À propos de Citrix Receiver pour iOS 5.9.x

Nov 18, 2015

> **Important**
>
> Citrix Receiver pour iOS 5.9.x ne prend pas en charge iOS 9. Si vous avez mis à niveau votre appareil vers iOS 9, mettez à niveau Citrix Receiver vers la dernière version.
>
> Pour mettre à niveau, accédez aux pages de téléchargement de Citrix : http://www.citrix.com/downloads/citrix-receiver/ios/receiver-for-ios.html.

Receiver pour iOS 5.9.6

Cette version résout un problème d'interopérabilité avec les claviers Bluetooth.

Receiver pour iOS 5.9.5

Nouveautés

- **Souris X1**. 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 connecter et activer la souris, accédez à Receiver Paramètres et sélectionnez le commutateur **Souris X1**.
  - Pour les gauchers, il est possible d'intervertir les boutons de la souris. Accédez à Receiver Paramètres et sélectionnez le commutateur **Gaucher**. Ou, à partir du Panneau de configuration de Windows, accédez à Propriétés de souris.

  Pour de plus amples informations sur la souris Citrix X1, consultez http://www.citrix.com/products/mouse/overview.html.

- **Prise en charge améliorée des moniteurs externes**. Receiver pour iOS prend en charge les moniteurs externes avec iPhone et iPad.
  - Pour activer les moniteurs externes, accédez à Citrix Receiver Paramètres > Options d'affichage et sélectionnez le commutateur **Affichage externe**.
  - La fonctionnalité Moniteur externe est disponible via les méthodes suivantes :
    - AirPlay
    - Adaptateur Lightning vers VGA
    - Adaptateur Lightning Digital AV

      Remarque : l'adaptateur Lightning Digital AV n'a pas été testé.
  - 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.
- **Mode Touchpad/présentation – Version d'évaluation**. 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, accédez à Citrix Receiver Paramètres > Options d'affichage et sélectionnez les commutateurs **Affichage externe** et **Mode de présentation**.
  - Le mode Touchpad/présentation est compatible avec la souris X1.
  - Le mode Touchpad/présentation est disponible en version d'évaluation et n'est pas destiné à être utilisé dans un environnement de production.

Problèmes résolus

- Les modifications des événements associés à l'état du clavier sont incorrectement renvoyées pour Citrix Mobility Pack. [#522269]
- La taille de l'écran de résolution de session est incorrecte lors de l'utilisation du mode Ajuster à l'écran sur une application optimisée par Citrix Mobility Pack. [#545325]
- Il est difficile de faire défiler l'écran de session. [#545324]

Receiver pour iOS 5.9.4

Nouveautés

- Prise en charge des protocoles TLS 1.0, 1.1 et 1.2. Vous pouvez modifier votre environnement afin qu'il utilise ces trois protocoles. Receiver pour iOS utilise 1.2 s'il est disponible, puis 1.1, puis TLS 1.0 en dernier recours.
- Graphiques améliorés pour iPhone 6 Plus et autres téléphones dotés d'un affichage Retina.
  - Possibilité de lancer des sessions haute-résolution à l'aide de l'option Ajuster à l'écran dans Paramètres > Options d'affichage.

Problèmes résolus

- Mobility SDK renvoie maintenant la valeur **5** pour **orientationFaceUp** et la valeur **6** pour **orientationFaceDown**.
- Problème de dégradation des couleurs.
- Problème de perte d'images 3D Pro.
- Problème avec la loupe sur iPad.

Receiver pour iOS 5.9.3

Nouveautés

- Expérience utilisateur améliorée lors de la reconnexion à une session via Worx Home.

Problèmes résolus

- Lors de l'utilisation d'une session RDP (Remote Desktop Protocol) publiée en plein écran au sein d'une session ICA, aucune lettre majuscule n'est envoyée.
- Problème intermittent avec le clavier à l'écran.
- Problèmes de résolution d'App Switcher.
- Anomalies graphiques mineures lorsque l'appareil est pivoté.
- Problème occasionnel avec le lancement d'un bureau via NetScaler.

Receiver pour iOS 5.9.2

Nouveautés

- Résolution des problèmes « d'écran noir » observés dans les versions précédentes.
- Résolution des problèmes liés au SDK Mobility.
- Ajout d'une option pour activer les extensions de clavier (mise à jour de sécurité).
- Afin de prévenir une nouvelle attaque, telle que POODLE, contre le protocole SSLv3, ce dernier est désactivé dans cette version de Receiver pour iOS. Pour plus d'informations, veuillez consulter l'article CTX 200238.
  Remarque : vous devez vous assurer que TLS 1.0 est activé.

Receiver pour iOS 5.9.1

Nouveautés

- Prise en charge de iOS 8.
- Dictée Siri restaurée avec Citrix Receiver.
- Vous pouvez accéder à plus d'une application à la fois et basculer entre les applications d'un simple balayage du doigt. L'utilitaire App Switcher démarre automatiquement lorsque vous ouvrez une seconde application dans la même session. Vous pouvez effectuer un balayage depuis le bord de l'écran pour sélectionner l'application publiée suivante. Pour utiliser cette fonctionnalité, les applications doivent être publiées par l'administrateur sur le même serveur.
- La fonctionnalité Contrôle de l'espace de travail est disponible dans **Paramètres > Avancé > Contrôle de l'espace de travail**.
- La journalisation avancée est activée afin de recueillir des données de diagnostic permettant de faciliter la résolution des problèmes liés à l'authentification, aux magasins et aux connexions. Les options de journalisation se trouvent dans **Paramètres > Assistance > Options de journal**.
- L'option ShareFile dans **Paramètres > Avancé** n'est plus disponible. Pour utiliser ShareFile, téléchargez l'application Citrix ShareFile depuis le App Store.

Remarque : lorsque la stratégie « Affichage automatique du clavier » est activée via une stratégie Citrix, vous devrez toucher à deux reprises la zone de texte (saisie) pour afficher le clavier à l'écran.

Receiver pour iOS 5.9

Nouveautés

- Receiver offre une prise en charge limitée des cartes à puce.
  Remarque : les clients qui utilisent des périphériques NetScaler certifiés FIPS doivent configurer leurs 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.
- Prise en charge de iOS 7.1.
- Prise en charge des certificats SHA2.
- Prise en charge de l'implémentation de l'accès à l'aide d'un seul nom de domaine complet.

Problèmes résolus dans 5.9 - 5.9.x

Les problèmes suivants ont été corrigés depuis la dernière version de ce produit.

- Après que vous ayez ouvert une application qui contient des données modifiables, lorsque vous réalisez un toucher avec

trois doigts, il se peut que le clavier virtuel ne s'affiche pas. [#394204]

- Si l'écran apparaît déformé ou qu'un écran noir s'affiche après le démarrage d'un VDA ou alors que vous travaillez dans le Centre de contrôle où le Centre de notification, actualisez votre session en touchant l'écran de l'appareil ou en le faisant pivoter. [#406877]
- Lorsque la redirection Windows Media était activée (sur l'écran Paramètres), Citrix offrait les suggestions suivantes pour améliorer votre expérience de visualisation. Dans 5.9.x, ces suggestions ne sont plus nécessaires :
  - Lorsque vous regardez une vidéo sur le lecteur Windows Media sur un bureau virtuel et que vous tapotez sur Accueil sur l'appareil iOS, lorsque Receiver reprend, il se peut que l'écran vidéo soit noir. Pour reprendre la vidéo, lors de la reprise de Receiver, tapotez sur le bouton Pause dans le lecteur Windows Media. Puis tapotez Lecture.
  - Pour rechercher un nouveau point dans une vidéo s'exécutant sur le lecteur Windows Media, tapotez l'emplacement désiré sur la barre de progression, plutôt que de faire glisser l'icône vers celui-ci. Si vous faites glisser l'icône vers le nouvel emplacement, lors de rares occasions, un écran noir apparaît. Tapotez la barre de progression et la vidéo devrait démarrer à nouveau.
- Si vous tapotez sur le bouton Ouvrir une session après avoir tapé un mot de passe d'une longueur de un caractère, vous ne pouvez pas démarrer une application publiée tant que vous n'avez pas redémarré Receiver. [#395745]
- Lors de l'utilisation de Receiver sur un appareil exécutant iOS 7, l'ajout d'une application au magasin et le lancement de cette application peut entraîner l'échec de Receiver. [#443642]
- Lorsque vous utilisez Citrix Receiver sur un iPad, l'ouverture d'un lien de jeton RSA à partir d'un e-mail peut entraîner l'échec de Receiver après son lancement.[#443365]
- Lorsque vous créez un nouveau magasin à partir de Receiver et que vous importez un nouveau certificat client pour l'authentification, la saisie de l'URL du certificat et la sélection du certificat installé peuvent entraîner l'apparition du nom et prénom de l'utilisateur dans le champ de nom d'utilisateur plutôt que nomutilisateur@domaine. [#444021]
- Lorsque vous ajoutez un compte via Receiver, vous ne pourrez peut-être pas continuer au-delà de l'écran de sélection du certificat afin d'atteindre l'invite d'authentification pour LDAP. [#443641]

Problèmes connus

- 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]
- Les performances peuvent se dégrader lors de l'utilisation de moniteurs externes avec une résolution supérieure à 720 pixels.
- Il est possible que la souris X1 ne puisse pas être couplée à un autre périphérique tant que vous n'utilisez pas l'option Oublier cet appareil dans les réglages Bluetooth sur iOS.
- Il est possible que la souris X1 n'interagisse pas avec les icônes d'application sur l'écran de lancement des applications. [#560429]
- Il est possible que l'audio ne soit pas lu sur un périphérique AirPlay. [#55671]
- Il est possible que la souris X1 n'interagisse pas avec la barre d'outils de session durant une session. [#554469]
- Le problème suivant se produit lors de la connexion à une session de bureau virtuel XenDesktop : connexion au bureau virtuel, ouverture d'Internet Explorer et accès à un site à l'aide de formulaires de saisie de texte. Le clavier tactile s'affiche comme prévu ; toutefois, lorsque les utilisateurs se déconnectent puis qu'ils se reconnectent au bureau virtuel, le clavier tactile ne s'affiche plus automatiquement. La solution consiste à toucher l'écran avec trois doigts pour ouvrir le clavier tactile. [#461011]
- Sur l'iPhone uniquement, le défilement horizontal sur l'écran d'accueil n'est pas disponible pour le compte Store Web. [#338903]
- Sur le clavier étendu dans Microsoft Excel, l'utilisation des touches Ctrl ou Maj ne permet pas de sélectionner plusieurs cellules dans une feuille de calcul. Pour contourner le problème, appuyez sur la cellule et faites glisser votre doigt sur les

cellules adjacentes pour les sélectionner. [#339030]

- Lors de la configuration d'un nouveau compte utilisateur, il est possible que la page Inscription de certificats ne s'affiche pas tout de suite. [#339996]
- Le jeton logiciel RSA exige à tort que les utilisateurs entrent leur mot de passe et code PIN (au lieu du code PIN uniquement) chaque fois qu'ils ouvrent une session. [#350169]
- Si vous modifiez le type d'authentification dans NetScaler Gateway après que les utilisateurs aient créé un compte, le nouveau profil d'authentification n'est pas enregistré et il est possible que les utilisateurs ne puissent plus ouvrir de session. [#350206]
- Lorsqu'un fichier audio ou vidéo est exécuté dans une application publiée sur votre bureau, si vous modifiez le paramètre Données cellulaires sur l'écran Paramètres de I à O puis I à nouveau, le bureau ne répond plus. [#387530]
- Lorsque vous accédez à un magasin avec carte à puce et à un autre magasin sans carte à puce, le lancement de chaque magasin de manière consécutive peut entraîner l'échec du lancement du second magasin. Pour contourner le problème, quittez l'application Receiver et redémarrez-la avant de lancer un nouveau type de magasin. [#452347]
- Lorsque vous ouvrez une session sans vous authentifier à l'aide d'une carte à puce, vous ne pourrez peut-être pas utiliser la signature numérique de carte à puce dans la session. Pour éviter ce problème, ouvrez votre session en vous authentifiant à l'aide d'une carte à puce lorsque vous prévoyez d'utiliser la signature dans la session. [#457961]
- Lorsque vous ajoutez un compte uniquement avec le nom de domaine complet, le processus peut échouer. Pour éviter ce problème, entrez le nom de domaine complet au format suivant : https://FQDN, où *FQDN* est l'adresse de votre nom de domaine complet. [#458569]
- Lorsque vous lancez une application à laquelle vous n'avez pas souscrit, la session peut se bloquer sans afficher d'invite d'ouverture de session. Pour éviter ce problème, ouvrez d'abord une session sur le magasin ou souscrivez à l'application avant de la lancer. [#460159]
- Lorsque vous ajoutez un magasin et que l'option Carte à puce est activée, si vous le supprimez le magasin puis que vous l'ajoutez à nouveau dans les 10 minutes qui suivent, NetScaler peut afficher un message d'erreur.
  Pour éviter ce problème, attendez 10 minutes avant d'ajouter à nouveau un magasin qui a été supprimé. [#466490]

- Avec la redirection Windows Media activée (sur l'écran Paramètres), Citrix vous offre les suggestions suivantes pour améliorer votre expérience de visualisation :
  - La démo n'est pas prise en charge lors de l'utilisation du clavier pour naviguer sur les appareils exécutant iOS 7. Pour continuer et configurer le compte, touchez le champ d'e-mail. [#414965]
  - Pour de meilleurs résultats, conservez de l'espace libre sur l'appareil iOS lorsque vous utilisez la redirection Windows Media. Nous suggérons environ 1 Go, suivant la taille de la vidéo.

Configuration système requise

Nov 18, 2015

Appareil

> ### Important
>
> Citrix Receiver pour iOS 5.9.x ne prend pas en charge iOS 9. Si vous avez mis à niveau votre appareil vers iOS 9, mettez à niveau Citrix Receiver vers la dernière version.
>
> Pour mettre à niveau, accédez aux pages de téléchargement de Citrix : http://www.citrix.com/downloads/citrix-receiver/ios/receiver-for-ios.html.

- Citrix Receiver pour iOS 5.9.x prend en charge iOS 6.1.x, 7 et 8.
- Cette mise à jour logicielle est prise en charge sur les appareils suivants :
  - iPhone 4, 4S, 5, 5c, 5s, 6 et 6 Plus. Les seules versions de Receiver prises en charge sur l'iPhone 5c et 5s sont Receiver pour iOS 5.9 et 5.9.x.
  - Tous les modèles d'iPad.
  - iPod Touch de 5ème génération.
- Prise en charge de moniteurs externes
  - iPhone - aucun.
  - 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** (ci-dessous).

Serveur

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 2.6 (recommandé)
    Permet d'accéder directement aux magasins StoreFront. Receiver prend également en charge les versions antérieures 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

Connectivité et authentification

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				Oui*	Non
Cartes à puce	Oui	Oui		Oui*	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 dans eDocs.

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**	Oui			
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.

Cartes à puce

- Receiver offre une prise en charge limitée des cartes à puce.
  Remarque : les clients qui utilisent des périphériques NetScaler certifiés FIPS doivent configurer leurs 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

Nov 18, 2015

Receiver nécessite 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 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 » qui correspond à votre version de l'Interface Web.

Configurer StoreFront.

Nov 18, 2015

Pour configurer StoreFront

Remarque :

- Seules les éditions 9.3 et 10.0 de Citrix Access Gateway édition Enterprise sont prises en charge par Receiver pour iOS 5.6 et 5.7 lors de l'utilisation de StoreFront.
- 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.

Pour configurer Access 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 Access Gateway.

- Seuls Citrix Access Gateway 9.3 et 10.0 édition Enterprise et Access Gateway 5.0.4 sont pris en charge par Receiver pour iOS 5.6 et 5.7 utilisant StoreFront.
- Pour de plus amples informations, consultez la rubrique correspondant à votre version d'Access Gateway dans eDocs.

Pour configurer Receiver pour accéder aux applications

1. Lors de la création d'un nouveau compte, dans le champ Paramètres de compte, entrez l'adresse URL de votre boutique, telle questorefront.organisation.com..
2. Continuez en renseignant les champs restants et sélectionnez la méthode d'authentification à Access 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

Nov 18, 2015

Remarque :

- Les éditions 9.x et 10.x d'Access Gateway édition Enterprise sont prises en charge par Receiver pour iOS 5.5 et 5.6 à l'aide de sites XenApp Services.
- L'authentification du certificat client est prise en charge par Receiver pour iOS 5.5, 5.6, 5.7 et 5.9.
- Seules les éditions 9.x et 10.x 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 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 sont extraites à partir du champ spécifié du certificat. Ce champ est généralement Subject:CN. Si le nom d'utilisateur est extrait avec succès, l'utilisateur est authentifié. Si l'utilisateur ne fournit pas de certificat valide durant la négociation TLS ou si l'extraction du nom d'utilisateur échoue, l'authentification échoue.

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.

Pour configurer le site XenApp Services

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.

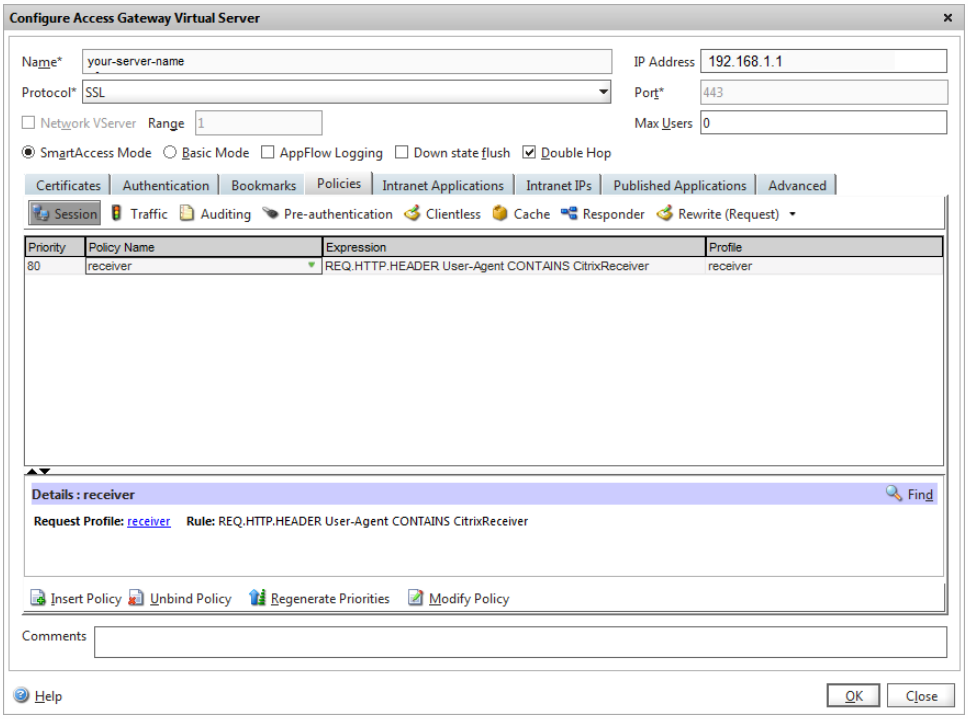
1. Dans le site XenApp Services, sélectionnez Gérer l'accès client sécurisé > Modifier les paramètres d'accès au client sécurisé.
2. Dans Méthode d'accès, choisissez Passerelle directe.
3. Entrez le nom de domaine complet du boîtier Access Gateway.
4. Entrez les informations de Secure Ticket Authority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

Pour configurer le boîtier Access Gateway

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.

Pour configurer l'appareil mobile pour l'application Receiver

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 ou le nom d'utilisateur et de groupe de l'utilisateur 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, le champ nom d'utilisateur de l'écran d'ouverture de session est renseigné avec le nom d'utilisateur provenant du certificat, et les utilisateurs entrent les informations manquantes, telles que le mot de passe et le domaine requis pour l'authentification au domaine.
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

Nov 18, 2015

Pour configurer le site XenApp Services

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).

Pour configurer Secure Gateway

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.

Pour configurer l'appareil mobile pour l'application Receiver

1. Ouvrez Paramètres de compte, et dans le champ d'adresse, entrez le nom de domaine complet de votre serveur Secure Gateway :

- 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. Dans les paramètres Citrix Access Gateway, désactivez Access Gateway.

Configurer Access Gateway édition Enterprise

Nov 18, 2015

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 Receivers 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 au travers d'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 eDocs.

Configurer l'Interface Web

Nov 18, 2015

Pour configurer le site Interface Web

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.

Pour lancer des applications sur l'appareil iOS

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 comptes manuellement

Nov 18, 2015

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.

Pour configurer des comptes manuellement

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

Nov 18, 2015

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 importer un jeton logiciel RSA SecurID dans Citrix Receiver

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

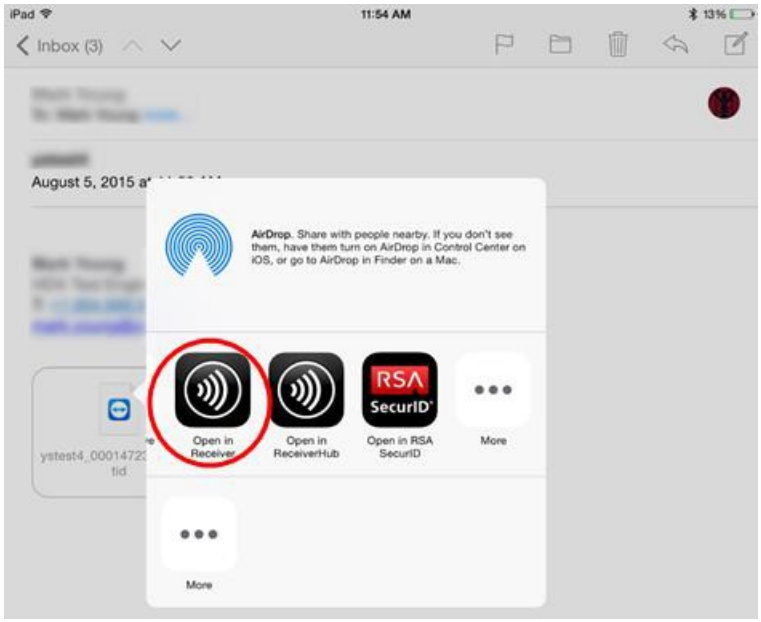
Les stratégies de longueur du code PIN, de type de code PIN (numérique uniquement, alphanumérique), et de réutilisations du code PIN sont spécifiées sur le serveur d'administration RSA.

Vos utilisateurs ne doivent effectuer cette opération qu'une seule fois. Une fois que vos utilisateurs se sont authentifiés 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**.

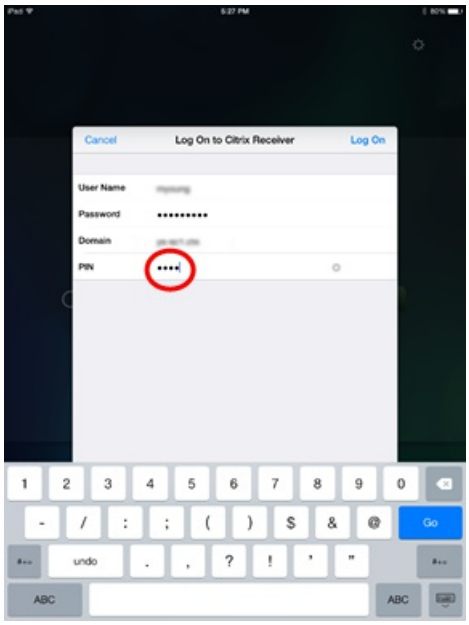
Après avoir cliqué sur **OK**, un message vous indiquera que le jeton a été importé avec succès.

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**.

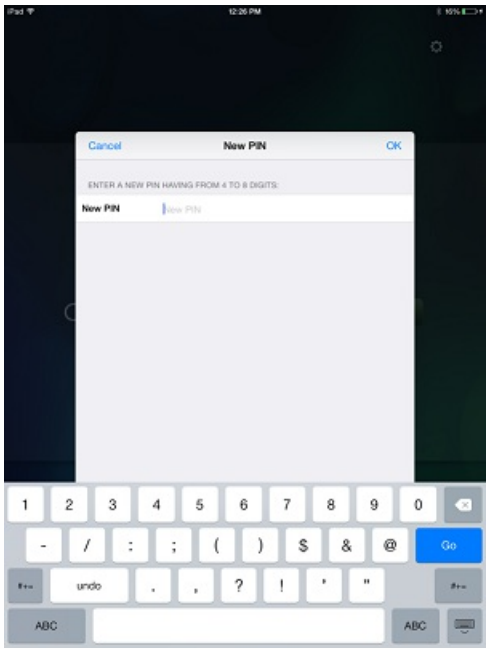
4. Sur l'écran d'ouverture de session :

- 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.

Prise en charge du mode Jeton suivant

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

Nov 18, 2015

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

Configurer la découverte de compte basée sur une adresse e-mail

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.

Fournir un fichier de provisioning aux utilisateurs

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.

Fournir aux utilisateurs une adresse URL de configuration générée automatiquement

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.

Fournir aux utilisateurs des informations de compte à entrer manuellement

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.

Partage de sessions

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.

Configurer des appareils mobiles automatiquement

Nov 18, 2015

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.

Enregistrer des mots de passe

Nov 18, 2015

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.

- Si vous activez l'enregistrement du mot de passe, 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), 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 StoreFront.

Pour annuler l'enregistrement des mots de passe

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.

Essayez le site de démo

Nov 18, 2015

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

Nov 18, 2015

Sessions déconnectées

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

- 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.

Problèmes avec le pavé numérique dans les applications

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.

Perte de qualité audio HDX depuis XenDesktop

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.

Comptes de démo disponibles depuis le Citrix Cloud

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.

Mots de passe expirés

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

Connexions lentes

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.

La connexion à l'aide d'un proxy n'est pas prise en charge

Receiver ne peut pas se connecter à des réseaux avec proxy Wi-Fi ou LAN.

Les applications peuvent s'ouvrir dans des sessions différentes

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.