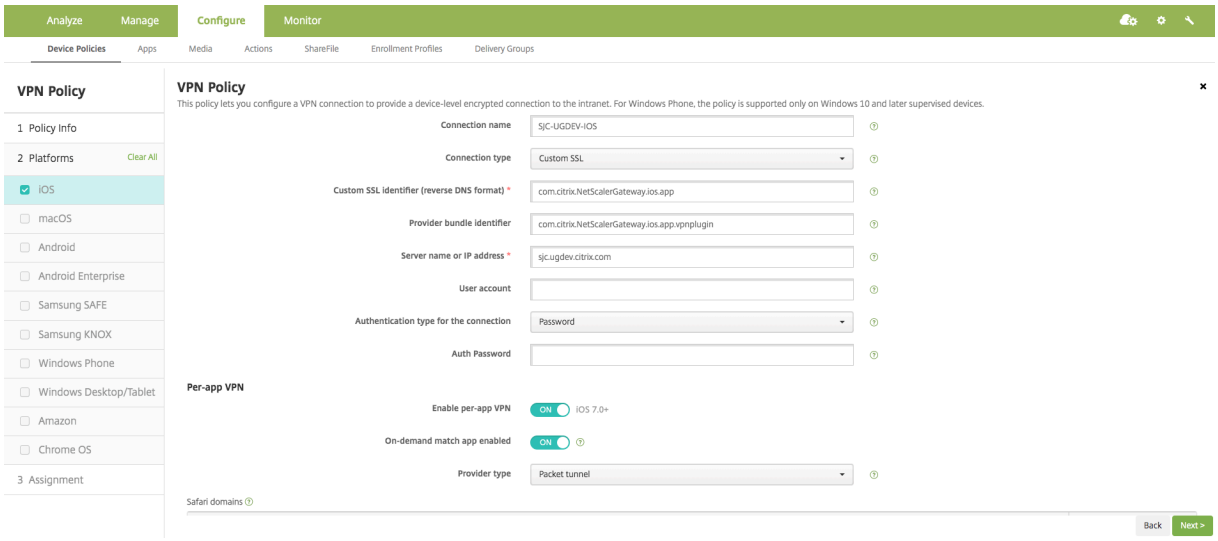
4. Dans **Type de fournisseur**, sélectionnez **Tunnel de paquets**.

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

5. La configuration du domaine Safari est facultative. Lorsque le domaine Safari est configuré, Citrix SSO démarre automatiquement lorsque les utilisateurs lancent Safari et accèdent à une URL correspondant à celle du champ **Domaine**. Ceci n'est pas recommandé si vous souhaitez restreindre le VPN pour une application spécifique.

Remarque : Dans la charge utile VPN MDM, ce champ correspond aux principaux **SafariDomains**.

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



14. Cliquez sur **Suivant.**

15 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 tunneling dans un VPN par application

Les clients MDM peuvent configurer le split tunneling dans le VPN Per-App pour Citrix SSO. Pour ce faire, la paire clé/valeur suivante doit être ajoutée à la section de configuration 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 alors 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 pour les fournisseurs MDM. Vous devez contacter 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 l'utilisateur

Les clients MDM peuvent empêcher les utilisateurs de créer manuellement des profils VPN à partir de l'application Citrix SSO. Pour ce faire, la paire clé/valeur suivante doit être ajoutée à la section de configuration 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 alors 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 pour les fournisseurs MDM. Vous devez contacter 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.

Problèmes connus

Description du problème : Tunneling pour les adresses de nom complet contenant un domaine « .local » dans les configurations VPN par application ou VPN à la demande. Il y a un bogue dans le framework d'extension réseau d'Apple qui empêche les adresses FQDN contenant .local dans la partie domaine (par exemple http://wwww.abc.local) d'être tunnelées sur l'interface TUN du système. Le trafic de cette adresse est envoyé via l'interface physique de l'appareil à la place. Le problème est observé uniquement avec les configurations VPN par application ou VPN à la demande et n'est pas vu avec les configurations VPN à l'échelle du système. Citrix a déposé un rapport de bogue radar auprès d'Apple, et Apple avait noté que selon RFC-6762 :https://tools.ietf.org/html/rfc6762, .local est une requête DNS multicast (MDN) et n'est donc pas un bogue. Cependant, Apple n'a pas encore fermé le bogue et il n'est pas clair si le problème sera résolu dans les futures versions iOS.

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

Limitations

- le split tunneling basé sur le nom de domaine complet n'est pas encore entièrement pris en charge.
- 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.

Configurer Citrix SSO pour les utilisateurs macOS

April 18, 2023

L'application Citrix SSO pour macOS offre la meilleure solution d'accès aux applications et de protection des données offerte par Citrix Gateway. Vous pouvez désormais accéder en toute sécurité aux applications stratégiques, aux postes de travail virtuels et aux données d'entreprise, où que vous soyez et à tout moment.
Citrix SSO est le client VPN de nouvelle génération pour Citrix Gateway pour créer et gérer les connexions VPN à partir de périphériques macOS. Citrix SSO est construit à l'aide du framework Network Extension (NE) d'Apple. Le framework NE d'Apple est une bibliothèque moderne qui contient des API qui peuvent être utilisées pour personnaliser et étendre les fonctionnalités de réseau de base de macOS. L'extension réseau avec prise en charge du VPN SSL est disponible sur les appareils fonctionnant sous macOS 10.11 +.

L'application Citrix SSO remplace le plug-in Citrix Gateway hérité basé sur les extensions Kernel (KE) qui sera bientôt obsolète par Apple. L'application Citrix SSO prend en charge des fonctionnalités avancées telles que les connexions initiées par le serveur et DTLS.

L'application Citrix SSO fournit une prise en charge complète de la gestion des périphériques 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.
L'application Citrix SSO pour macOS peut être installée à partir d'un Mac App Store.

Comparaison des fonctionnalités entre Citrix VPN et Citrix SSO

Le tableau suivant compare la disponibilité de diverses fonctionnalités entre Citrix VPN et Citrix SSO.

Fonctionnalité	Citrix VPN	Citrix SSO
Méthode de distribution des applications	page de téléchargements Citrix	Magasin d'applications
Nombre de connexions en tunnel	128	128

Fonctionnalité	Citrix VPN	Citrix SSO
Accès depuis le navigateur	Pris en charge	Non pris en charge
Accès depuis l'application native	Pris en charge	Pris en charge
Split Tunneling (DÉSACTIVÉ/ACTIVÉ/INVERSE)	Pris en charge	Pris en charge
Split DNS (LOCAL/DISTANT/LES DEUX)	DISTANT	DISTANT
Accès au réseau local	Activer/Désactiver	Toujours activé
Prise en charge des connexions initiées par le serveur (SIC)	Non pris en charge	Pris en charge
Transférer la connexion	Pris en charge	Pris en charge
Proxy côté client	Pris en charge	Non pris en charge
Prise en charge d'EPA Classic/Opswat	Pris en charge	Pris en charge
Prise en charge des certificats d'appareil	Pris en charge	Pris en charge
Prise en charge du délai d'expiration de session	Pris en charge	Pris en charge
Prise en charge du délai d'expiration forcé	Pris en charge	Pris en charge
Prise en charge du délai d'inactivité	Pris en charge	Non pris en charge
IPV6	Non pris en charge	Pris en charge
Itinérance du réseau (Basculer entre Wi-Fi, Ethernet, etc.)	Pris en charge	Pris en charge
Prise en charge des applications intranet	Pris en charge	Pris en charge
Prise en charge de DTLS pour UDP	Non pris en charge	Pris en charge
Prise en charge du CLUF	Pris en charge	Pris en charge
Intégration appli + Receiver	Pris en charge	Non pris en charge

Fonctionnalité	Citrix VPN	Citrix SSO
Authentification — Local, LDAP, RADIUS	Pris en charge	Pris en charge
Authentification du certificat client	Pris en charge	Pris en charge
Prise en charge de TLS (TLS1, TLS1.1 et TLS1.2)	Pris en charge	Pris en charge
Authentification à deux facteurs	Pris en charge	Pris en charge

Compatibilité avec les produits MDM

Citrix SSO 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) à l'aide de laquelle les administrateurs MDM peuvent appliquer la conformité des machines utilisateur final avant de se connecter à Citrix Gateway. NAC sur Citrix SSO nécessite un serveur MDM tel que XenMobile ou Intune et Citrix Gateway. Pour en savoir plus sur NAC, cliquez sur ici.

Configurer un profil VPN géré par MDM pour Citrix SSO

La section suivante capture les instructions étape par étape pour configurer les profils VPN à l'échelle du périphérique et par application pour Citrix SSO à l'aide de Citrix Endpoint Management (anciennement XenMobile) à titre d'exemple. D'autres solutions MDM peuvent utiliser ce document comme référence lorsque vous travaillez avec Citrix SSO.

> **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 serveurs proxy à la demande, Always-On, en suivant la documentation Citrix Endpoint Management (anciennement XenMobile) ou celle d'Apple Configuration de la charge utile VPN MDM.

Profils VPN au niveau du périphérique

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

Pour configurer un VPN au niveau du périphérique sur Citrix Endpoint Management

Procédez comme suit pour configurer un VPN au niveau du périphérique.

1. Sur la console Citrix Endpoint Management MDM, accédez à **Configurer** > **Stratégies de périphérique** > **Ajouter une nouvelle stratégie**.

2. Sélectionnez **macOS** dans le volet gauche de la Plate-forme de stratégie. Sélectionnez **Stratégie VPN** dans le volet droit.

3. Dans la page **Informations sur la stratégie**, entrez un nom et une description de stratégie valides, puis cliquez sur **Suivant**.

4. Sur la page **Détail de la stratégie** pour macOS, tapez un nom de connexion valide et choisissez **SSL personnalisé** dans **Type de connexion**.

Remarque : 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 l'**identifiant SSL personnalisé (format DNS inverse)**, entrez **com.citrix.netscalerGateway.macos.app**. Il s'agit de l'identificateur de bundle pour l'application Citrix SSO sur macOS.

Remarque : Dans la charge utile VPN MDM, l'identificateur SSL personnalisé correspond à la clé **VPNSubType**.

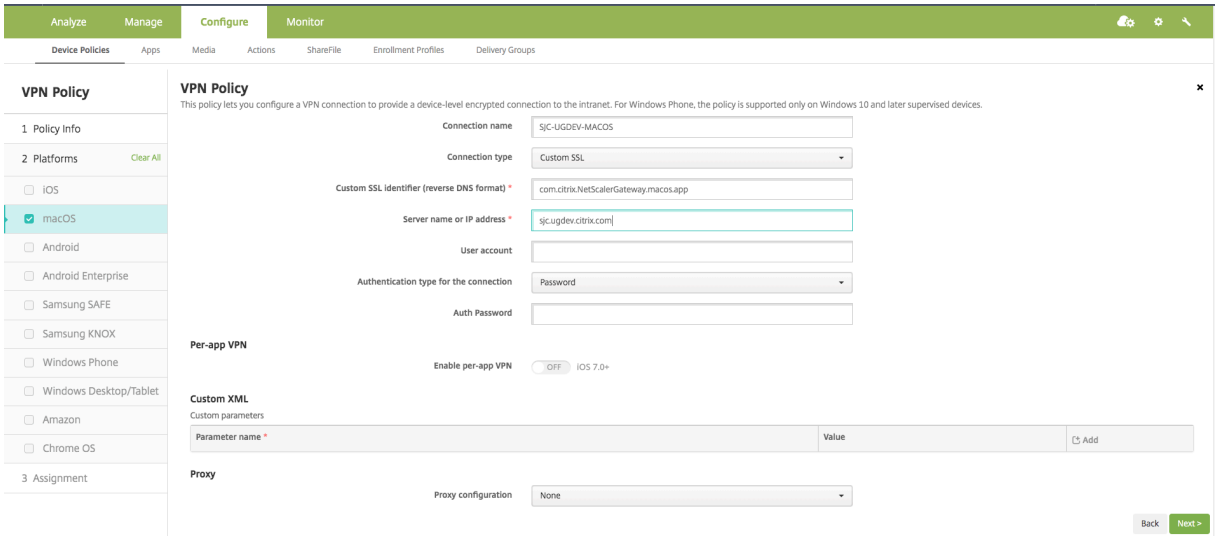
6. Dans l'**identifiant du bundle fournisseur**, entrez **com.citrix.NetScalerGateway.macos.app.vpnplugin**. Il s'agit de l'identificateur de bundle de l'extension réseau contenue dans le binaire de l'application Citrix SSO macOS.

Remarque : Dans la charge utile VPN MDM, l'identificateur de bundle du 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 Citrix ADC associé à cette instance de Citrix Endpoint Management.

Les champs restants de la page de configuration sont facultatifs. Les configurations de ces champs se trouvent dans la documentation Citrix Endpoint Management.

8 Cliquez sur **Suivant**.



9 Cliquez sur **Enregistrer**.

Profils VPN par application

Les profils VPN par application sont utilisés pour configurer VPN pour une application spécifique. Le trafic provenant uniquement de l'application spécifique est acheminé vers Citrix Gateway. La charge utile VPN par application prend en charge toutes les clés pour VPN à l'échelle de l'appareil ainsi que quelques clés supplémentaires.

Pour configurer un VPN par application sur Citrix Endpoint Management

Procédez comme suit pour configurer un VPN par application sur Citrix Endpoint Management :

1. Terminez la configuration VPN au niveau du périphérique sur Citrix Endpoint Management.

2. Activez le commutateur **Activer Per App VPN** dans la section Per App VPN.

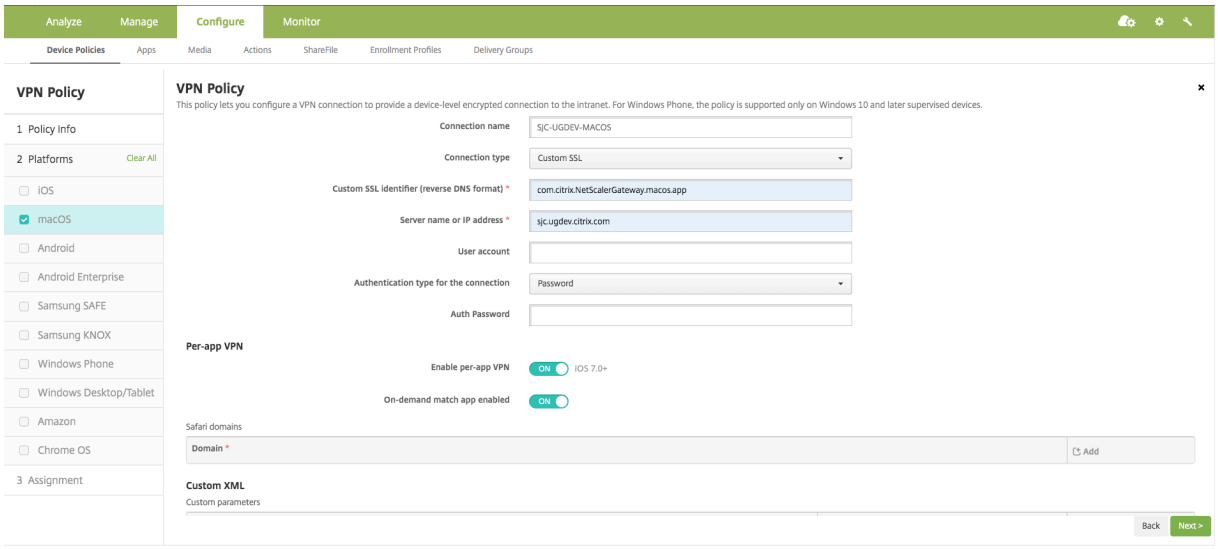
3. Activez le commutateur **Correspondance d'application à la demande activée** si Citrix SSO doit être démarré automatiquement lorsque l'application Match est lancée. Ceci est recommandé pour la plupart des cas par application.

Remarque : Dans la charge utile VPN MDM, ce champ correspond à la clé **OnDemandMatchAppenabled**.

5. La configuration du domaine Safari est facultative. Lorsque le domaine Safari est configuré, Citrix SSO démarre automatiquement lorsque les utilisateurs lancent Safari et accèdent à une URL correspondant à celle du champ **Domaine**. Ceci n'est pas recommandé si vous souhaitez restreindre le VPN pour une application spécifique.

Remarque : Dans la charge utile VPN MDM, ce champ correspond aux principaux **SafariDomains**.

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



13. Cliquez sur **Suivant**.

14. 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 tunneling dans un VPN par application

Les clients MDM peuvent configurer le split tunneling dans le VPN Per-App pour Citrix SSO. Pour ce faire, la paire clé/valeur suivante doit être ajoutée à la section de configuration fournisseur du profil VPN créé sur le serveur MDM.

```
- Clé = "PerAppSplitTunnel"
- Valeur = "true ou 1 ou yes"
```

La clé est sensible à la casse et doit correspondre exactement alors 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 pour les fournisseurs MDM. Vous devez contacter 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 l'utilisateur

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

```
- Clé = "disableUserProfiles"
- Valeur = "true ou 1 ou yes"
```

La clé est sensible à la casse et doit correspondre exactement alors 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 pour les fournisseurs MDM. Vous devez contacter 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.

Problèmes connus

Voici les problèmes connus actuellement.

- La connexion EPA échoue si l'utilisateur est placé dans un groupe de quarantaine.
- Le message d'avertissement de délai d'expiration forcé n'est pas affiché.
- L'application SSO permet de se connecter si le tunnel split est activé et qu'aucune application intranet n'est configurée.

Limitations

Voici les limitations actuelles.

- Certaines analyses EPA (par exemple, analyses de gestion des correctifs, analyse du navigateur Web, processus d'échec) peuvent échouer en raison d'un accès restreint à l'application SSO en raison du sandboxing.
- Le split tunneling basé sur les ports/protocoles n'est pas pris en charge.

Questions fréquentes

Cette section capture les FAQ sur l'application Citrix SSO.

En quoi l'application Citrix SSO est-elle différente de l'application Citrix VPN ?
Citrix SSO est le client VPN SSL de nouvelle génération pour Citrix ADC. L'application utilise le cadre d'extension réseau d'Apple pour créer et gérer des connexions VPN sur les appareils iOS et macOS. Citrix
VPN est le client VPN hérité qui a utilisé les API VPN privées d'Apple qui est désormais obsolète. La prise en charge du VPN Citrix sera supprimée de l'App Store dans les mois à venir.

Qu'est-ce que NE ?
Le framework Network Extension (NE) d'Apple est une bibliothèque moderne qui contient des API qui peuvent être utilisées pour personnaliser et étendre les fonctionnalités de réseau de base d'iOS et de macOS. Network
Extension avec prise en charge du VPN SSL est disponible sur les appareils exécutant iOS 9+ et macOS 10.11+.

Quelles versions de Citrix ADC sont-elles compatibles avec Citrix SSO ?
Les fonctionnalités VPN dans Citrix SSO sont prises en charge sur Citrix ADC versions 10.5 et supérieures. Le TOTP est disponible sur Citrix ADC version 12.0 et supérieure. La notification Push sur Citrix ADC n'a pas encore été annoncée
publiquement. L'application nécessite les versions iOS 9+ et macOS 10.11+.

Comment fonctionne l'authentification basée sur le certificat pour les clients non MDM ?
Les clients qui ont précédemment distribué des certificats par courrier électronique ou par navigateur pour effectuer l'authentification de certificat client dans Citrix VPN doivent noter cette modification lors de l'utilisation de Citrix SSO. Ceci est principalement vrai pour les clients non-MDM qui n'utilisent pas un serveur MDM pour distribuer des certificats utilisateur. Veuillez vous référer à « Importation de certificats dans Citrix SSO via e-mail » pour pouvoir distribuer des certificats.

Qu'est-ce que le contrôle d'accès réseau (NAC) ? Comment configurer NAC avec Citrix SSO et Citrix Gateway ?
Les clients MDM Microsoft Intune et Citrix Endpoint Management (anciennement XenMobile) peuvent tirer parti de la fonctionnalité de contrôle d'accès réseau (NAC) dans Citrix SSO. Avec NAC, les administrateurs peuvent sécuriser leur réseau interne d'entreprise en ajoutant une couche d'authentification supplémentaire pour les appareils mobiles gérés par un serveur MDM. Les administrateurs peuvent appliquer une vérification
de conformité des périphériques au moment de l'authentification dans Citrix SSO.

Pour utiliser NAC avec Citrix SSO, vous devez l'activer sur Citrix Gateway et le serveur MDM.

- Pour activer NAC sur Citrix ADC, reportez-vous à cette rubrique lien.
- Si le fournisseur MDM est Intune, reportez-vous à cette rubrique lien.

- Si le fournisseur MDM est Citrix Endpoint Management (anciennement XenMobile), reportez-vous à cette section lien.

Remarque : La version minimale prise en charge de Citrix SSO est 1.1.6 et supérieure.

Questions fréquentes

April 18, 2023

Cette section capture les questions fréquemment posées sur l'application Citrix SSO.

En quoi l'application Citrix SSO est-elle différente de l'application Citrix VPN ?
Citrix SSO est le client VPN SSL de nouvelle génération pour Citrix ADC. L'application utilise le cadre d'extension réseau d'Apple pour créer et gérer des connexions VPN sur les appareils iOS et macOS. Citrix
VPN est le client VPN hérité qui a utilisé les API VPN privées d'Apple qui est désormais obsolète. La prise en charge du VPN Citrix sera supprimée de l'App Store dans les mois à venir.

Qu'est-ce que NE ?
Le framework Network Extension (NE) d'Apple est une bibliothèque moderne qui contient des API qui peuvent être utilisées pour personnaliser et étendre les fonctionnalités de réseau de base d'iOS et de macOS. Network
Extension avec prise en charge du VPN SSL est disponible sur les appareils exécutant iOS 9+ et macOS 10.11+.

Quelles versions de Citrix ADC sont-elles compatibles avec Citrix SSO ?
Les fonctionnalités VPN dans Citrix SSO sont prises en charge sur Citrix ADC versions 10.5 et supérieures. Le TOTP est disponible sur Citrix ADC version 12.0 et supérieure. La notification Push sur Citrix ADC n'a pas encore été annoncée
publiquement. L'application nécessite les versions iOS 9+ et macOS 10.11+.

Comment fonctionne l'authentification basée sur le certificat pour les clients non MDM ?
Les clients qui ont déjà distribué des certificats via courrier électronique ou navigateur pour effectuer l'authentification de certificat client dans Citrix VPN doivent noter cette modification lors de l'utilisation de Citrix SSO. Ceci est
principalement vrai pour les clients non-MDM qui n'utilisent pas de serveur MDM pour distribuer des certificats utilisateur. Veuillez vous référer à « Importation de certificats dans Citrix SSO via e-mail » pour pouvoir
distribuer des certificats.

Qu'est-ce que le contrôle d'accès réseau (NAC) ? Comment configurer NAC avec Citrix SSO et Citrix Gateway ?
Les clients MDM Microsoft Intune et Citrix Endpoint Management (anciennement XenMobile) peuvent

tirer parti de la fonctionnalité de contrôle d'accès réseau (NAC) dans Citrix SSO. Avec NAC, les administrateurs
peuvent sécuriser leur réseau interne d'entreprise en ajoutant une couche supplémentaire d'authentification pour les appareils mobiles gérés par un serveur MDM. Les administrateurs peuvent appliquer une vérification
de conformité des périphériques au moment de l'authentification dans Citrix SSO.

Pour utiliser NAC avec Citrix SSO, vous devez l'activer sur Citrix Gateway et le serveur MDM.

- Pour activer NAC sur Citrix ADC, reportez-vous à cette rubrique lien.
- Si le fournisseur MDM est Intune, reportez-vous à cette rubrique lien.
- Si le fournisseur MDM est Citrix Endpoint Management (anciennement XenMobile), reportez-vous à cette section lien.

Remarque : La version minimale prise en charge de Citrix SSO est 1.1.6 et supérieure.

Citrix SSO pour appareils Android

March 13, 2020

Citrix SSO fournit la meilleure solution d'accès aux applications et de protection des données offerte par Citrix 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.

Configurer l'application Citrix SSO dans un environnement MDM

March 13, 2020

Pour configurer l'application Citrix SSO dans un environnement MDM, reportez-vous à la section Configurer le protocole Citrix SSO pour Android.

Remarque :

- Dans un environnement non-MDM, les utilisateurs créent manuellement des profils VPN.
- Vous pouvez également créer une configuration gérée par Android Enterprise pour Citrix SSO. Pour plus de détails, consultez Configurer les profils VPN pour Android Enterprise.

NetScaler