À propos de Citrix Receiver pour iOS 6

Jul 13, 2016

Améliorations apportées à Net Promoter Score (NPS)

Des améliorations ont été apportées à la fonctionnalité NPS pour iOS Receiver dans cette version. Citrix Receiver pour iOS invite maintenant les utilisateurs à évaluer leur expérience lors du téléchargement depuis l'App Store d'Apple. Ces commentaires permettent à Citrix de promouvoir le développement continu de ses produits.

Prise en charge de la vue fractionnée

Cette version de iOS Receiver prend en charge la nouvelle fonctionnalité de vue fractionnée sur les iPad et iPad Pro. Grâce à la vue fractionnée, Citrix Receiver pour iOS vous permet d'ouvrir deux applications simultanément et de les afficher côte à côte. Lorsqu'elle est utilisée en conjonction avec XenApp ou XenDesktop, cette fonctionnalité améliore la productivité en vous permettant d'utiliser votre iPad en tant que remplacement de votre poste de travail, particulièrement lorsqu'elle est combinée avec d'autres périphériques, tels qu'un clavier logiciel, la souris X1 ou l'Apple Pencil.

Améliorations supplémentaires apportées dans cette version

Cette version contient les fonctionnalités et améliorations suivantes :

- Prise en charge dans la session des cartes à puce SITHS
- Possibilité d'activer l'option caffeine (ce qui empêche un iPad d'entrer en mode veille) avant d'ajouter un magasin
- Prise en charge de WebFront (pour StoreFront non authentifié)

> **Remarque**
>
> Citrix Receiver pour iOS 6.1.5 fonctionne avec iOS 9.3.

Prise en charge de iOS 9.

Vous informe lorsqu'un appareil iOS a été jailbreaké et vous permet d'empêcher les appareils jailbreakés d'exécuter des applications via StoreFront ou l'Interface Web. Vous pouvez en apprendre davantage sur cette nouvelle fonctionnalité ici : Bloquer les appareils jailbreakés.

Citrix Receiver pour iOS 6.1.1 et 6.1.2 ne contiennent aucune nouvelle fonctionnalité autres que celles incluses dans 6.1.0, mais ils contiennent des corrections.

La version de maintenance de Citrix Receiver pour iOS 6.1.3 contient un certain nombre de corrections et d'améliorations, notamment :

- Améliorations apportées à la compatibilité avec l'iPad Pro, avec prise en charge du clavier à l'écran sur l'iPad Pro.
- Recherche Spotlight iOS de contenu d'applications publiées ; grâce à cette fonctionnalité, vous pouvez rechercher des applications et des bureaux publiés à l'aide du mécanisme de recherche Spotlight.
- Contrôle de la vitesse de la souris X1 ; un paramètre dans Citrix Receiver vous permet de personnaliser la vitesse de la souris X1.

La version de maintenance de Citrix Receiver pour iOS 6.1.3 résout les problèmes suivants :

- Résolution d'un problème d'authentification avec une stratégie NetScaler. [#616573]
- Résolution d'un problème lié à un blocage inattendu lors de la déconnexion d'une session. [#616611]

> **Remarque**
>
> Pour de plus amples informations sur les corrections apportées à la version 6.1.0 (et au-delà) reportez-vous aux listes des problèmes résolus plus loin dans cet article.

Cette version prend en charge le canal virtuel Framehawk, un nouveau canal virtuel ICA qui étend les technologies HDX Citrix afin d'améliorer l'expérience utilisateur sur les connexions sans fil haut débit dans lesquelles la perte de paquets et la latence sont des problèmes courants. Pour de plus amples informations, consultez la section Nouveautés dans XenApp 7.6 et XenDesktop 7.6. Lors de l'utilisation de la fonctionnalité Framehawk :

- Le protocole CGP (Common Gateway Protocol) doit être activé.
- Dans le fichier de modèle ICA, ajoutez « Framehawk=yes ».

Malgré l'activation du protocole CGP pour la connexion aux sessions Framehawk, la fiabilité de session n'est pas disponible.

Receiver pour iOS 6.0 prend désormais en charge le 64 bits avec le SDK iOS 8, inclus dans Xcode 6 ou version ultérieure. Tenez compte de ce qui suit lors de l'utilisation de cette fonctionnalité : les appareils iOS équipés de puces Apple A7 et Apple A8 contiennent des puces 64 bits, ce qui comprend :

- iPhone 5S ou plus récent
- iPad Air ou plus récent
- iPad Mini 2 ou plus récent

- Résolution d'un problème dans lequel le lancement d'une application échouait.
- Nombreux scénarios de test supplémentaires utilisés pour vérifier l'intégrité
- Métriques supplémentaires capturés pour améliorer l'expérience utilisateur

- Résolution d'un problème d'authentification avec une stratégie NetScaler. [#616573]
- Résolution d'un problème lié à un blocage inattendu lors de la déconnexion d'une session. [#616611]

- Résolution d'un problème lié aux fuseaux horaires.
- Résolution de plusieurs problèmes qui entraînaient le blocage de sessions.

- Résolution d'un problème dans lequel les utilisateurs ne pouvaient pas se reconnecter à leurs comptes après s'être déconnectés manuellement ou lorsque le délai d'inactivité des sessions était dépassé.
  [#600659]
- Workflow d'authentification du jeton RSA amélioré de façon à ce que les utilisateurs ne soient plus invités à fournir leur jeton à deux reprises.
  [#597857]
- Résolution d'un problèmes de compatibilité qui empêchait les utilisateurs de s'authentifier auprès de leurs magasins lors de l'utilisation de NetScaler 11.0 en tant que passerelle.
  [#558212]
- Résolution d'un problème lié à la résolution de l'écran iPad Pro.

- Résolution d'un problème dans lequel Citrix Receiver ne parvenait pas à se connecter à un compte via Netscaler Gateway quand le nom commun dans le certificat était aussi son adresse IP.
  [#594157]
- Résolution d'un problème dans lequel Citrix Receiver affichait continuellement « Veuillez patienter... » après l'ajout d'un compte.
  [#595978]
- Résolution d'un problème dans lequel lorsque le niveau de journalisation était défini sur Débogage, Citrix Receiver se

bloquait après utilisation de l'option « Demander l'aide de l'assistance. »
[#595980]

- Résolution d'un problème dans lequel une application se bloquait après avoir été redémarrée.
[#596993]

- Résolution d'un problème dans lequel Citrix Receiver ne reconnaissait pas certains certificats de carte à puce.
[#587428]
- Résolution d'un problème relatif à la reconnexion ou au basculement vers une session VDA Linux.
[#558369]
- Améliorations d'ordre général apportées aux jetons logiciels et aux certificats clients.
[#586361]

Nous avons corrigé plusieurs problèmes liés à l'utilisation sur iOS 9 :

- Le dock du clavier étendu ne s'affichait pas au bon endroit lors de l'utilisation d'un clavier Bluetooth.
[#579307]
- Les nouveaux boutons d'annulation et de restauration sur iOS9 n'étaient pas complètement fonctionnels.
[#579318]
- Les clics de la souris Citrix X1 ne portaient pas le focus sur les champs de texte lors de l'utilisation d'un clavier Bluetooth. Appuyez plutôt sur le champ du texte.
[#579362]
- Le clavier s'affichait de façon anormale après l'activation et la désactivation du bouton Utiliser le clavier Unicode dans la session.
[#579496]
- La liste des touches étendues et le clavier Citrix se chevauchaient en mode paysage.
[#580117]
- Le sélecteur d'applications affichait des aperçus de façon anormale après la rotation de l'appareil.
[#580980]
- La session ne répondait plus après l'utilisation de la saisie vocale Siri à partir du clavier.
[#582046]

- Receiver se plantait lors du lancement d'une application transparente.
[#584383]
- Vous pouvez maintenant accéder aux paramètres de la souris Citrix X1 sans avoir à créer de compte.
[#587422]
- Un jeton RSA ne pouvait pas être lu par Receiver.
[#587423]
- Il n'était pas possible d'ajouter des comptes StoreFront via NetScaler lors de l'utilisation de webfront.
[#587426]
- Les cartes à puce ne reconnaissaient pas les certificats.

[#587428]

- Lorsqu'un nouveau mot de passe est défini, une erreur « Infos d'identification incorrectes » s'affiche.Malgré ce message d'erreur, le nouveau mot de passe est correctement défini. Le message d'erreur peut être ignoré. Utilisez le nouveau mot de passe lors de la prochaine ouverture de session. [#70576123]

- Citrix Receiver peut ne pas parvenir à lancer une session avec une carte à puce via NetScaler Gateway après la fermeture de session.
  [#586984]
- Il est possible qu'une erreur de type échec de connexion s'affiche après la fermeture d'une session à l'aide d'une carte à puce.
  [#577175]
- Citrix Receiver ne parvient pas à lire une carte à puce lors de l'envoi d'un e-mail crypté par un certificat de carte à puce.
  [#587869]
- Citrix Receiver affiche une erreur lors de l'ajout d'un compte StoreFront via NetScaler Gateway par le biais de la configuration manuelle.
  [#590576]

Si vous exécutez Citrix Receiver pour iOS 6.0 ou 6.0.1 sur iOS 9, vous pouvez rencontrer les problèmes suivants :

- Le dock du clavier étendu ne s'affichait pas au bon endroit lors de l'utilisation d'un clavier Bluetooth.
  [#579307]
- Les nouveaux boutons d'annulation et de restauration sur iOS9 n'étaient pas complètement fonctionnels.
  [#579318]
- Les clics de la souris Citrix X1 ne portaient pas le focus sur les champs de texte lors de l'utilisation d'un clavier Bluetooth. Appuyez plutôt sur le champ du texte.
  [#579362]
- Le clavier s'affichait de façon anormale après l'activation et la désactivation du bouton Utiliser le clavier Unicode dans la session.
  [#579496]
- La liste des touches étendues et le clavier Citrix se chevauchaient en mode paysage.
  [#580117]
- Le sélecteur d'applications affichait des aperçus de façon anormale après la rotation de l'appareil.
  [#580980]
- La session ne répondait plus après l'utilisation de la saisie vocale Siri à partir du clavier.
  [#582046]

- Si vous utilisez une application CMP et que Receiver est configuré pour utiliser une résolution fixe, la résolution de la session n'est pas correcte. Pour résoudre ce problème, utilisez l'option Ajuster à l'écran lors de la configuration de la résolution d'écran.

[#574443]

- Lors de l'utilisation d'une carte à puce pour l'authentification, Receiver ne parvient pas à fermer la session correctement ; après fermeture de la session, le bureau semble toujours actif.
  [#577175]
- Lorsque vous définissez une résolution d'écran fixe, il est possible que le curseur de la souris se déplace au-delà des limites de l'écran.
  [#578081]
- Lorsque vous utilisez NetScaler et que certaines stratégies graphiques sont appliquées, Receiver peut déconnecter une session lorsqu'une vidéo 1080p est lue.
  [#569392]
- Dans certains cas dans lesquels la stratégie de canal virtuel Framehawk est appliquée, une session peut afficher de faibles performances lors de l'exécution de certaines combinaisons de touches utilisant la touche MAJ ; les caractères suivants sont concernés : %, #, :, !, ?. Pour résoudre ce problème, Citrix recommande de déconnecter puis de reconnecter la session.
  [#570236]
- Lors de l'utilisation de l'authentification par carte à puce, Receiver peut ne pas afficher correctement l'écran d'ouverture de session demandant la saisie du code PIN de l'utilisateur après la fermeture de session. Par ailleurs, la fermeture de session suivie de l'ajout d'une application favorite échoue ; Receiver affiche une erreur indiquant que la session n'a pas pu être redémarrée car l'utilisateur n'a pas pu se connecter.
  [#555804, #556580]
- Receiver peut ne pas parvenir à se reconnecter à une session VDA sur Linux.
  [#558369]
- Dans un environnement en langue chinoise, Receiver peut se planter lors de l'insertion de certains symboles (“{“ ou “}”) dans la zone de recherche des applications.
  [#578322]

Configuration système requise pour Citrix Receiver pour iOS 6

Jan 29, 2016

Dans cet article :

- Citrix Receiver pour 6.1, 6.1.1 et 6.1.2 prend en charge iOS 7, 8 et 9.
- Citrix Receiver pour iOS 6.0 et 6.0.1 prend en charge iOS 7, 8 et 9 (quelques problèmes connus).
- Cette mise à jour logicielle est prise en charge sur les appareils suivants :
  - iPhone 4, 4S, 5, 5c, 5s, 6, 6 Plus, 6s et 6s Plus.
  - Tous les modèles d'iPad (y compris le iPad Pro). La prise en charge de l'iPad Pro ne comprend pas :
    - Apple Pencil
    - Vue fractionnée
    - Clavier logiciel natif
  - iPod Touch de 5ème génération.
- Prise en charge de moniteurs externes
  - iPhone - si pris en charge par iOS.
  - iPad - si pris en charge par iOS (n'utilise pas l'écran entier).

Important

Pour de plus amples informations sur la sécurisation des connexions à votre environnement Citrix, consultez la section Connectivité et authentification (ci-dessous).

Pour de plus amples informations sur les problèmes liés à l'exécution de Citrix Receiver 6.0 et 6.0.1 sur iOS 9, consultez Prise en charge d'iOS 9.

Assurez-vous d'installer toutes les dernières corrections à chaud pour vos serveurs.

- Pour les connexions aux applications et bureaux virtuels, Citrix Receiver prend en charge Citrix StoreFront et l'Interface Web.
  StoreFront :
  - StoreFront 3.0 (recommandé)
    Permet d'accéder directement aux magasins StoreFront. Receiver prend également en charge les versions antérieures de StoreFront.

Remarque : cette version de Receiver pour iOS comprend le canal virtuel Framehawk. Cette version s'intègre avec la dernière version de StoreFront 3.0. Pour profiter de cette nouvelle fonctionnalité, Citrix recommande d'installer la dernière version de StoreFront.

- StoreFront configuré avec un site Receiver pour Web
  Permet d'accéder aux magasins StoreFront à partir d'un navigateur Web Safari. Les utilisateurs doivent ouvrir le fichier ICA manuellement à l'aide de la fonction Ouvrir dans du navigateur. Pour prendre connaissance des limitations de ce déploiement, consultez la documentation StoreFront.

Interface Web :

- Interface Web 5.4 avec des sites Interface Web
- Interface Web 5.4 avec des sites XenApp Services
- Interface Web sur NetScaler (accès par navigateur Safari uniquement)
  Vous devez activer les stratégies de réécriture fournies par NetScaler.

- **XenDesktop** et **XenApp** (l'un des produits suivants) :
  - Citrix XenDesktop 4, 5, 5.5, 5.6, 7, 7.x, 7.5 et 7.6
  - Citrix XenApp 7.5 et 7.6
  - Citrix XenApp 6.5 pour Windows Server 2008 R2
  - Citrix XenApp 6 pour Windows Server 2008 R2
  - Citrix XenApp Fundamentals 6.0 pour Windows Server 2008 R2
  - Citrix XenApp 5 pour Windows Server 2008
  - Citrix XenApp 5 pour Windows Server 2003
  - Citrix Presentation Server 4.5
- VDI-in-a-Box 5.2.x et 5.3.x

Pour les connexions à StoreFront, Receiver prend en charge les méthodes d'authentification suivantes :

	Receiver pour Web à l'aide de navigateurs	Site StoreFront Services (natif)	Site StoreFront XenApp Services (natif)	NetScaler sur Receiver pour Web (navigateur)	NetScaler sur site StoreFront Services (natif)
Anonyme	Oui	Oui			
Domaine	Oui	Oui	Oui	Oui*	Oui*
Authentification unique au domaine	Oui	Oui	Oui		
Jeton de sécurité				Oui*	Oui*
Deux facteurs (domaine avec jeton de sécurité)				Oui*	Oui*

SMS Cartes à puce	Receiver pour Web à l'aide de navigateurs	Site StoreFront Services (natif) Oui	Site StoreFront XenApp Services (natif)	NetScaler sur Receiver pour Web (navigateur) Oui*	NetScaler sur site StoreFront Services (natif) Non Oui*
Certificat utilisateur				Oui (NetScaler Gateway Plugin)	Oui (NetScaler Gateway Plugin)

*Uniquement disponible pour les sites Receiver pour Web et les déploiements qui contiennent NetScaler Gateway, avec ou sans installation du plug-in associé sur la machine.

Pour de plus amples informations sur les versions de NetScaler Gateway et d'Access Gateway prises en charge par StoreFront, reportez-vous à la documentation NetScaler Gateway, Access Gateway et StoreFront.

Pour les connexions à l'Interface Web 5.4, Receiver prend en charge les méthodes d'authentification suivantes :
Remarque : l'Interface Web utilise le terme Explicite pour représenter l'authentification par jeton de sécurité et domaine.

	Interface Web (navigateurs)	Site Interface Web XenApp Services	NetScaler sur l'Interface Web (navigateur)	NetScaler sur un site Interface Web XenApp Services
Anonyme	Oui			
Domaine	Oui	Oui	Oui*	
Authentification unique au domaine	Oui			
Jeton de sécurité			Oui*	
Deux facteurs (domaine avec jeton de sécurité)			Oui*	
SMS			Oui*	
Cartes à puce**				
Certificat utilisateur			Oui (requiert NetScaler Gateway Plugin)	

À propos des connexions sécurisées et des certificats

Certificats privés (auto-signés)

Si un certificat privé est installé sur la passerelle distante, le certificat racine de l'autorité de certification doit être installé sur

l'appareil de façon à pouvoir accéder aux ressources Citrix à l'aide de Citrix Receiver.

Remarque : si le certificat de la passerelle distante ne peut pas être vérifié lors de la connexion (car le certificat racine n'est pas inclus dans le magasin de clés), un avertissement relatif à un certificat non approuvé s'affiche. Si un utilisateur choisit d'ignorer l'avertissement, une liste des applications s'affiche ; toutefois, les applications ne démarrent pas.

Importation de certificats racine sur iPad et iPhone

Obtenez le certificat racine auprès de l'émetteur du certificat et envoyez-le par e-mail à un compte de messagerie configuré sur votre appareil. Lorsque vous cliquez sur la pièce jointe, vous êtes invité à importer le certificat racine.

Certificats génériques

Les certificats génériques remplacent les certificats de serveur individuel pour n'importe quel serveur situé dans le même domaine. Citrix Receiver pour iOS prend en charge les certificats génériques.

Certificats intermédiaires et NetScaler Gateway

Si votre chaîne de certificat contient un certificat intermédiaire, ce dernier doit être ajouté au certificat du serveur NetScaler Gateway (ou Access Gateway). Pour de plus amples informations sur l'installation de certificats intermédiaires dans NetScaler Gateway ou Access Gateway, consultez la documentation dans eDocs. De plus, pour les installations Access Gateway, consultez l'article de la base de connaissances qui correspond à votre édition :

CTX114146 : comment installer un certificat intermédiaire sur Access Gateway édition Enterprise

Voir aussi :

CTX124937 : comment configurer Access Gateway édition Enterprise pour l'utiliser avec Citrix Receiver pour appareils mobiles

L'authentification RSA SecurID est prise en charge pour les configurations Secure Gateway (via l'Interface Web uniquement) et toutes les configurations Access Gateway prises en charge.

Receiver prend en charge toutes les méthodes d'authentification prises en charge par Access Gateway. Pour de plus amples informations sur l'authentification, reportez-vous à la documentation NetScaler Gateway (ou Access Gateway) et aux rubriques figurant sous la section « Gérer » dans la documentation StoreFront de eDocs. Pour de plus amples informations sur les autres méthodes d'authentification prises en charge par l'Interface Web, reportez-vous à la rubrique « Configuration de l'authentification pour l'Interface Web » dans la documentation Interface Web.

Citrix Receiver offre une prise en charge limitée des cartes à puce.

Si vous utilisez des périphériques NetScaler certifiés FIPS, configurez vos systèmes afin de refuser les renégociations SSL. Pour de plus amples informations, consultez la section Comment configurer le paramètre -denySSLReneg.
Les configurations et produits suivants sont pris en charge :

- Lecteurs pris en charge :
  - Precise Biometrics Tactivo pour iPad Mini Firmware version 3.8.0
  - Precise Biometrics Tactivo pour iPad (4ème génération) et Tactivo pour iPad (3ème génération) et iPad 2 Firmware version 3.8.0
  - Lecteurs de carte à puce BaiMobile® 301MP et 301MP-L

  Middleware de carte à puce VDA pris en charge
- ActiveIdentity

- Cartes à puce prises en charge :
  - Cartes PIV
  - Cartes CAC
- Configurations prises en charge :
  - Authentification par carte à puce à NetScaler Gateway avec StoreFront 2.x et XenDesktop 5.6 et version supérieure ou XenApp 6.5 et version supérieure.

Configurer votre environnement

Jan 29, 2016

Receiver prend en charge la configuration de l'Interface Web pour votre déploiement XenApp. Il existe deux types de sites Interface Web : les sites XenApp Services (anciennement Program Neighborhood Services) et les sites XenApp Web. Les sites Interface Web permettent aux machines clientes de se connecter à la batterie de serveurs. Plusieurs solutions permettent d'assurer l'authentification entre Receiver et un site Interface Web, notamment Citrix Access Gateway et Citrix Secure Gateway.

Par ailleurs, vous pouvez configurer StoreFront de manière à fournir des services d'authentification et de mise à disposition de ressources pour Receiver, ce qui vous permet de créer de façon centralisée des magasins d'entreprise destinés à délivrer des bureaux, applications ainsi que d'autres ressources aux utilisateurs.

Pour plus d'informations sur la configuration des connexions, y compris des vidéos, des blogs et un forum d'assistance, connectez-vous à http://community.citrix.com.

Avant d'autoriser vos utilisateurs à accéder aux applications hébergées sur votre déploiement XenApp ou XenDesktop, configurez les composants suivants dans votre déploiement comme indiqué ci-dessous.

- Lors de la publication d'applications sur vos batteries ou sites, envisagez les options suivantes pour améliorer l'expérience des utilisateurs qui accèdent aux applications par le biais des magasins StoreFront.
  - Veillez à inclure des descriptions claires des applications publiées, car ces descriptions sont consultées par les utilisateurs dans Citrix Receiver.
  - Vous pouvez augmenter la visibilité des applications publiées auprès des utilisateurs d'appareils mobiles en répertoriant les applications dans la liste Sélection de Citrix Receiver. Pour renseigner cette liste sur Citrix Receiver, modifiez les propriétés des applications publiées sur vos serveurs et ajoutez la chaîne KEYWORDS:Featured au champ Description de l'application.
  - Pour que le mode Ajuster à l'écran puisse adapter l'application à la taille de l'écran des appareils mobiles, modifiez les propriétés des applications publiées sur vos serveurs et ajoutez la chaîne KEYWORDS:mobile au champ Description de l'application. Ce mot-clé active également la fonctionnalité de défilement automatique pour l'application.
  - Pour abonner automatiquement tous les utilisateurs d'un magasin à une application, ajoutez la chaîne KEYWORDS:Auto à la description que vous fournissez lors de la publication de l'application dans XenApp. Lorsque les utilisateurs ouvrent une session dans le magasin, l'application est automatiquement provisionnée sans qu'ils aient à y souscrire manuellement.

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

- Si l'Interface Web de votre déploiement XenApp ou XenDesktop ne dispose ni d'un site Web, ni d'un site XenApp Services, créez-en un. Le nom du site et sa méthode de création dépendent de la version de l'Interface Web que vous avez installée. Pour obtenir des instructions sur la création de l'un de ces sites, consultez la rubrique « Création de sites » correspondant à votre version de l'Interface Web.

Configurer StoreFront.

Jan 29, 2016

Remarque :

- Lors de l'utilisation de StoreFront, Receiver prend en charge Citrix Access Gateway Enterprise Edition à partir de la version 9.3, et NetScaler Gateway jusqu'à la version 11.
- Receiver pour iOS prend uniquement en charge les sites XenApp Services sur l'Interface Web.
- Receiver pour iOS prend en charge le lancement de sessions à partir de Receiver pour Web, à condition que le navigateur Web fonctionne avec Receiver pour Web. Si le lancement échoue, configurez votre compte directement via Receiver pour iOS. Les utilisateurs doivent ouvrir le fichier ICA manuellement à l'aide de la fonction Ouvrir dans du navigateur. Pour prendre connaissance des limitations de ce déploiement, consultez la documentation StoreFront.

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

1. Installez et configurez StoreFront. Pour de plus amples informations, consultez la rubrique StoreFront dans la section Technologies > StoreFront de eDocs. Pour les administrateurs soucieux d'exercer un contrôle plus rigoureux, Citrix fournit un modèle que vous pouvez utiliser pour créer un site de téléchargement pour Receiver pour iOS.
2. Configurez des magasins pour StoreFront comme vous le feriez pour toute autre application XenApp ou XenDesktop. Aucune configuration spéciale n'est nécessaire pour les appareils mobiles. Pour plus de détails, consultez la section *— Options d'accès utilisateur* dans la section StoreFront de eDocs. Pour les appareils mobiles, utilisez l'une de ces méthodes :
   - Fichier de provisioning. Vous pouvez fournir aux utilisateurs des fichiers de provisioning (.cr) contenant les informations nécessaires pour se connecter aux magasins. Après l'installation, les utilisateurs ouvrent le fichier sur leur appareil configurer automatiquement Citrix Receiver. Par défaut, les sites Receiver pour Web offrent aux utilisateurs un fichier de provisioning destiné au magasin pour lequel le site est configuré. Alternativement, vous pouvez utiliser la console de gestion Citrix StoreFront pour générer des fichiers de provisioning pour des magasins uniques ou multiples que vous distribuez manuellement à vos utilisateurs.
   - Configuration manuelle. Vous pouvez informer directement les utilisateurs des adresses URL d'Access Gateway ou de magasin nécessaire à l'accès à leurs bureaux ou applications. Pour les connexions via Access Gateway, les utilisateurs doivent également connaître l'édition du produit et la méthode d'authentification requise. Après installation, les utilisateurs entrent ces détails dans Citrix Receiver, qui tente de vérifier la connexion et, si réussi, invite les utilisateurs à ouvrir une session.
   - Configuration automatique. Appuyez sur **Ajouter un compte** sur l'écran de bienvenue et entrez l'URL du serveur StoreFront dans le champ d'adresse. Le compte est configuré lorsqu'il est ajouté.

Pour configurer Access Gateway et NetScaler Gateway

Si certains de vos utilisateurs se connectent en dehors du réseau interne (par exemple, les utilisateurs qui se connectent via Internet ou à partir d'emplacements distants), configurez l'authentification via NetScaler Gateway ou Access Gateway.

- Lors de l'utilisation de StoreFront, Receiver prend en charge Citrix Access Gateway Enterprise Edition à partir de la version 9.3, et NetScaler Gateway jusqu'à la version 11.
- Pour de plus amples informations, consultez la rubrique correspondant à votre version d'Access Gateway ou de NetScaler

Gateway dans eDocs.

1. Si vous voulez configurer Receiver de manière à accéder directement aux applications lors de la création d'un nouveau compte, dans le champ Adresse, entrez l'adresse URL de votre magasin, telle questorefront.organisation.com.
2. Sélectionnez l'option Utiliser carte à puce si vous utilisez une carte à puce pour l'authentification.
3. Pour une configuration manuelle (accessible en appuyant sur Options > Installation manuelle), continuez en renseignant les champs restants et sélectionnez la méthode d'authentification à Access Gateway (ou NetScaler Gateway), telle que l'activation du jeton de sécurité, le choix du type d'authentification et l'enregistrement des paramètres.

Remarque : les ouvertures de session sur le magasin sont valides pendant environ une heure. Une fois cette période écoulée, les utilisateurs doivent de nouveau ouvrir une session pour actualiser ou lancer d'autres applications.

Configurer l'authentification du certificat client

Jan 29, 2016

Remarque :

- Lors de l'utilisation de StoreFront, Receiver prend en charge Citrix Access Gateway Enterprise Edition à partir de la version 9.3, et NetScaler Gateway jusqu'à la version 11.
- L'authentification du certificat client est prise en charge par Receiver pour iOS à partir de la version 5.5.
- Seules les éditions 9.x et 10.x (et les versions ultérieures) d'Access Gateway Enterprise prennent en charge l'authentification du certificat client.
- Les types d'authentification double doivent être CERT et LDAP.
- Receiver prend également en charge l'authentification facultative du certificat client.
- Seuls les certificats P12 sont pris en charge.

Les utilisateurs qui ouvrent une session sur un serveur virtuel Access Gateway (ou NetScaler Gateway) peuvent également être authentifiés en fonction des attributs du certificat client qui est présenté au serveur virtuel. L'authentification du certificat client peut également être utilisée avec un autre type d'authentification, à savoir LDAP, afin de fournir une authentification double.

Pour authentifier les utilisateurs en fonction des attributs du certificat du côté client, l'authentification du client doit être activée sur le serveur virtuel et le certificat client doit être demandé. Vous devez lier un certificat racine au serveur virtuel sur Access Gateway.

Lorsque les utilisateurs ouvrent une session sur le serveur virtuel Access Gateway, après l'authentification, les informations sur le nom d'utilisateur et le domaine sont extraites à partir du champ spécifié du certificat. Ces informations doivent figurer dans le champ **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** du certificat. Elles sont au format « nomd'utilisateur@domaine ». Si le nom d'utilisateur et le domaine sont extraits avec succès, et que l'utilisateur fournit les autres informations requises (par exemple un mot de passe), l'utilisateur est authentifié. Si l'utilisateur ne fournit pas un certificat et des informations d'identification valides, ou si l'extraction du nom d'utilisateur/domaine échoue, l'authentification échoue.

Si c'est l'utilisateur qui fournit le nom d'utilisateur et le domaine plutôt que le certificat (approche plus sécurisée), supprimez le champ **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** du certificat client.

Vous pouvez authentifier les utilisateurs en fonction du certificat client en définissant le type d'authentification par défaut de manière à utiliser le certificat client. Vous pouvez également créer une action de certificat dont la tâche est de définir les opérations à réaliser durant l'authentification basée sur un certificat client SSL.

Si vous n'avez pas encore créé de site XenApp Services, créez-en un pour les appareils mobiles dans la console XenApp ou la console Interface Web (en fonction de la version de XenApp que vous avez installée).

Receiver pour appareils mobiles utilise un site XenApp Services (anciennement appelé site Agent Program Neighborhood) pour obtenir des informations sur les applications auxquelles un utilisateur est autorisé à accéder et les présenter au logiciel Receiver exécuté sur l'appareil. Ce processus est similaire à la manière dont vous utilisez l'Interface Web pour les connexions XenApp SSL traditionnelles pour lesquelles une passerelle Access Gateway peut être configurée.

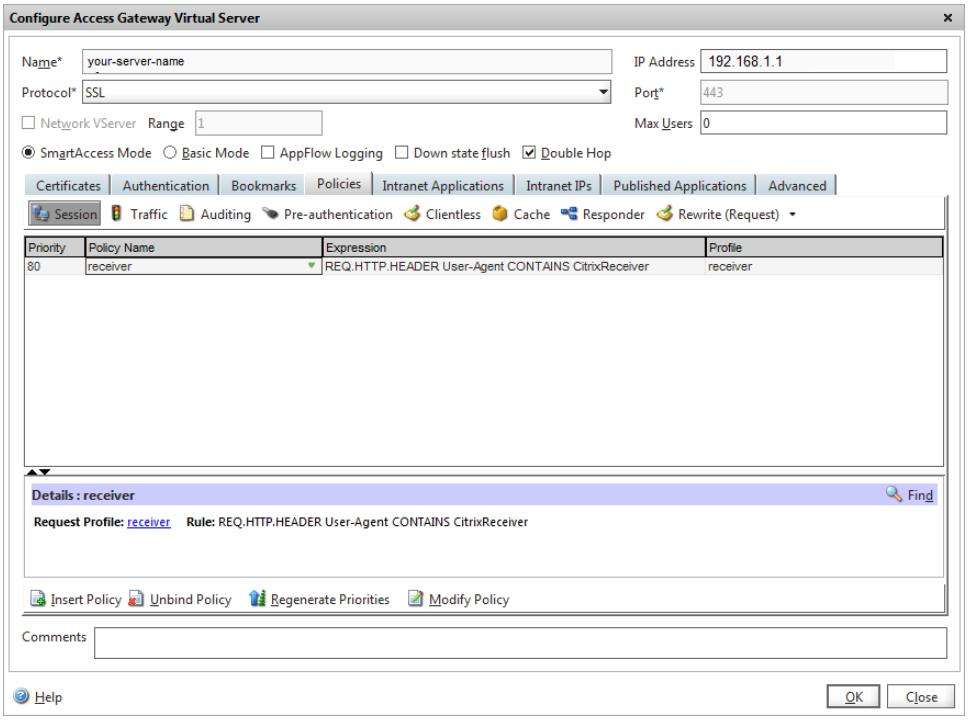
Configurez le site XenApp Services pour Receiver pour appareils mobiles afin de prendre en charge les connexions en provenance d'Access Gateway.

1. Dans le site XenApp Services, sélectionnez Gérer l'accès client sécurisé > Modifier les paramètres d'accès au client sécurisé.
2. Dans Méthode d'accès, choisissez Passerelle directe.
3. Entrez le nom de domaine complet du boîtier Access Gateway.
4. Entrez les informations de Secure Ticket Authority (STA).

Pour l'authentification du certificat client, configurez Access Gateway avec l'authentification à deux facteurs à l'aide de deux stratégies d'authentification : Cert et LDAP. Pour de plus amples informations, reportez-vous à la version d'Access Gateway édition Enterprise (9.x uniquement) ou Access Gateway 10 dans eDocs et accédez à la rubrique :
— Configuration de l'authentification du certificat client
.

1. Créez une stratégie de session sur Access Gateway de manière à autoriser les connexions XenApp entrantes provenant du Receiver, et spécifiez l'emplacement du site XenApp Services que vous venez de créer.
   - Créez une nouvelle stratégie de session pour identifier Receiver pour appareils mobiles comme étant à l'origine de la connexion. Lors de la création de la stratégie de session, configurez l'expression suivante et sélectionnez Match All Expressions en tant qu'opérateur de l'expression :

     REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver



   - Dans la configuration de profil associé pour la stratégie de session, sur l'onglet Security, définissez Default Authorization sur Allow.
     Sur l'onglet Published Applications, s'il ne s'agit pas d'un paramètre global (vous avez coché la case Override Global), assurez-vous que la valeur ON est attribuée au champ ICA Proxy.

     Dans le champ Web Interface Address, entrez l'adresse URL, y compris le fichier config.xml pour le site XenApp Services que les utilisateurs de l'appareil utilisent, telle que http://XenAppServerName/Citrix/PNAgent/config.xml ou

http://XenAppServerName/CustomPath/config.xml.

- Associez la stratégie de session à un serveur virtuel.
- Créez des stratégies d'authentification pour Cert et LDAP.
- Associez les stratégies d'authentification au serveur virtuel.
- Configurez le serveur virtuel afin de demander des certificats clients dans la négociation TLS (sur l'onglet Certificate, ouvrez SSL Parameters, et pour Client Authentication, définissez Client Certificate sur Mandatory.
  Important : si le certificat de serveur utilisé sur Access Gateway fait partie d'une chaîne de certificats (avec un certificat intermédiaire), assurez-vous que les certificats intermédiaires sont également installés sur Access Gateway. Pour de plus amples informations sur l'installation de certificats, consultez la documentation Access Gateway.

Si l'authentification du certificat client est activée sur Access Gateway, les utilisateurs sont authentifiés en fonction de certains attributs du certificat client. Une fois l'authentification terminée, le nom d'utilisateur et le domaine sont extraits du certificat et les stratégies spécifiées pour cet utilisateur sont appliquées.

1. À partir de Receiver, ouvrez Compte, et dans le champ Serveur, entrez le nom de domaine complet de votre serveur Access Gateway, tel queServeurCertificatClientGateway.organisation.com. Receiver détecte automatiquement que le certificat client est requis.
2. Deux choix se présentent à l'utilisateur: il peut soit installer un nouveau certificat, soit en sélectionner un dans la liste des certificats déjà installés. Pour l'authentification du certificat client iOS, le certificat doit uniquement être téléchargé et installé par l'application Receiver.
3. Après avoir sélectionné un certificat valide, les champs nom d'utilisateur et domaine de l'écran d'ouverture de session sont renseignés avec le nom d'utilisateur provenant du certificat, et l'utilisateur entre les informations restantes, y compris le mot de passe.
4. Si l'authentification du certificat client est définie sur Facultative, les utilisateurs peuvent ignorer la sélection du certificat en appuyant sur le bouton Précédent de la page des certificats. Dans ce cas, Receiver établit la connexion et affiche l'écran d'ouverture de session.
5. Ceci fait, les utilisateurs peuvent lancer des applications sans avoir à fournir le certificat. Receiver stocke le certificat du compte et l'utilise automatiquement lors des ouvertures de session suivantes.

Configurer Secure Gateway

Jan 29, 2016

Remarque :

- Secure Gateway 3.x est pris en charge par Receiver pour iOS à l'aide de sites XenApp Services.
- Secure Gateway 3.x est pris en charge par Receiver pour iOS à l'aide de sites Web XenApp.
- Seule l'authentification à un facteur est prise en charge sur les sites XenApp Services. L'authentification à un facteur et l'authentification à deux facteurs sont toutes les deux prises en charge sur les sites XenApp Web.
- Vous devez utiliser l'Interface Web 5.4, qui est prise en charge par tous les navigateurs intégrés.

Avant de commencer la configuration, installez et configurez Secure Gateway de sorte qu'elle fonctionne avec l'Interface Web. Vous pouvez modifier ces instructions afin de les adapter à votre environnement spécifique.

Si vous utilisez une connexion Secure Gateway, ne configurez pas les paramètres Citrix Access Gateway sur le Receiver.

Receiver pour appareils mobiles utilise un site XenApp Services (anciennement appelé site Agent Program Neighborhood) pour obtenir des informations sur les applications auxquelles un utilisateur est autorisé à accéder et les présenter au logiciel Receiver exécuté sur l'appareil. Ce processus est similaire à la manière dont vous utilisez l'Interface Web pour les connexions XenApp SSL traditionnelles pour lesquelles une passerelle Access Gateway peut être configurée. Cette capacité de configuration est intégrée aux sites XenAppServices exécutés sur l'Interface Web 5. x.

Configurez le site XenApp Services pour prendre en charge des connexions provenant d'une connexion Secure Gateway :

1. Dans le site XenApp Services, sélectionnez Gérer l'accès client sécurisé > Modifier les paramètres d'accès au client sécurisé.
2. Dans Méthode d'accès, choisissez Passerelle directe.
3. Entrez le nom de domaine complet du boîtier Secure Gateway.
4. Entrez les informations de Secure Ticket Authority (STA).
   Remarque : pour Secure Gateway, Citrix recommande d'utiliser le chemin d'accès par défaut Citrix pour ce site (http://NomServeurXenApp/Citrix/PNAgent). Le chemin d'accès par défaut permet à vos utilisateurs de spécifier le nom de domaine complet de la passerelle Secure Gateway à laquelle ils se connectent plutôt que le chemin d'accès complet au fichier config.xml qui réside sur le site XenApp Services (tel quehttp://NomServeurXenApp/Cheminpersonnalisé/config.xml).

1. Sur Secure Gateway, utilisez l'assistant de configuration de Secure Gateway pour configurer Secure Gateway de manière à fonctionner avec le serveur du réseau sécurisé qui héberge le site XenApp Services. Après avoir sélectionné l'option Indirect, entrez le chemin d'accès du nom de domaine complet de votre serveur Secure Gateway et complétez les étapes suivantes de l'assistant.
2. Testez une connexion à partir d'une machine utilisateur pour vous assurer que Secure Gateway est correctement configuré en termes de réseau et d'allocation de certificat.

1. Lors de l'ajout d'un compte Secure Gateway, entrez le nom de domaine complet correspondant de votre serveur Secure Gateway dans le champ **Adresse** :

- Si vous avez créé le site XenApp Services à l'aide du chemin par défaut (/Citrix/PNAgent), entrez le FQDN de Secure Gateway :https://FQDNdeSecureGateway.nomd'entreprise.com
- Si vous avez personnalisé le chemin d'accès au site XenApp Services, entrez le chemin d'accès complet au fichier config.xml, tel que :https://FQDNdeSecureGateway.nomd'entreprise.com/CheminPersonnalisé/config.xml

2. Si vous configurez manuellement le compte, désactivez l'option Access Gateway **Nouveau compte**.

Configurer Access Gateway édition Enterprise

Jan 29, 2016

Remarque :

- Access Gateway édition Enterprise 9.x et 10.x sont pris en charge par Receiver pour iOS à l'aide des sites XenApp Services ou des sites d'ancienne génération sur les serveurs StoreFront.
- Access Gateway édition Enterprise 9.x et 10.x sont pris en charge par Receiver pour iOS à l'aide des sites Web XenApp.
- Receiver pour Web n'est pas pris en charge par les Receiver pour iOS.
- Access Gateway édition Enterprise 9.x et 10.x sont pris en charge par Receiver pour iOS pour accéder aux magasins StoreFront.
- L'authentification à source unique et l'authentification à double source sont toutes les deux prises en charge sur les sites Interface Web et StoreFront.
- Vous devez utiliser l'Interface Web 5.4, qui est prise en charge par tous les navigateurs intégrés.
- Vous pouvez créer de multiples stratégies de session sur le même serveur virtuel en fonction du type de connexion (telle que ICA, CVPN ou VPN) et du type de Receiver (Receiver pour Web ou des logiciels Receiver installés localement). Toutes les stratégies peuvent être appliquées à partir d'un serveur virtuel unique.
- Lorsque les utilisateurs créent des comptes sur Receiver, ils doivent entrer les informations d'identification au compte, telles que leur adresse e-mail ou le nom de domaine complet du serveur Access Gateway. À titre d'exemple, si la connexion échoue lors de l'utilisation du chemin d'accès par défaut, les utilisateurs doivent entrer le chemin d'accès complet au serveur Access Gateway.

Pour permettre aux utilisateurs distants de se connecter via Access Gateway à votre déploiement CloudGateway, vous pouvez configurer Access Gateway en vue de son utilisation avec StoreFront. La méthode que vous allez choisir pour autoriser l'accès dépend de l'édition de CloudGateway dans votre déploiement :

- Si vous déployez CloudGateway Express dans votre réseau, autorisez les connexions des utilisateurs internes ou distants à StoreFront via Access Gateway en intégrant Access Gateway et StoreFront. Cette fonctionnalité permet aux utilisateurs de se connecter à StoreFront pour accéder aux applications publiées XenApp et aux bureaux virtuels XenDesktop. Les utilisateurs se connectent via Citrix Receiver.

Pour de plus amples informations sur la configuration de ces connexions, reportez-vous à la section Intégration d'Access Gateway avec CloudGateway et aux autres rubriques sous ce nœud dans eDocs.

Vous trouverez des informations sur les paramètres requis par Receiver pour appareils mobiles dans les rubriques suivantes :

- Création du profil de session pour Receiver pour CloudGateway Enterprise
- Création du profil de session pour Receiver pour CloudGateway Express
- Configuration de stratégies d'accès sans client personnalisées pour Receiver
- Configuration de Secure Browse dans Access Gateway (appareils iOS uniquement, non requis pour les appareils Android)
- Autorisation de l'accès à partir d'appareils mobiles
- Outil MDX Toolkit pour applications mobiles

Pour permettre aux utilisateurs distants de se connecter via Access Gateway à votre déploiement Interface Web, configurez Access Gateway de manière à fonctionner avec l'Interface Web, comme décrit dans la rubrique Configuration d'Access Gateway édition Enterprise pour communiquer avec l'Interface Web et ses sous-rubriques dans Citrix eDocs.

Configurer l'Interface Web

Jan 29, 2016

Les utilisateurs d'iPhone et d'iPad peuvent lancer des applications via votre site Interface Web et le navigateur Safari intégré à leur appareil mobile. Configurez le site Interface Web comme vous le feriez pour toute autre application XenApp. Si aucun site XenApp Services n'est configuré pour l'appareil mobile, Receiver utilise automatiquement votre site Interface Web. Aucune configuration spéciale n'est nécessaire pour les appareils mobiles.

L'Interface Web 5.x est prise en charge par le navigateur Safari intégré.

Sur l'appareil mobile, les utilisateurs peuvent se connecter au site Interface Web à l'aide de leur nom de connexion et mot de passe.

Configurer des appareils mobiles automatiquement

Jan 29, 2016

Utilisez Citrix Mobile Receiver Setup URL Generator sur un PC ou Mac pour configurer rapidement Citrix Receiver pour des appareils mobiles. Utilisez cet outil pour configurer les paramètres des comptes XenApp, puis envoyez par e-mail les configurations à tous les appareils.

Étant donné que le nom d'utilisateur et le mot de passe sont saisis par l'utilisateur, la configuration ne requiert que le nom du serveur, l'adresse du serveur, le nom de domaine et les informations relatives à Access Gateway (le cas échéant).

1. Depuis un PC ou Mac, ouvrez Mobile Receiver Setup URL Generator depuis http://community.citrix.com/MobileReceiverSetupUrlGenerator/.
2. Pour Account Description, entrez le nom du compte, comme le groupe ou le département, par exemple, Production ou Ventes.
3. Pour Server Address, tapez l'adresse de votre batterie de serveurs XenApp, par exemple, gateway.mabatteriedeserveurs.net.
4. Pour Domain, tapez le nom de domaine de la batterie de serveurs à laquelle vous connectez vos utilisateurs.
5. Pour activer une configuration Access Gateway, sélectionnez la case à cocher Use Gateway.
    1. Sous Gateway type, choisissez l'édition d'Access Gateway déployée dans la batterie de serveurs à laquelle vous connectez vos utilisateurs. (Contactez votre administrateur si vous ne connaissez pas l'édition.)
    2. Sous Gateway Authentication Type, choisissez la méthode d'authentification utilisée dans votre infrastructure.
6. Cliquez sur Generate URL.
7. Dans Your Result, cliquez sur configuration link, et copiez le lien généré.

Utilisez le courrier électronique pour envoyer le lien directement aux appareils mobiles pour que les utilisateurs terminent leur compte de configuration pour Receiver sur l'appareil.
Important : certains BlackBerry nécessitent un e-mail formaté en texte brut pour pouvoir associer correctement l'adresse URL pré-configurée avec Receiver. Il est donc recommandé d'envoyer l'adresse URL sous forme d'e-mail en texte brut aux utilisateurs de BlackBerry.

Configurer des comptes manuellement

Jan 29, 2016

En général, lorsque Receiver se connecte à une passerelle Access Gateway, Receiver tente de localiser un site XenApp Services ou XenApp Web après l'authentification. Si aucun site n'est détecté, Receiver affiche une erreur. Pour éviter ce problème, vous pouvez configurer un compte manuellement pour faire en sorte que Receiver se connecte à Access Gateway.

1. Touchez l'icône Comptes dans le coin supérieur droit et dans l'écran Comptes, touchez le signe Plus (+). L'écran Nouveau compte s'affiche.
2. Dans le coin inférieur gauche, touchez l'icône à gauche de Options et touchez Installation manuelle. Des champs supplémentaires s'affichent sur l'écran.
3. Dans le champ Adresse, entrez l'adresse URL sécurisée du site ou de la passerelle Access Gateway, en fonction de celui ou celle à laquelle vous voulez vous connecter (par exemple, agee.masociété.com).
4. Sélectionnez l'une des options de connexion suivantes. Les champs restants sur l'écran changent, en fonction de votre sélection.
   - Interface Web : permet à Receiver d'afficher un site XenApp Web similaire à un navigateur Web. Également appelé Affichage Web.
   - XenApp Services : permet à Receiver de localiser un site XenApp Services spécifique pour lequel l'authentification via Access Gateway n'est pas configurée. Dans les options supplémentaires qui s'affichent à l'écran, saisissez les informations d'identification d'ouverture de session au site.
     - http:// : s'il existe plusieurs magasins, une liste s'affiche et l'utilisateur peut choisir le magasin à ajouter.
     - http:///citrix/ : cela ajoute le magasin StoreFront .
     - http:///citrix/PnAgent/config.xml : cela ajoute le magasin PNAgent d'ancienne génération par défaut.
     - http:///citrix//PnAgent/config.xml : cela ajoute le magasin PNAgent d'ancienne génération associé au .
   - Access Gateway : permet à Receiver de se connecter à un site XenApp Services via une passerelle Access Gateway spécifique. Dans les options supplémentaires qui s'affichent à l'écran, sélectionnez l'édition de serveur et ses informations d'identification d'ouverture de session, y compris si un jeton de sécurité est requis pour l'authentification.
5. Pour le certificat de sécurité, utilisez le paramètre dans le champ Ignorer les avertissements de certificat pour spécifier si vous voulez vous connecter au serveur même s'il dispose d'un certificat non valide, auto-signé ou expiré. Le paramètre par défaut est OFF.
   Important : si vous activez cette option, vous devez vous assurer que vous vous connectez au serveur correct. Citrix recommande fortement que tous les serveurs possèdent un certificat valide afin de protéger les machines utilisateur des attaques de sécurité en ligne. Un serveur sécurisé utilise un certificat SSL délivré depuis une autorité de certification. Citrix ne prend pas en charge les certificats auto-signés et ne recommande pas d'ignorer le certificat de sécurité.
6. Touchez Enregistrer.
7. Entrez votre nom d'utilisateur et mot de passe (ou jeton, si vous avez sélectionné l'authentification à deux facteurs) et touchez Ouvrir une session. L'écran Citrix Receiver s'affiche, dans lequel vous pouvez accéder à vos bureaux et ajouter et ouvrir vos applications.

Fournir l'authentification RSA SecurID pour appareils iOS

Jan 29, 2016

L'authentification RSA SecurID pour Citrix Receiver est prise en charge pour les configurations Secure Gateway (via l'Interface Web uniquement) et toutes les configurations NetScaler Gateway.

Pour obtenir des instructions sur la configuration de l'authentification RSA SecurID sur NetScaler Gateway, consultez :

- Configuration de l'authentification RSA SecurID sur NetScaler Gateway 11.0
- Configuration de l'authentification RSA SecurID sur NetScaler Gateway 10.5
- Configuration de l'authentification RSA SecurID sur NetScaler Gateway 10.1

Schéma d'URL requis pour le jeton logiciel sur Receiver : le jeton logiciel RSA SecurID utilisé par Receiver enregistre uniquement le schéma d'URL com.citrix.securid.

Si les utilisateurs ont installé Citrix Receiver et RSA SecurID sur leur appareil iOS, ils doivent sélectionner le schéma d'URL « com.citrix.securid » pour importer RSA SecurID Software Authenticator (jeton logiciel) sur l'application Receiver de leur appareil.

Pour utiliser un jeton logiciel RSA avec Citrix Receiver, demandez à vos utilisateurs de suivre cette procédure.

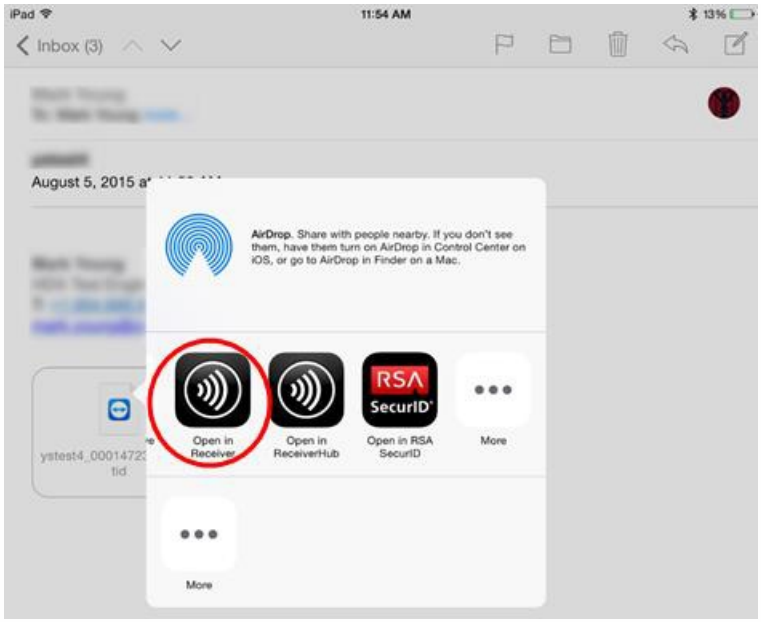
Les stratégies de longueur du code PIN, de type de code PIN (numérique uniquement, alphanumérique), et de réutilisations du code PIN sont spécifiées sur le serveur d'administration RSA.

Vos utilisateurs ne doivent effectuer cette opération qu'une seule fois, après s'être authentifiés avec succès auprès du serveur RSA. Après vérification de leur code PIN, ils sont également authentifiés auprès du serveur StoreFront, et ce dernier présente les applications et bureaux publiés disponibles.

Pour utiliser un jeton logiciel RSA avec Citrix Receiver

1. Importez le jeton logiciel RSA qui vous a été fourni par votre organisation.

À partir de l'e-mail contenant votre fichier SecurID, sélectionnez **Ouvrir Receiver** en tant que destination d'importation.



Une fois le jeton logiciel importé, Citrix Receiver s'ouvre automatiquement.

2. Si votre organisation vous a fourni un mot de passe pour l'importation, entrez-le et cliquez sur **OK**.

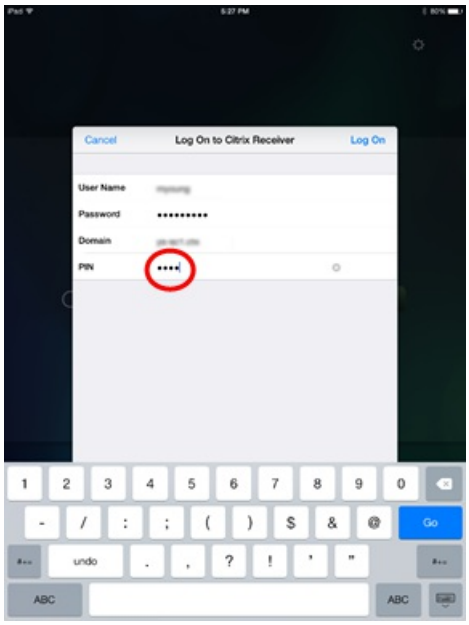
Après avoir cliqué sur **OK**, un message vous indiquera que le jeton a été importé avec succès.

3. Fermez le message d'importation et cliquez sur **Ajouter un compte** dans Citrix Receiver.

- Entrez l'adresse URL du magasin fournie par votre organisation.
- Cliquez sur **Suivant**.

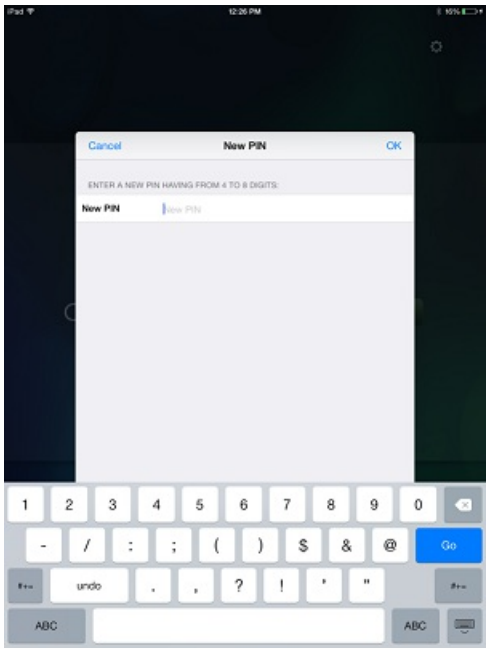
4. Sur l'écran d'ouverture de session :

- Entrez vos informations d'identification : nom d'utilisateur, mot de passe et domaine (telles que exemple.com).
- Pour le champ de code PIN, entrez **0000**, sauf si votre organisation vous a fourni un code PIN par défaut différent. (Le code PIN 0000 est le code RSA par défaut, mais il est possible que votre organisation l'ait modifié pour se conformer à ses stratégies de sécurité.)
- Dans le coin supérieur gauche, cliquez sur **Ouvrir une session**.



5. Lorsque vous cliquez sur le bouton Ouvrir une session, vous êtes invité à créer un nouveau code PIN.

Entrez un code PIN comprenant de 4 à 8 chiffres et cliquez sur **OK**.



6. Vous êtes ensuite invité à vérifier votre nouveau code PIN. Retapez votre code PIN, puis cliquez sur **OK**.

Après avoir cliqué sur OK, vous pourrez accéder à vos applications et à vos bureaux.

Si vous configurez Access Gateway pour utiliser l'authentification RSA SecurID, Receiver prend en charge le mode Jeton suivant. Lorsque cette fonctionnalité est activée et qu'un utilisateur entre un mot de passe incorrect à trois reprises (valeur par défaut), Access Gateway Plug-in invite l'utilisateur à attendre que le jeton suivant soit actif avant d'ouvrir une session. Le serveur RSA peut être configuré pour désactiver un compte utilisateur si un utilisateur se connecte un certain nombre de fois à l'aide d'un mot de passe incorrect.

Fournir des informations d'accès aux utilisateurs d'appareils iOS

Jan 29, 2016

Vous devez fournir aux utilisateurs les informations de compte Receiver dont ils ont besoin pour accéder à leurs applications, données et bureaux hébergés. Vous pouvez leur fournir ces informations de la façon suivante :

- Configurer la découverte de compte basée sur une adresse e-mail
- Fournir un fichier de provisioning aux utilisateurs
- Fournir aux utilisateurs une adresse URL de configuration générée automatiquement
- Fournir aux utilisateurs des informations de compte à entrer manuellement

Vous pouvez configurer Receiver de manière à utiliser la découverte de compte basée sur e-mail. Une fois configuré, plutôt que d'entrer une adresse URL de serveur, les utilisateurs entrent leur adresse e-mail durant l'installation et la configuration de Receiver. Receiver identifie le serveur Access Gateway ou StoreFront, ou le boîtier virtuel AppController associé à l'adresse e-mail en se basant sur les enregistrements SRV de DNS et invite les utilisateurs à ouvrir une session pour accéder à leurs applications, données et bureaux publiés.

Remarque : la découverte de compte basée sur l'adresse e-mail n'est pas prise en charge si Receiver se connecte à un déploiement Interface Web.
Pour configurer votre serveur DNS afin de prendre en charge la découverte basée sur l'adresse e-mail, consultez la section Configurer la découverte de compte basée sur une adresse e-mail dans la documentation StoreFront.

Pour configurer Access Gateway afin d'accepter les connexions utilisateur à l'aide d'une adresse e-mail pour découvrir l'adresse URL de StoreFront ou d'Access Gateway, consultez la section Connexion à StoreFront à l'aide de la découverte basée sur l'adresse e-mail dans la documentation Access Gateway.

Vous pouvez utiliser StoreFront pour créer des fichiers de provisioning contenant les détails des comptes. Vous pouvez mettre ces fichiers à la disposition de vos utilisateurs pour leur permettre de configurer Receiver automatiquement. Après l'installation de Receiver, il leur suffit d'ouvrir le fichier .cr sur l'appareil pour configurer Receiver. Si vous configurez des sites Receiver pour Web, les utilisateurs peuvent également obtenir les fichiers de provisioning à partir de ces sites.

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

Vous pouvez utiliser le générateur d'adresse URL de configuration pour configurer Receiver pour les appareils mobiles. Une fois Receiver installé, les utilisateurs n'ont qu'à cliquer sur cette URL pour configurer leur compte et accéder à leurs ressources. Utilisez cet outil pour configurer les paramètres des comptes et envoyez ces informations par e-mail ou publiez-les auprès de tous vos utilisateurs simultanément.

Pour plus d'informations, consultez la section Pour configurer des appareils mobiles automatiquement.

Si vous fournissez aux utilisateurs des informations de compte à entrer manuellement, vous devez leur communiquer les

informations suivantes afin de leur permettre de se connecter à leurs applications et bureaux hébergés avec succès :

- L'adresse URL de StoreFront ou du site XenApp Services hébergeant les ressources ; par exemple :nomserveur.société.com..
- Pour permettre l'accès à l'aide d'Access Gateway, fournissez l'adresse d'Access Gateway et la méthode d'authentification requise.
  Pour de plus amples informations sur la configuration d'Access Gateway ou de Secure Gateway, consultez la documentation Access Gateway ou XenApp (pour Secure Gateway).

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

Sur un iPad, lorsque des utilisateurs ferment la session d'un compte Receiver et qu'ils sont toujours connectés à des applications ou bureaux, ils ont la possibilité de se déconnecter ou de fermer la session :

- **Déconnecter** : ferme la session du compte, mais laisse l'application Windows ou le bureau exécuté sur le serveur, de sorte que l'utilisateur peut démarrer un autre appareil, lancer Receiver et se reconnecter au dernier état avant la déconnexion de l'iPad. Cette option permet aux utilisateurs de se reconnecter à partir d'un autre appareil et de reprendre le travail dans les applications en cours d'exécution.
- **Fermer la session** : ferme la session du compte, ferme les applications Windows, et ferme la session sur le serveur XenApp ou XenDesktop. Cette option permet aux utilisateurs de se déconnecter du serveur et de fermer la session du compte ; lorsque Receiver est ouvert de nouveau, il s'ouvre à son état par défaut.

Activation de la souris Citrix X1, d'un moniteur externe et des fonctionnalités de présentation

Jan 29, 2016

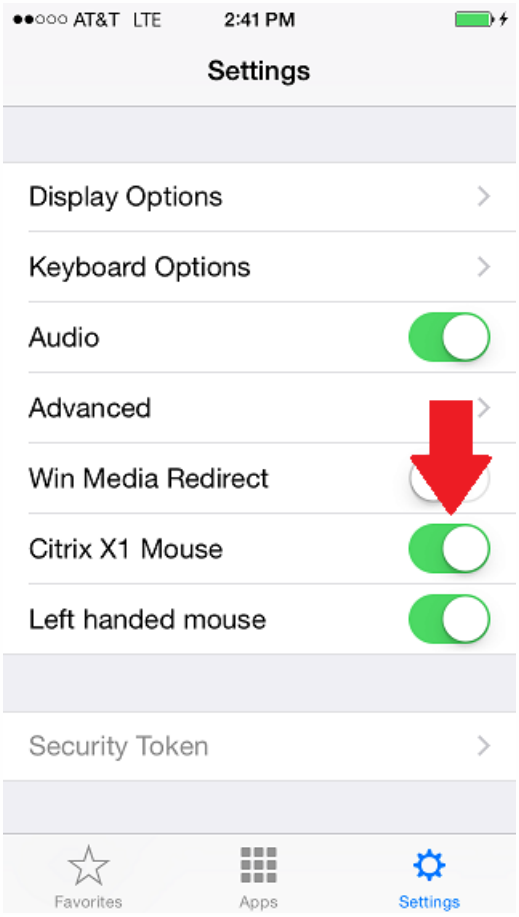
Pour faciliter l'utilisation d'applications Windows sur votre appareil iOS, vous pouvez configurer Citrix Receiver de manière à utiliser la souris Citrix X1 avec les applications HDX exécutées dans une session XenApp ou XenDesktop.

Vous pouvez également configurer les paramètres Receiver afin d'utiliser un moniteur externe et d'utiliser votre appareil iOS en tant que clavier ou touchpad pour contrôler l'affichage. Cela vous permet de réaliser des présentations sur votre appareil iOS.

Vous pouvez connecter et utiliser la souris Citrix X1 dans les sessions Citrix HDX. Receiver ne prend en charge qu'un seul modèle de souris pour le moment. Pour de plus amples informations sur la souris Citrix X1, consultez http://www.citrix.com/products/mouse/overview.html.

La souris Citrix X1 étant un périphérique bluetooth, vous devez activer bluetooth sur votre appareil iOS.

Pour vous connecter à la souris Citrix X1 et l'activer, appuyez sur **Paramètres** et activez le commutateur **Souris Citrix X1** dans Receiver.



Pour les gauchers, vous pouvez intervertir les boutons de la souris : dans Receiver, appuyez sur **Paramètres** et sélectionnez le commutateur **Gaucher**.

Si vous utilisez la souris Citrix X1 dans un bureau virtuel Windows, vous pouvez également activer la souris pour gaucher dans le Panneau de configuration de Windows. Accédez aux propriétés de la souris pour configurer votre souris.

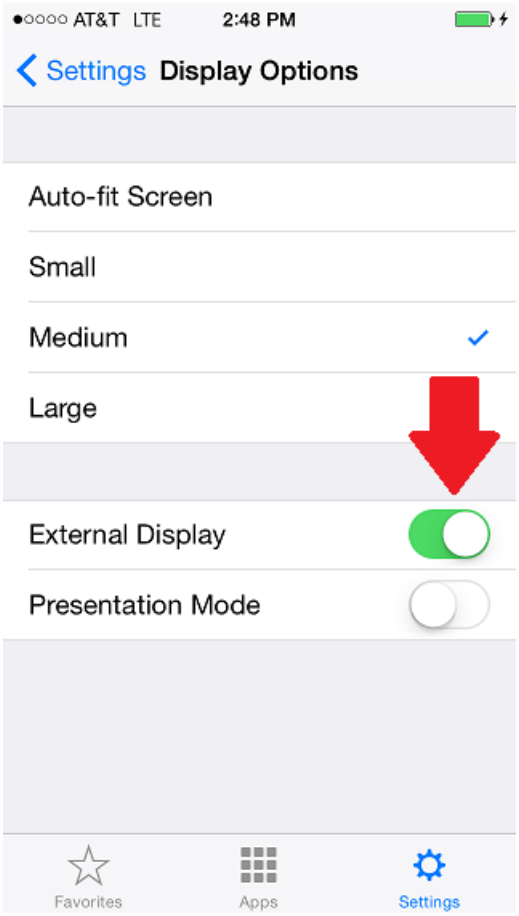
Receiver pour iOS prend en charge les moniteurs externes avec iPhone et iPad.

La fonctionnalité Moniteur externe est disponible via les méthodes suivantes :

- AirPlay
- Adaptateur Lightning vers VGA
- Adaptateur Lightning Digital AV

Un moniteur externe n'est pas recommandé pour les iPads (modèles antérieurs à Air) et iPhones (5c et antérieurs) plus anciens en raison des exigences élevées en matière de traitement.

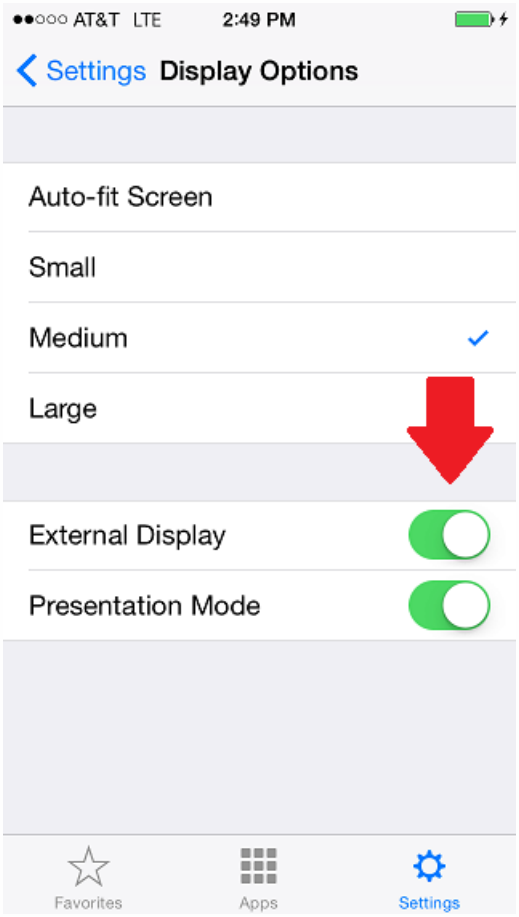
Pour activer les moniteurs externes, dans Receiver, appuyez sur **Paramètres** puis sur **Options d'affichage.** Sélectionnez le commutateur **Moniteur externe**.



Vous pouvez transformer votre iPad en clavier et touchpad lorsqu'il est connecté à un moniteur externe, tel que AppleTV ou

un câble Lightning vers HDMI, au lieu d'utiliser un clavier Bluetooth.

Pour activer le mode de présentation, dans **Receiver**, appuyez sur **Paramètres** puis sur **Options d'affichage**. Sélectionnez les commutateurs **Moniteur externe** *et* **Mode de présentation**.



Le moniteur externe et le mode de présentation sont compatibles avec la souris Citrix X1.

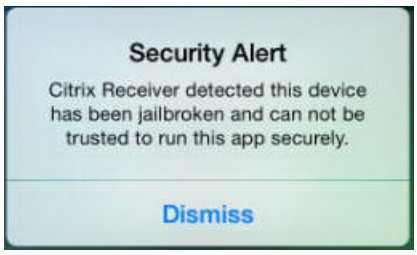
Empêcher les appareils jailbreakés d'exécuter des applications provenant de StoreFront

Jan 29, 2016

Dans cet article :

Vos utilisateurs peuvent compromettre la sécurité de votre déploiement en se connectant à l'aide d'appareils iOS jailbreakés. Les appareils jailbreakés sont des appareils qui ont été modifiés par leurs propriétaires, généralement dans le but de contourner certaines mesures de sécurité.

Lorsque Citrix Receiver détecte un appareil iOS jailbreaké, il affiche une alerte :



Pour sécuriser davantage votre environnement, vous pouvez configurer StoreFront ou l'Interface Web de manière à empêcher les appareils jailbreakés d'exécuter des applications.

Configuration requise

- Citrix Receiver pour iOS 6.1
- StoreFront 3.0 ou l'Interface Web 5.4
- Accès à StoreFront ou l'Interface Web via un compte d'administrateur

Pour empêcher les appareils jailbreakés d'exécuter des applications

1. Ouvrez une session sur le serveur StoreFront ou Interface Web en tant qu'utilisateur doté de privilèges d'administrateur.
2. Accédez au fichier default.ica, qui se trouve dans l'un des emplacements suivants :

- **C:\inetpub\wwwroot\Citrix***nommagasin***\conf** (Microsoft Internet Information Services)
- **C:\inetpub\wwwroot\Citrix***nommagasin***\App_Data** (Microsoft Internet Information Services)
- **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF** (Apache Tomcat)

3. Sous la section **[Application]** ajoutez ce qui suit :

```
AllowJailBrokenDevices=OFF
```

Extrait d'un fichier default.ica dans lequel AllowJailBrokenDevices est défini sur OFF :

```
[Application]
Launcher=PNAgent
TransportDriver=TCP/IP
DoNotUseDefaultCSL=On
BrowserProtocol=HTTPonTCP
LocHttpBrowserAddress=!
WinStationDriver=ICA 3.0
ProxyTimeout=30000
AutologonAllowed=ON
EnableIPCSessionControl=TRUE
AllowJailBrokenDevices=OFF

[EncRC5-0]
DriverNameWin32=pdc0n.dll
```

4. Enregistrez le fichier et redémarrez votre serveur StoreFront ou Interface Web.

Après avoir redémarré le serveur StoreFront, les utilisateurs qui ont vu l'alerte à propos des appareils jailbreakés ne peuvent pas lancer d'applications depuis votre serveur StoreFront ou Interface Web.

Pour autoriser les appareils jailbreakés à exécuter des applications

Si vous ne définissez pas AllowJailBrokenDevices, l'alerte est affichée par défaut aux utilisateurs d'appareils jailbreakés mais ils sont quand même autorisés à lancer des applications.

Si vous voulez spécifiquement autoriser vos utilisateurs à exécuter des applications sur des appareils jailbreakés :

1. Ouvrez une session sur le serveur StoreFront ou Interface Web en tant qu'utilisateur doté de privilèges d'administrateur.

2. Accédez au fichier default.ica, qui se trouve dans l'un des emplacements suivants :

- **C:\inetpub\wwwroot\Citrix***nommagasin***\conf** (Microsoft Internet Information Services)
- **C:\inetpub\wwwroot\Citrix***nommagasin***\App_Data** (Microsoft Internet Information Services)
- **./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF** (Apache Tomcat)

3. Sous la section **[Application]** ajoutez ce qui suit :

    AllowJailBrokenDevices=ON

Extrait d'un fichier default.ica dans lequel AllowJailBrokenDevices est défini sur ON :

```
[Application]
Launcher=PNAgent
TransportDriver=TCP/IP
DoNotUseDefaultCSL=On
BrowserProtocol=HTTPonTCP
LocHttpBrowserAddress=!
WinStationDriver=ICA 3.0
ProxyTimeout=30000
AutologonAllowed=ON
EnableIPCSessionControl=TRUE
AllowJailBrokenDevices=ON

[EncRC5-0]
DriverNameWin32=pdc0n.dll
```

4. Enregistrez le fichier et redémarrez votre serveur StoreFront ou Interface Web.

Lorsque vous définissez AllowJailBrokenDevices sur ON, vos utilisateurs voient l'alerte relative à l'utilisation d'un appareil

jailbreaké, mais ils peuvent exécuter des applications depuis StoreFront où l'Interface Web.

Enregistrer des mots de passe

Jan 29, 2016

La console de gestion de l'Interface Web Citrix vous permet de configurer la méthode d'authentification XenApp afin d'autoriser les utilisateurs à enregistrer leurs mots de passe. Lorsque vous configurez le compte utilisateur, le mot de passe crypté est enregistré jusqu'à ce que l'utilisateur se connecte. Tenez compte des considérations suivantes :

- Si vous activez l'enregistrement du mot de passe, Citrix Receiver stocke ce dernier et n'invite pas les utilisateurs à le réentrer pour se connecter à des applications.

> ## Remarque
>
> Le mot de passe est uniquement stocké si les utilisateurs entrent un mot de passe lors de la création de compte. Si aucun mot de passe n'est entré pour le compte, aucun mot de passe n'est enregistré, quelque soit le paramètre du serveur.

- Si vous désactivez l'enregistrement du mot de passe (paramètre par défaut), Citrix Receiver invite les utilisateurs à entrer leur mot de passe chaque fois qu'ils se connectent.

> ## Remarque
>
> L'enregistrement du mot de passe n'est pas disponible avec les connexions directes à StoreFront.

Si vous configurez le serveur de manière à enregistrer les mots de passe, les utilisateurs qui préfèrent demander des mots de passe à l'ouverture de session peuvent ignorer l'enregistrement des mots de passe :

- Lors de la création du compte, laissez le champ de mot de passe vide.
- Lors de la modification d'un compte, supprimez le mot de passe et enregistrez le compte.

À compter de la version 6.1.2, iOS pour Citrix Receiver introduit une fonctionnalité qui optimise le processus de connexion en vous permettant d'enregistrer votre mot de passe, ce qui élimine le besoin de vous authentifier chaque fois que vous ouvrez Citrix Receiver.

> ## Remarque
>
> La fonctionnalité d'enregistrement du mot de passe fonctionne avec le protocole PNA. Elle ne fonctionne pas avec le mode *natif* de StoreFront ; toutefois, elle fonctionne lorsque StoreFront active le mode PNA *d'ancienne génération*.

Configuration du mode d'ancienne génération PNA de StoreFront

Pour configurer le mode d'ancienne génération PNA de StoreFront afin d'activer la fonctionnalité d'enregistrement du mot de passe :

1. Si vous configurez un magasin existant, passez à l'étape 3.

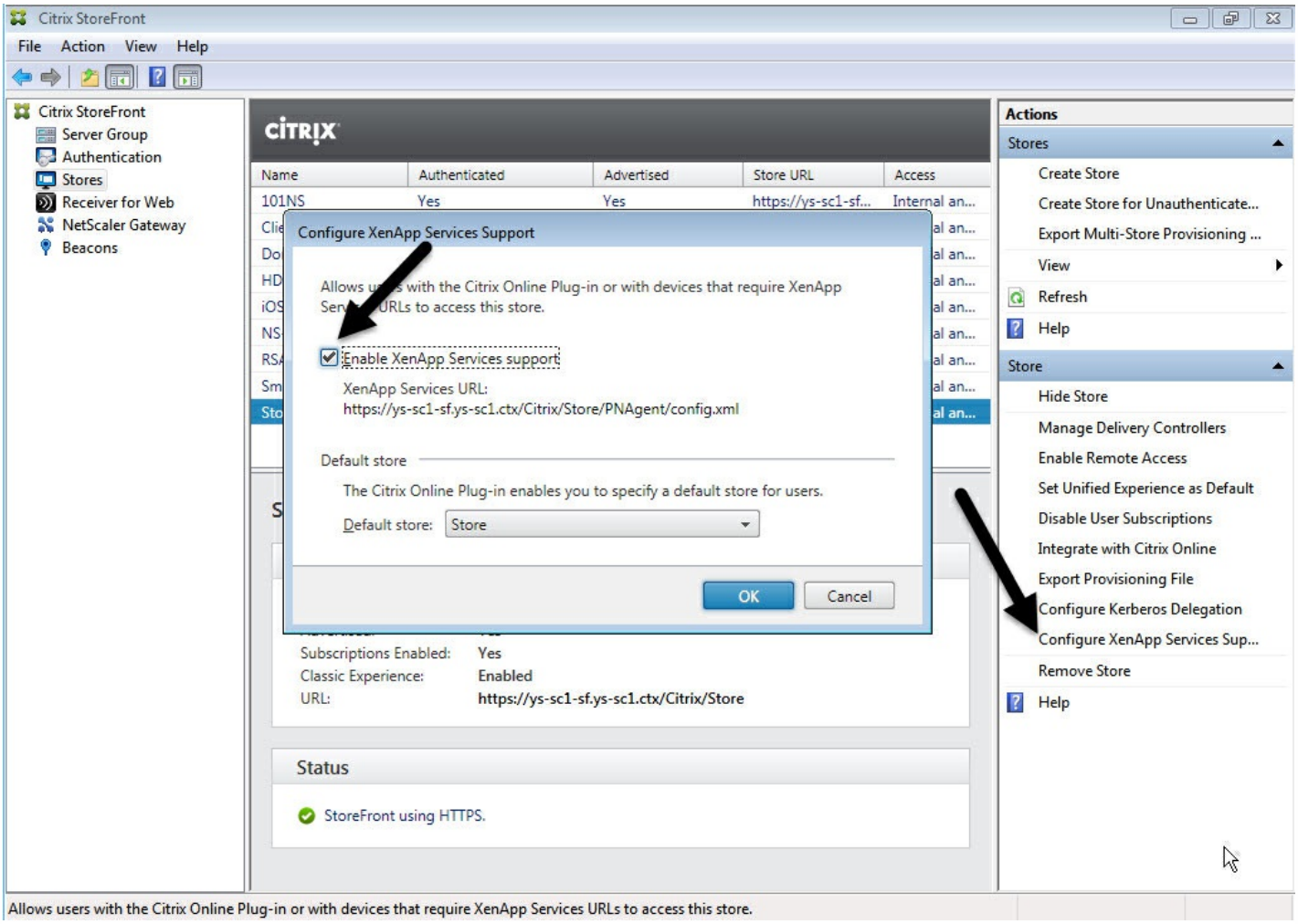
2. Pour configurer un nouveau déploiement StoreFront, suivez les recommandations détaillées dans Installer, configurer et désinstaller Citrix StoreFront.

3. Ouvrez la console de gestion Citrix StoreFront.

> ## Conseil
>
> Assurez-vous que l'URL de base utilise HTTPS et qu'elle est identique au nom commun spécifié lors de la génération de votre certificat SSL.

4. Sélectionnez le magasin à configurer.

5. Cliquez sur **Configurer la prise en charge de XenApp Services**.



7. Activez **Prise en charge d'ancienne version** et cliquez sur **OK**.

8. Accédez au fichier de configuration de modèle sur c:\inetpub\wwwroot\Citrix\\Views\PnaConfig\.

9. Effectuez une copie de sauvegarde de Config.aspx.

10. Ouvrez le fichier d'origine Config.aspx.

11. Modifiez la ligne **false** et changez la valeur **false** sur **true**.

12. Enregistrez le fichier Config.aspx.

13. Sur le serveur StoreFront, exécutez PowerShell avec des droits d'administration.

14. Dans la console PowerShell :

    a. cd "c:\Program Files\Citrix\Receiver StoreFront\Scripts"

    b. Tapez "Set-ExecutionPolicy RemoteSigned"

    c. Tapez ".\ImportModules.ps1"

    d. Tapez "Set-DSDerviceMonitorFeature –ServiceUrl https://localhost:443/StorefrontMonitor"

15. Si vous disposez d'un groupe StoreFront, exécutez les mêmes commandes sur tous les membres du groupe.

Configuration de NetScaler

Pour configurer NetScaler afin de prendre en charge la fonctionnalité d'enregistrement de mot de passe :

1. Ouvrez une session sur la console de gestion NetScaler.

> ### Remarque
>
> Cette configuration utilise des serveurs d'équilibrage de charge NetScaler. Si NetScaler n'est pas encore configuré sur votre environnement, suivez le guide de déploiement de Citrix sur : Guide de déploiement de Citrix NetScaler et Citrix XenDesktop 7 (en anglais).

2. Suivez les recommandations de Citrix pour créer un certificat pour votre ou vos serveurs d'équilibrage de charge.

3. Sur l'onglet de configuration, accédez à Traffic Management -> Load Balancing -> Servers. Cliquez sur **Add**.

4. Entrez le nom et l'adresse IP du serveur StoreFront. Cliquez sur **Create**.

> ### Conseil
>
> Si vous disposez d'un groupe StoreFront, répétez l'étape 5 pour tous les serveurs du groupe.

5. Sur l'onglet de configuration, accédez à Traffic Management -> Load Balancing -> Monitor. Cliquez sur **Add**.

6. Entrez un nom pour le moniteur. Sélectionnez le type **STOREFRONT**.

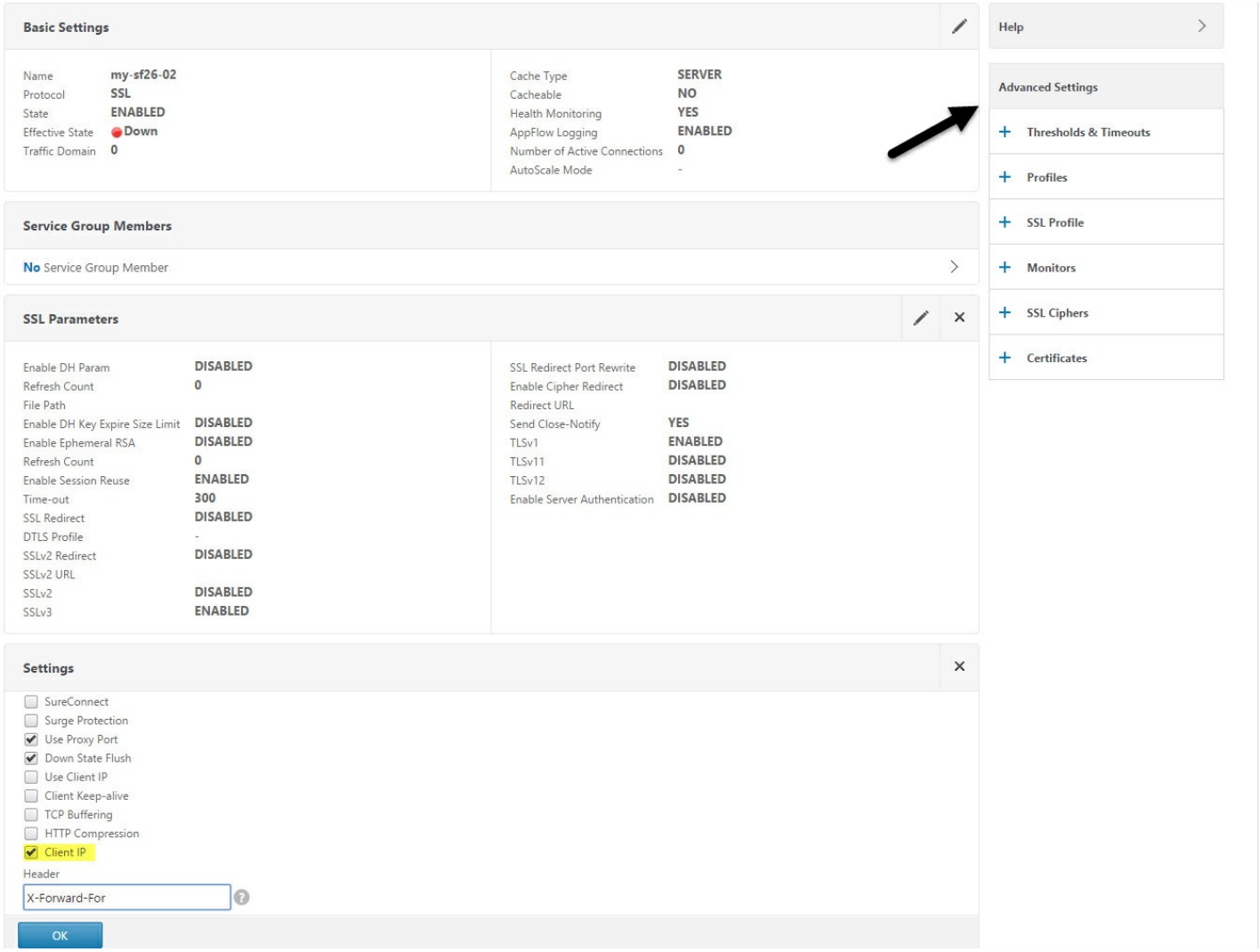
7. En bas de la page, sélectionnez **Secure** (ceci est requis car le serveur StoreFront utilise HTTPS).

8. Cliquez sur l'onglet **Special Parameters**. Entrez le nom du StoreFront configuré précédemment et sélectionnez **Check Backed Services**. Cliquez sur **Create**.

9. Sur l'onglet **Configuration**, accédez à Traffic Management -> Load Balancing -> Service Groups. Cliquez sur **Add**.

10. Entrez un nom pour votre groupe de services et définissez le protocole sur **SSL**. Cliquez sur **OK**.

11. Sur le côté droit de l'écran, sous Advanced Settings, sélectionnez **Settings**.



12. Activez l'option Client IP et entrez ce qui suit pour la valeur Header : **X-Forwarded-For**. Cliquez sur **OK**.

13. Sur le côté droit de l'écran, sous Advanced Settings, sélectionnez **Monitors**.

14. Cliquez sur la flèche pour ajouter de nouveaux moniteurs.

15. Cliquez sur le bouton **Add** et sélectionnez le menu déroulant **Select Monitor** ; une liste des moniteurs va s'afficher (ceux configurés sur NetScaler).

16. Cliquez sur le bouton radio en regard du ou des moniteurs que vous avez créés précédemment et cliquez sur **Select**, puis

sur **Bind**.

17. Sur le côté droit de l'écran (sous Advanced Settings), sélectionnez **Members**.

18. Cliquez sur la flèche pour ajouter de nouveaux membres au groupe de services.

19. Cliquez sur le bouton **Add** et sélectionnez le menu déroulant **Select Member**.

20. Sélectionnez le bouton radio **Server Based** ; une liste des membres du serveur va s'afficher (ceux configurés sur NetScaler).

21. Cliquez sur le bouton radio en regard du ou des serveurs StoreFront que vous avez créés précédemment.

22. Entrez 443 pour le numéro de port et spécifiez un numéro Hash ID unique, puis cliquez sur **Create**.

23. Cliquez sur **Done**.

> ## Conseil
>
> Si tout a été configuré correctement, **Effective State** doit afficher un voyant vert, ce qui indique que la surveillance fonctionne correctement.

24. Accédez à Traffic Management -> Load Balancing -> Virtual Servers et cliquez sur **Add**.

25. Entrez un nom pour le serveur et sélectionnez **SSL** en tant que protocole.

26. Entrez l'adresse IP du serveur d'équilibrage de charge StoreFront. Cliquez sur **OK**.

27. Sélectionnez la liaison **Load Balancing Virtual Server Service Group**, cliquez sur la flèche et ajoutez le groupe de services créé précédemment.

28. Cliquez deux fois sur **OK**.

29. Allouez le certificat SSL créé pour le serveur virtuel d'équilibrage de charge. Sélectionnez **No Server Certificate**.

30. Sélectionnez le certificat du serveur d'équilibrage de charge dans la liste et cliquez sur **Bind**.

31. Ajoutez le certificat de domaine au serveur d'équilibrage de charge. Cliquez sur **No CA certificate**.

32. Sélectionnez le certificat de domaine et cliquez sur **Bind**.

33. Sur le côté droit de l'écran, sélectionnez **Persistence**.

34. Changez l'option Persistence sur **SOURCEIP** et définissez le délai d'expiration sur **20**. Cliquez sur **Save**.

35. Cliquez sur **Done**.

37. Sur votre serveur DNS de domaine, ajoutez le serveur d'équilibrage de charge (s'il n'a pas déjà été créé).

38. Lancez Citrix Receiver sur votre appareil iOS et entrez l'URL complète de XenApp. Par exemple :

    https:// Serveur virtuel>/Citrix/PNAgent/Config.xml

Conseil

Pour de plus amples informations, consultez Guide de déploiement de Citrix NetScaler et Citrix XenDesktop 7 (en anglais) et Installer, configurer et désinstaller Citrix StoreFront.

Essayez le site de démo

Jan 29, 2016

Lorsque des utilisateurs lancent Citrix Receiver pour la première fois, la page de bienvenue leur permet d'ouvrir un compte de démo dans le Citrix Cloud.

Les utilisateurs doivent s'enregistrer en entrant leur nom et adresse e-mail (l'adresse e-mail est pré-remplie sur certains appareils). Le site de démo est déjà configuré avec des applications publiées de manière à ce que les utilisateurs puissent tester Citrix Receiver immédiatement.

Les utilisateurs peuvent ajouter, modifier et supprimer leurs comptes dans Receiver.

Résolution des problèmes

Jan 29, 2016

Les utilisateurs peuvent se déconnecter (mais pas fermer de session) d'une session Receiver des manières suivantes :

- Lors de l'affichage d'une application ou d'un bureau publié dans une session :
  - appuyez sur la flèche en haut de l'écran pour afficher le menu déroulant de la session.
  - appuyez sur le bouton **Accueil** pour revenir à votre point de départ.
  - remarquez l'ombre blanche sous l'icône de l'une des applications publiées toujours dans une session active ; appuyez sur l'icône.
  - appuyez sur Déconnecter.
- Fermer Receiver :
  - appuyez deux fois sur le bouton **Accueil** de l'appareil.
  - localisez Receiver dans la vue du sélecteur d'application iOS.
  - appuyez sur Déconnecter dans la boîte de dialogue qui s'affiche.
- En appuyant sur le bouton d'accueil sur leur appareil mobile.
- En tapant sur Accueil ou Basculer dans le menu déroulant de l'application.

La session affiche un état déconnecté. Bien que l'utilisateur puisse se reconnecter ultérieurement, vous pouvez vous assurer que les sessions déconnectées sont rendues inactives après un certain laps de temps. Pour ce faire, configurez un délai d'expiration de session pour la connexion ICA-tcp dans la configuration d'hôte de session Bureau à distance (anciennement appelée « Configuration des services Terminal Server »). Pour de plus amples informations sur la configuration de Services Bureau à distance (anciennement appelée « Services Terminal Server »), reportez-vous à la documentation produit Microsoft Windows Server.

Si les utilisateurs observent des problèmes avec des touches numériques ne fonctionnant pas correctement dans les applications publiées, ils peuvent essayer de désactiver le clavier Unicode dans Receiver. Pour ce faire, à partir de l'onglet Paramètres, touchez Options du clavier, et pour Utiliser le clavier Unicode, sélectionnez Off.

Depuis XenDesktop, il se peut que la qualité de l'audio HDX vers le Receiver pour iOS soit inférieure lors de l'utilisation de l'audio avec de la vidéo. Ce problème se produit lorsque les stratégies HDX XenDesktop ne peuvent gérer la quantité de données audio avec les données vidéo. Pour des suggestions sur la création de stratégies destinées à améliorer la qualité audio, consultez l'article http://support.citrix.com/article/ctx123543.

Les utilisateurs qui ne disposent pas d'un compte peuvent créer un compte utilisateur de démo sur le site de démo du Citrix Cloud à l'adresse http://citrixcloud.net/.

Le Citrix Cloud permet aux utilisateurs de bénéficier de la puissance des solutions Citrix sans avoir à préparer et configurer leur propre environnement. L'environnement de démo du Citrix Cloud utilise un certain nombre de solutions Citrix clés, telles que XenServer, XenApp, NetScaler et Access Gateway.

Sachez toutefois que les données ne sont pas sauvegardées dans cet environnement de démo, il est donc possible que

vous ne puissiez pas vous reconnecter à votre session après vous être déconnecté.

Receiver permet aux utilisateurs de modifier leurs mots de passe quand ils ont expiré. Ils sont invités à entrer les informations requises.

Si vous rencontrez des problèmes tels que des connexions lentes au site XenApp Services, des icônes d'application manquantes ou des messages « Erreur de pilote de protocole », procédez comme suit pour les résoudre : sur le serveur XenApp et Citrix Secure Gateway ou le serveur Interface Web, désactivez les propriétés de la carte Ethernet PV Citrix pour l'interface réseau (toutes activées par défaut) :

- Large Send Offload
- Offload IP Checksum
- Offload TCP Checksum
- Offload UDP Checksum

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

Ce problème côté serveur peut se produire même lorsque le partage d'application est activé. Il s'agit d'un problème intermittent pour lequel aucune solution n'existe.