



# Secure Web

## **Contents**

<b>Nouveautés dans Secure Web</b>	<b>3</b>
<b>Problèmes connus et résolus</b>	<b>14</b>
<b>Intégration et déploiement de Secure Web</b>	<b>15</b>
<b>Protection des données iOS</b>	<b>28</b>
<b>Fonctionnalités Secure Web</b>	<b>29</b>

## Nouveautés dans Secure Web

February 25, 2021

**Remarque :**

la prise en charge des versions Android 6.x et iOS 11.x de Secure Hub, Secure Mail, Secure Web et de l'application Citrix Workspace a pris fin en juin 2020.

### Nouveautés dans la version actuelle

#### Secure Web 21.2.0

**Revamping des couleurs pour Secure Web.** Secure Web est conforme aux mises à jour des couleurs de la marque Citrix.

#### Secure Web pour Android

**Fonctionnement régulier sur les appareils pliables.** Secure Web pour Android inclut des correctifs pour un fonctionnement régulier sur les appareils pliables.

### Nouveautés dans les versions précédentes

#### Secure Web 21.1.5

##### Secure Web pour iOS

Cette version inclut des corrections de bogues.

#### Secure Web 21.1.0

Cette version inclut des corrections de bogues.

#### Secure Web 20.12.0

##### Secure Web pour iOS

Cette version inclut des corrections de bogues.

#### Secure Web 20.11.0

Cette version inclut des corrections de bogues.

### **Secure Web 20.10.5**

#### **Secure Web pour Android**

**Prise en charge des bibliothèques AndroidX.** Conformément aux recommandations de Google, Secure Web prend en charge les bibliothèques **AndroidX**, qui remplacent les bibliothèques **android.support**-packaged.

### **Secure Web 20.10.0**

#### **Secure Web pour Android**

Secure Web prend en charge les exigences actuelles de l'API cible de Google Play pour Android 10.

### **Secure Web 20.9.5**

#### **Secure Web pour iOS**

Cette version inclut des corrections de bogues.

### **Secure Web 20.9.0**

#### **Secure Web pour Android**

**Remarque :**

la prise en charge d'Android 6.x a pris fin le 15 septembre 2020.

### **Secure Web 20.8.5**

#### **Secure Web pour Android**

Secure Web pour Android prend en charge Android 11.

### **Secure Web 20.8.0**

#### **Secure Web pour Android**

**Double mode pour la version Android de Secure Web.** Un SDK MAM (Mobile Application Management ou Gestion d'applications mobiles) est disponible pour remplacer les zones de fonctionnalités MDX qui ne sont pas couvertes par les plates-formes iOS et Android. La technologie d'encapsulation MDX devrait atteindre la fin de son cycle de vie en septembre 2021. Pour continuer à gérer vos applications d'entreprise, vous devez incorporer le SDK MAM.

A partir de la version 20.8.0, les applications Android sont publiées avec le SDK MDX et MAM en préparation à la stratégie MDX EOL mentionnée précédemment. Le mode double MDX fournit un moyen de

passer aux nouveaux SDK MAM à partir de MDX Toolkit d'ancienne génération. L'utilisation du mode double vous permet de continuer à gérer les applications à l'aide de MDX Toolkit (**MDX d'ancienne génération**) ou de basculer vers le nouveau SDK MAM pour la gestion des applications.

Une fois que vous passez au SDK MAM pour la gestion des applications, Citrix implémente d'autres modifications et ne nécessite aucune action de la part des administrateurs.

Pour plus d'informations sur le SDK MAM, consultez les articles suivants :

- [Présentation du SDK MAM](#)
- Section Citrix Developer sur [Gestion des appareils](#)
- [article de blog Citrix](#)
- Téléchargez le SDK lorsque vous vous connectez à [Téléchargements de Citrix](#)

### Conditions préalables

Pour un déploiement réussi de la fonction mode double :

- Mettez à jour votre Citrix Endpoint Management vers 10.12 RP2 et versions ultérieures, ou 10.11 RP5 et versions ultérieures.
- Mettez à jour vos applications mobiles vers la version 20.8.0 ou ultérieure.
- Mettez à jour le fichier de stratégies vers la version 20.8.0 ou ultérieure.
- Si votre organisation utilise des applications tierces, assurez-vous d'incorporer le SDK MAM à vos applications tierces avant de passer à l'option SDK MAM pour vos applications de productivité mobiles Citrix. Toutes vos applications gérées doivent être déplacées vers le SDK MAM en même temps.

#### Remarque :

le SDK MAM est pris en charge pour tous les clients basés sur le cloud.

### Limitations

- Le SDK MAM est uniquement pris en charge pour les applications publiées sous la plate-forme Android Enterprise sur votre déploiement Citrix Endpoint Management. Pour les applications nouvellement publiées, le chiffrement par défaut est le chiffrement basé sur la plate-forme.
- Le SDK MAM prend uniquement en charge le chiffrement basé sur la plate-forme, et non le chiffrement MDX.
- Si vous ne mettez pas à jour Citrix Endpoint Management et que les fichiers de stratégie s'exécutent sur les versions 20.8.0 et ultérieures pour les applications mobiles, des entrées en double de la stratégie Mise en réseau sont créées pour Secure Web.

Lorsque vous configurez Secure Web dans Citrix Endpoint Management, la fonctionnalité mode double vous permet de continuer à gérer les applications à l'aide du MDX Toolkit (désormais **MDX**

**d'ancienne génération**) ou de basculer vers le nouveau **SDK MAM** pour la gestion des applications. Citrix vous recommande de passer au **SDK MAM**, car les SDK MAM sont plus modulaires et vous permettent d'utiliser uniquement un sous-ensemble des fonctionnalités MDX utilisées par votre organisation. Il réduit l'encombrement global in-binaire et runtime d'une application.

Vous disposez des options suivantes pour les paramètres de stratégie dans le **conteneur de stratégie MDX ou MAM SDK** :

- **SDK MAM**
- **MDX d'ancienne génération**

The screenshot shows the Citrix Cloud Endpoint Management interface. The 'Configure' tab is active, and the 'Apps' section is selected. The application being configured is 'Secure Mail'. The 'MDX or MAM SDK policy container' option is highlighted with a red box, showing 'MAM SDK' selected and 'Legacy MDX' unselected. Other configuration options include 'File name', 'App Description', 'App version', 'Minimum OS version', 'Maximum OS version', 'Excluded devices', 'Remove app if MDM profile is removed', 'Prevent app data backup', 'Force app to be managed', and 'App deployed via Volume purchase'.

Dans la stratégie **Conteneur de stratégie MDX ou MAM SDK**, vous pouvez uniquement changer votre option de **MDX d'ancienne génération** à SDK MAM. L'option permettant de passer du SDK MAM au **MDX d'ancienne génération** n'est pas autorisée et vous devez republier l'application. La valeur par défaut est MDX d'ancienne génération. Assurez-vous de définir le même mode de stratégie pour Secure Mail et Secure Web lorsqu'ils s'exécutent sur le même appareil. Vous ne pouvez pas définir deux modes différents sur le même appareil.

### Secure Web 20.7.5

Cette version inclut des corrections de bogues.

### **Secure Web 20.7.0**

**Prise en charge du multitâche.** Dans Secure Web pour iOS, utilisez deux applications simultanément avec le multitâche. Pour activer cette fonctionnalité, faites glisser une application hors du Dock. Déplacez-la sur le bord droit ou gauche de l'écran pour diviser et activer l'écran pour deux applications.

Pour connaître les dernières informations sur les applications de productivité mobiles, consultez l'article [Annonces récentes](#).

### **Secure Web 20.6.0**

Cette version inclut des corrections de bogues.

### **Secure Web 20.5.0**

Cette version inclut des corrections de bogues.

### **Secure Web 20.4.5**

**Accès aux signets dans de nouveaux onglets.** Dans Secure Web pour iOS, vous pouvez afficher, modifier et accéder aux signets lorsque vous ouvrez un nouvel onglet.

### **Secure Web 19.10.5 à 20.4.0**

Ces versions comprennent des corrections de bugs.

### **Secure Web 19.10.0**

**Secure Web iOS et Android prennent en charge la gestion du cryptage :** la gestion du cryptage vous permet d'utiliser la sécurité des plates-formes d'appareils modernes tout en veillant à ce que l'appareil reste dans un état adéquat pour utiliser efficacement la sécurité de la plate-forme. En utilisant la gestion du cryptage, vous éliminez la redondance du cryptage des données locales puisque le cryptage du système de fichiers est fourni par les plates-formes iOS et Android respectives. Pour activer cette fonctionnalité, un administrateur doit définir la stratégie MDX **Type de cryptage** sur **Cryptage de plate-forme avec application des règles de conformité** dans la console Citrix Endpoint Management.

la gestion du cryptage vous permet d'utiliser la sécurité des plates-formes d'appareils modernes tout en veillant à ce que l'appareil reste dans un état adéquat pour utiliser efficacement la sécurité de la plate-forme. En utilisant la gestion du cryptage, vous éliminez la redondance du cryptage des données locales puisque le cryptage du système de fichiers est fourni par les plates-formes iOS et Android. Pour activer cette fonctionnalité, un administrateur doit définir la stratégie MDX **Type de cryptage** sur

**Cryptage de plate-forme avec application des règles de conformité** dans la console Citrix Endpoint Management.

### Type de cryptage

Pour utiliser la fonctionnalité de gestion du cryptage, dans la console Endpoint Management, définissez la stratégie MDX **Type de cryptage** sur **Cryptage de plate-forme avec application des règles de conformité**. Cela permet d'activer la gestion du cryptage : toutes les données d'application cryptées existantes sur les appareils des utilisateurs passent en toute transparence à un état crypté par l'appareil et non par MDX. Au cours de cette transition, l'application est suspendue pour une migration de données unique. Une fois la migration réussie, la responsabilité du cryptage des données stockées localement est transférée de MDX à la plate-forme de l'appareil. MDX continue de vérifier la conformité de l'appareil à chaque lancement d'application. Cette fonctionnalité fonctionne à la fois dans les environnements MDM+MAM et MAM exclusif.

Lorsque vous définissez la stratégie **Type de cryptage** sur **Cryptage de plate-forme avec application des règles de conformité**, la nouvelle stratégie remplace votre cryptage MDX existant.

Pour plus d'informations sur les stratégies MDX de gestion du cryptage pour Secure Web, consultez la section **Cryptage** dans :

- [Stratégies MDX pour les applications de productivité mobiles pour iOS](#)
- [Stratégies MDX pour les applications de productivité mobiles pour Android](#)

### Comportement des appareils non conformes

Lorsqu'un appareil se trouve en dessous des exigences minimales de conformité, la stratégie MDX **Comportement des appareils non conformes** vous permet de sélectionner les mesures à prendre :

- **Autoriser l'application** : cette option autorise l'application à s'exécuter normalement.
- **Autoriser l'application après avertissement** : cette option avertit l'utilisateur qu'une application ne répond pas aux exigences minimales de conformité et autorise l'exécution de l'application. Il s'agit de la valeur par défaut.
- **Bloquer l'application** : cette option empêche l'exécution de l'application.

Les critères suivants déterminent si un appareil répond aux exigences minimales de conformité.

Appareils fonctionnant sous iOS :

- iOS 10 : une application exécute une version du système d'exploitation supérieure ou égale à la version spécifiée.
- Accès au débogueur : une application n'a pas activé le débogage.
- Appareil jailbreaké : une application n'est pas en cours d'exécution sur un appareil jailbreaké.
- Code secret de l'appareil : le code secret de l'appareil est défini sur Activé.
- Partage de données : le partage de données n'est pas activé pour l'application.



Appareils fonctionnant sous Android :

- Android SDK 24 (Android 7 Nougat) : une application exécute une version du système d'exploitation supérieure ou égale à la version spécifiée.
- Accès au débogueur : une application n'a pas activé le débogage.
- Appareils rootés : une application ne s'exécute pas sur un appareil rooté.
- Verrouillage de l'appareil : le code secret de l'appareil est défini sur Activé.
- Appareil crypté : une application est en cours d'exécution sur un appareil crypté.

### **Secure Web 19.9.5**

Cette version inclut des corrections de bogues.

### **Secure Web 19.9.0**

#### **Secure Web pour iOS**

Secure Web pour iOS prend en charge iOS 13.

#### **Secure Web pour Android**

Cette version inclut des corrections de bogues.

### **Secure Web pour Android 19.8.5**

Secure Web pour Android prend en charge Android Q.

### **Secure Web 19.8.0**

Cette version inclut des corrections de bogues.

### **Secure Web 19.7.5**

#### **Secure Web pour iOS**

Cette version inclut des améliorations de performance et des corrections de bogues.

#### **Secure Web pour Android**

À partir de cette version, Secure Web pour Android est uniquement pris en charge sur les appareils exécutant Android 6 ou version ultérieure.

### **Secure Web 19.3.0 à 19.6.5**

Ces versions incluent des améliorations de performance et des corrections de bogues.

### **Secure Web 19.2.0**

**Autoriser l'ouverture des liens dans Secure Web tout en assurant la sécurité des données.** Avec Secure Web, un tunnel VPN dédié permet aux utilisateurs d'accéder en toute sécurité aux sites contenant des informations sensibles. Cette fonctionnalité était déjà disponible pour Secure Web pour iOS. Cette version ajoute la prise en charge pour Android. Pour plus de détails, consultez [Fonctionnalités Secure Web](#).

### **Secure Web versions 18.11.5 à 19.1.5**

Ces versions incluent des améliorations de performance et des corrections de bogues.

### **Secure Web 18.11.0**

Dans Secure Web pour iOS, la liste de taille de cache pour les sites n'est plus signalée et n'apparaît pas dans les paramètres de l'application. La fonctionnalité de mise en cache par défaut reste la même.

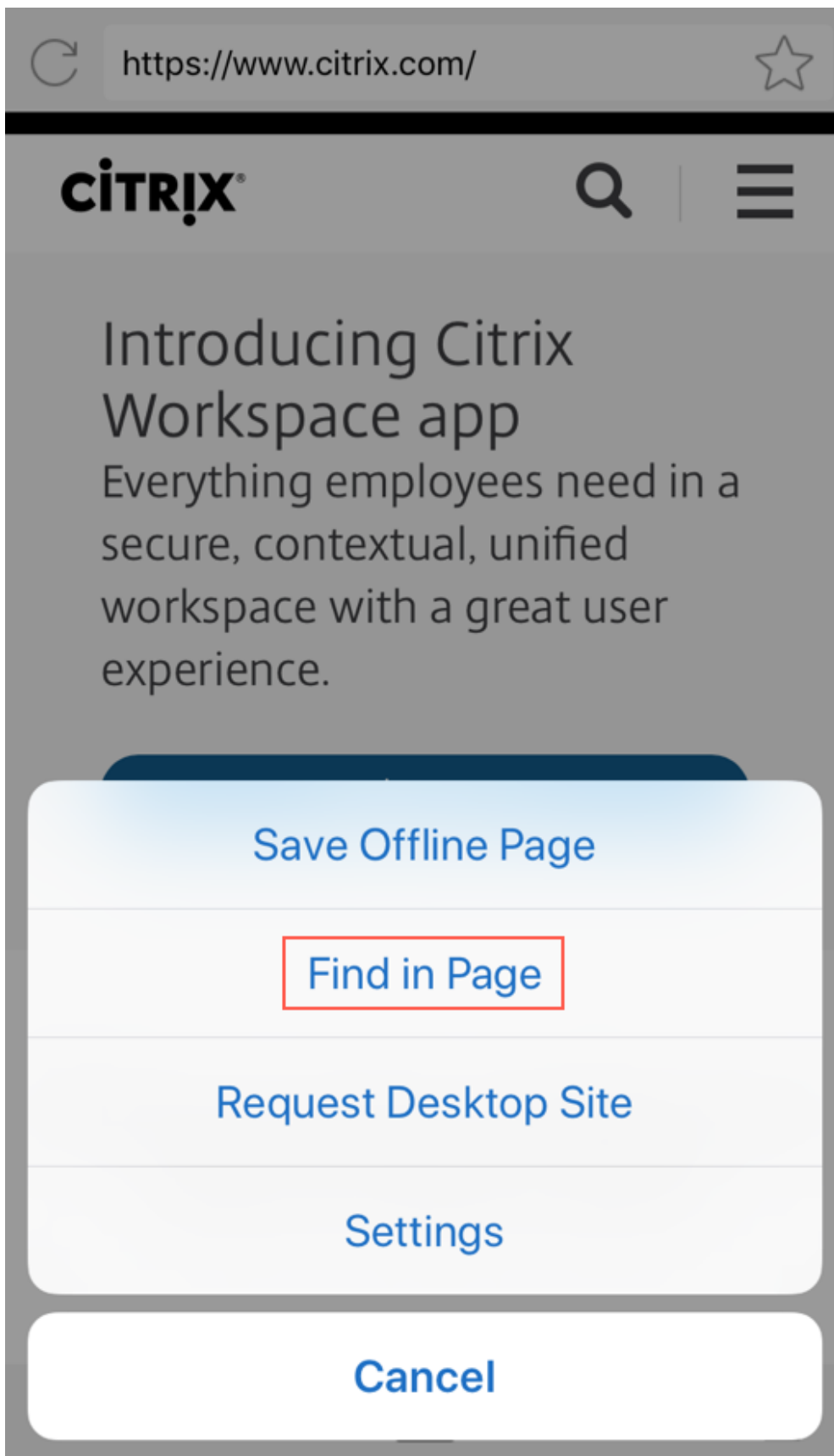
### **Secure Web 18.9.0 à 18.10.5**

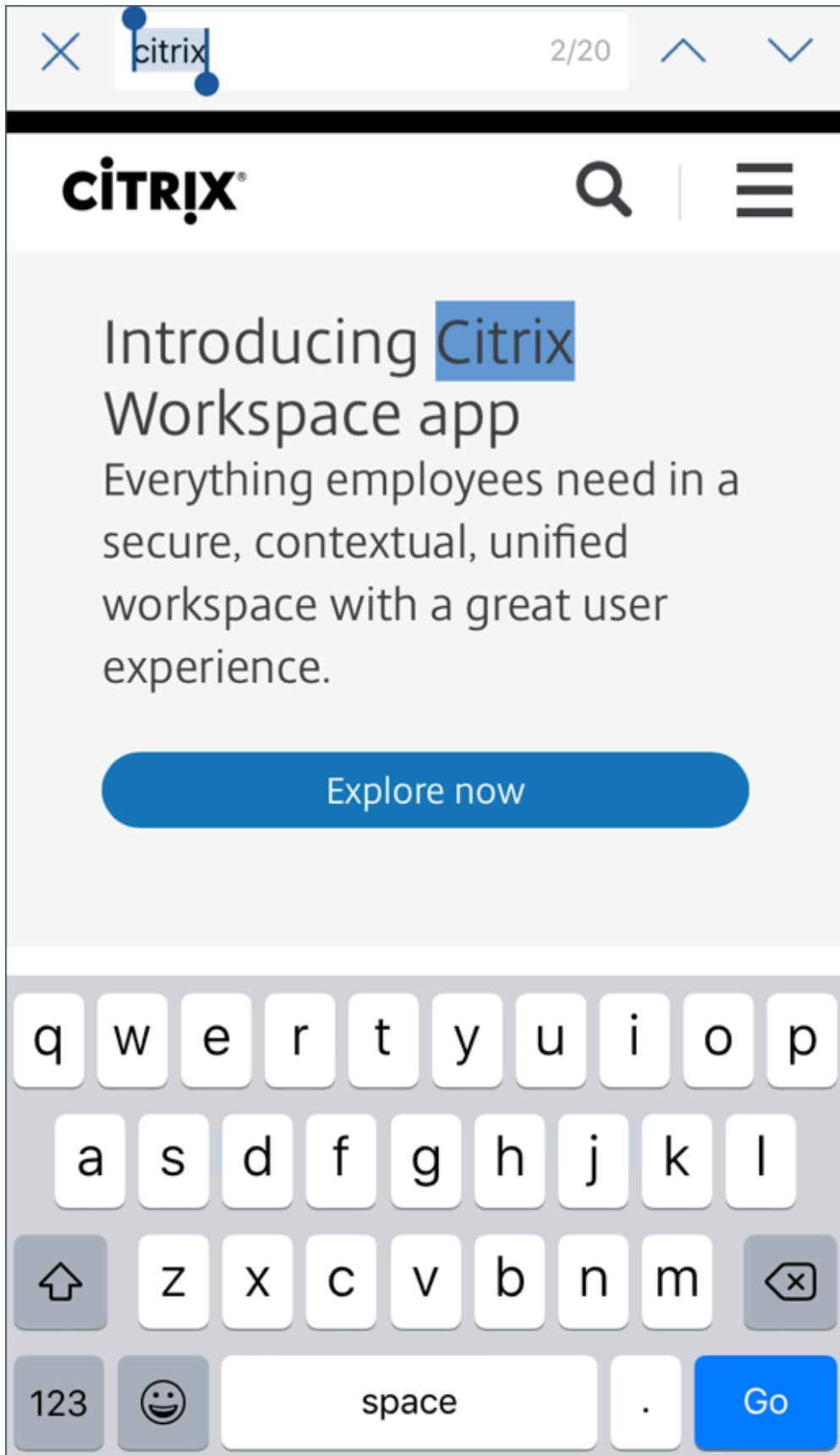
Ces versions incluent des améliorations de performance et des corrections de bogues.

### **Secure Web 10.8.65**

Les fonctionnalités suivantes sont nouvelles dans Secure Web 10.8.65 :

- **Tirer vers le bas pour actualiser.** Dans Secure Web pour iOS, les utilisateurs peuvent utiliser la fonction d'actualisation pour mettre à jour leurs données à l'écran.
- **Recherche en utilisant l'option Rechercher dans la page.** Vous pouvez rechercher des chaînes instantanément en utilisant l'option **Rechercher dans la page**. Cette option met en surbrillance les mots-clés lors de la recherche et affiche le nombre total de correspondances sur le côté droit de la barre d'outils. Lors de la relance, cette fonctionnalité conserve les derniers mots-clés recherchés.





- **Faire défiler vers le haut pour masquer les barres d'en-tête et de pied de page.** Dans Secure Web pour iOS, les barres d'en-tête et de pied de page sont masquées lorsque vous faites défiler vers le haut. Cela permet d'afficher davantage d'informations sur l'écran de votre appareil lors de la visualisation de pages Web.

### Secure Web 10.8.60

- Prise en charge de la langue polonaise

### Secure Web 10.8.35

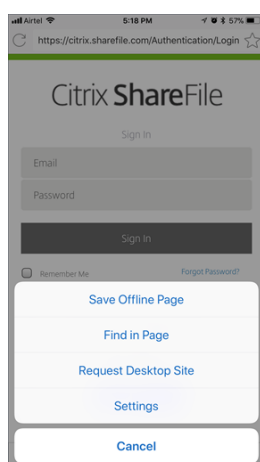
- **Tirer vers le bas pour actualiser.** Dans Secure Web pour Android, les utilisateurs peuvent utiliser la fonction d'actualisation pour mettre à jour leurs données à l'écran.

### Secure Web 10.8.15

- **Secure Web prend en charge Android Enterprise, anciennement appelé Android for Work.** Vous pouvez créer un profil de travail distinct à l'aide d'applications Android Enterprise dans Secure Mail. Pour plus de détails, consultez la section [Android Enterprise dans Secure Mail](#).
- **Secure Web pour Android peut afficher les pages Web en mode de bureau.** Dans le menu de dépassement, sélectionnez **Demander le site de bureau**. Secure Web affiche la version de bureau du site Web.

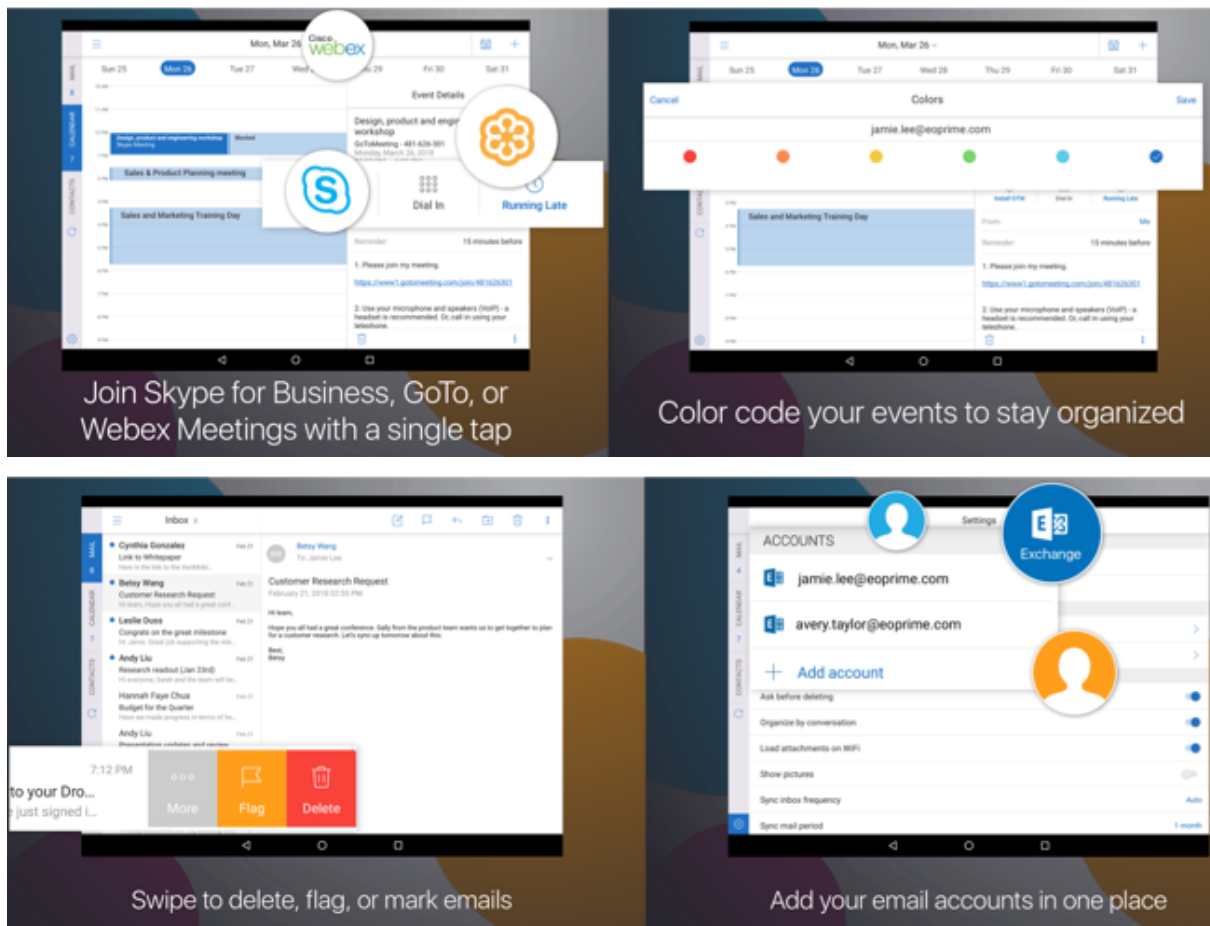
### Secure Web 10.8.10

- **Secure Web pour iOS peut afficher les pages Web en mode de bureau.** Dans le menu latéral, sélectionnez **Demander site de bureau** et Secure Web affiche la version de bureau du site Web.



### Secure Web 10.8.5

**Les polices, les couleurs et l'interface utilisateur de Secure Mail et de Secure Web pour iOS et Android ont fait l'objet d'améliorations.** Cette nouvelle mise en forme vous offre une expérience utilisateur enrichie tout en s'alignant étroitement sur l'esthétique de la marque Citrix à travers notre suite complète d'applications.



## Problèmes connus et résolus

February 25, 2021

Citrix prend en charge les mises à niveau à partir des deux dernières versions des applications de productivité mobiles.

## Secure Web 20.2.0

### Secure Web pour Android

Il n'y a aucun problème connu ou résolu dans cette version.

## Secure Web 21.1.5

Il n'y a aucun problème connu ou résolu dans cette version.

## Secure Web 21.1.0

Il n'y a aucun problème connu ou résolu dans cette version.

## Problèmes connus et résolus dans les versions antérieures

Pour connaître les problèmes connus et résolus dans les versions antérieures de Secure Mail, consultez la section [Problèmes connus et résolus dans les versions antérieures](#).

## Intégration et déploiement de Secure Web

January 18, 2021

Pour intégrer et délivrer Secure Web, suivez ces étapes :

1. Pour activer l'authentification unique (SSO) sur le réseau interne, configurez Citrix Gateway.  
Pour le trafic HTTP, Citrix ADC peut fournir l'authentification unique (SSO) pour tous les types d'authentification proxy pris en charge par Citrix ADC. Pour le trafic HTTPS, la stratégie Activer la mise en cache du mot de passe Web permet à Secure Web de s'authentifier et de fournir l'authentification unique (SSO) au serveur proxy via MDX. MDX prend uniquement en charge l'authentification de proxy NTLM, Digest et de base. Le mot de passe est mis en cache à l'aide de MDX et stocké dans le coffre partagé de Endpoint Management, une zone de stockage sécurisée pour les données applicatives sensibles. Pour plus d'informations sur la configuration de Citrix Gateway, consultez la section [Citrix Gateway](#).
2. Téléchargez Secure Web.
3. Déterminez la manière dont vous souhaitez configurer les connexions utilisateur au réseau interne.
4. Ajoutez Secure Web à Endpoint Management à l'aide des mêmes étapes que pour d'autres applications MDX et configurez des stratégies MDX. Pour de plus amples informations sur les stratégies spécifiques à Secure Web, consultez la section Stratégies Secure Web.

## Configuration des connexions utilisateur

Secure Web prend en charge les configurations suivantes pour les connexions utilisateur :

- **Navigation sécurisée** : les connexions qui sont tunnelisées sur le réseau interne peuvent utiliser une variante d'un VPN sans client, appelé Navigation sécurisée. Il s'agit de la configuration par défaut spécifiée pour la stratégie **Mode VPN préféré**. Navigation sécurisée est recommandé pour les connexions qui nécessitent l'authentification unique (SSO).
- **Tunnel VPN complet** : les connexions qui sont tunnelisées sur le réseau interne peuvent utiliser un tunnel VPN complet, configuré par la stratégie **Mode VPN préféré**. Un tunnel VPN complet est recommandé pour les connexions qui utilisent des certificats clients ou des connexions SSL de bout en bout vers une ressource dans le réseau interne. Le paramètre Tunnel VPN complet gère les protocoles faisant appel à TCP et peut être utilisé avec des ordinateurs Windows et Mac, ainsi qu'avec des appareils iOS et Android.
- La stratégie **Autoriser le basculement vers le mode VPN** permet le basculement automatique entre les modes de tunnel VPN complet et de navigation sécurisée si nécessaire. Cette stratégie est désactivée par défaut. Lorsque cette stratégie est activée, une demande réseau qui a échoué en raison d'une demande d'authentification qui ne peut pas être traitée dans le mode VPN préféré est de nouveau tentée dans un autre mode. Par exemple, le mode Tunnel VPN complet, mais pas le mode Navigation sécurisée peut utiliser des demandes d'accès au serveur pour les certificats clients. De même, les demandes d'authentification HTTP sont plus susceptibles d'être traitées avec l'authentification unique (SSO) lorsqu'elles utilisent le mode Navigation sécurisée.
- **Tunnel VPN complet avec PAC** : vous pouvez utiliser un fichier PAC (Proxy Automatic Configuration) avec un déploiement de tunnel VPN complet pour les appareils iOS. Un fichier PAC contient des règles qui définissent la manière dont les navigateurs Web sélectionnent un serveur proxy pour accéder à une URL spécifiée. Les règles du fichier PAC peuvent spécifier la procédure à suivre pour les sites internes et externes. Secure Web analyse les règles du fichier PAC et envoie les informations sur le serveur proxy à Citrix Gateway.
- Lorsqu'un fichier PAC est utilisé, les performances du tunnel VPN complet sont comparables au mode de navigation sécurisée. Pour de plus amples informations sur la configuration du fichier PAC, consultez la section Tunnelisation VPN complète avec le fichier PAC.
- **Split tunneling inverse** : dans le mode **INVERSE**, le trafic des applications intranet contourne le tunnel VPN tandis que le reste du trafic passe par le tunnel VPN. Cette stratégie peut être utilisée pour consigner tout le trafic LAN non local.

### Étapes de configuration pour le split tunneling inverse

Pour configurer le mode Split tunneling inverse sur Citrix Gateway, procédez comme suit :

1. Accédez à **Stratégies > Session**.
2. Sélectionnez la stratégie Secure Hub, puis accédez à **Expérience client > Split tunneling**.



3. Sélectionnez **INVERSE**.**Stratégie MDX Liste d'exclusion de split tunneling inverse**

Vous configurez la stratégie de mode de split tunneling inverse avec la plage Exclusion dans Citrix Endpoint Management. La plage est basée sur une liste séparée par des virgules de suffixes DNS et de noms de domaine complets. Cette liste définit les URL pour lesquelles le trafic doit être envoyé sur le réseau local (LAN) de l'appareil et ne sera pas envoyé à Citrix ADC.

Le tableau suivant indique si Secure Web invite l'utilisateur à entrer des informations d'identification, en fonction de la configuration et du type de site :

Mode de connexion	Type de site	Mise en cache du mot de passe	Authentification unique (SSO) configurée pour Citrix Gateway	Secure Web demande des identifiants lors du premier accès à un site Web	Secure Web demande des identifiants lors de l'accès ultérieur à un site Web	Secure Web demande des identifiants après le changement de mot de passe
Navigation sécurisée	HTTP	Non	Oui	Non	Non	Non
Navigation sécurisée	HTTPS	Non	Oui	Non	Non	Non
VPN complet	HTTP	Non	Oui	Non	Non	Non
VPN complet	HTTPS	Oui, si la stratégie MDX Secure Web Active la mise en cache du mot de passe Web est définie sur Activé.	Non	Oui ; requis pour mettre en cache les informations d'identification dans Secure Web.	Non	Oui

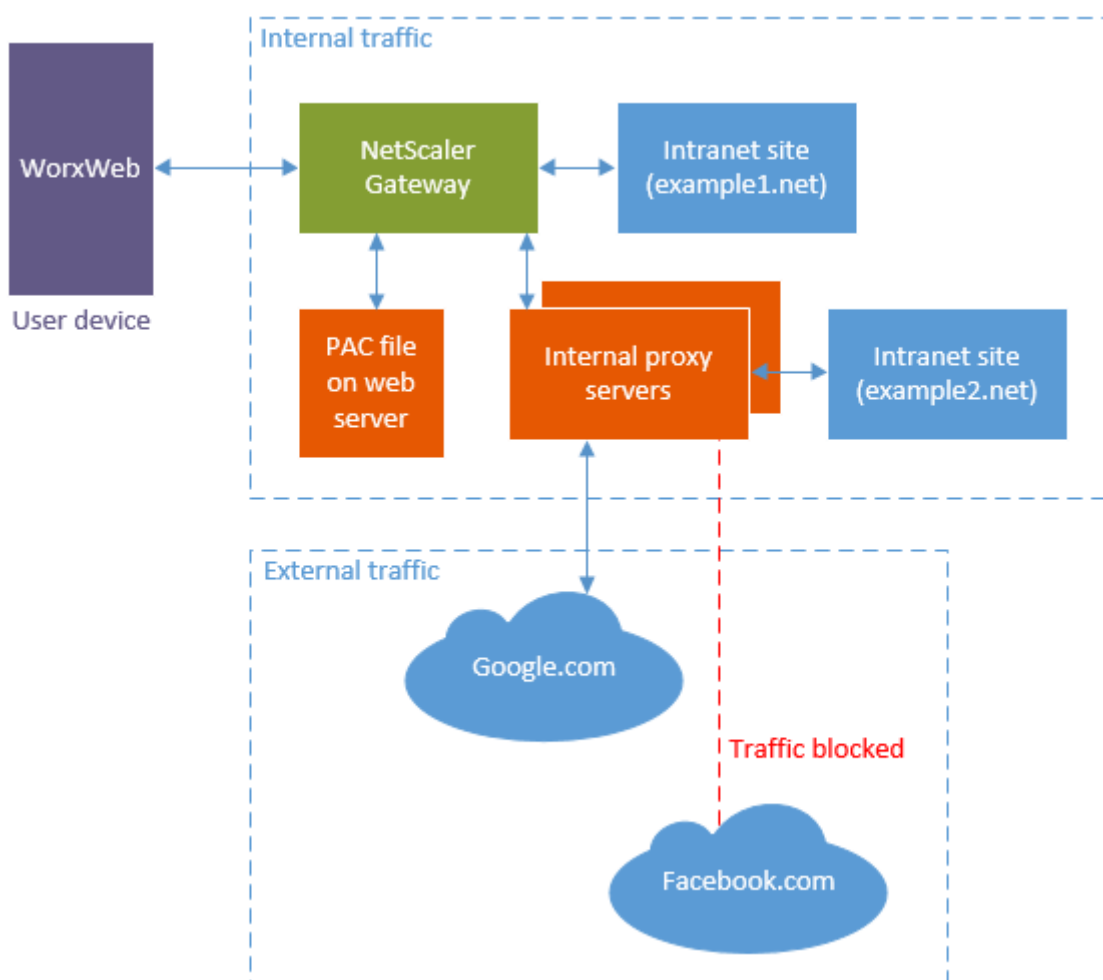
## Tunnelisation VPN complète avec le fichier PAC

Important :

Si Secure Web est configuré avec un fichier PAC et que Citrix ADC est configuré pour utiliser un proxy, Secure Web expire. Supprimez les stratégies de trafic Citrix Gateway configurées pour le proxy avant d'utiliser le paramètre Tunnel VPN complet avec le fichier PAC.

Lorsque vous configurez Secure Web pour la tunnelisation VPN complète avec votre fichier PAC ou un serveur proxy, Secure Web envoie l'ensemble du trafic au proxy via Citrix Gateway. Citrix Gateway achemine ensuite le trafic conformément aux règles de configuration du proxy. Dans cette configuration, Citrix Gateway ignore le fichier PAC ou le serveur proxy. Le flux du trafic est le même que pour la tunnelisation VPN complète sans PAC.

Le diagramme suivant illustre le flux du trafic lorsque les utilisateurs Secure Web accèdent à un site Web :



Dans cet exemple, les règles de trafic spécifient ce qui suit :

- Citrix Gateway se connecte directement au site intranet `example1.net`.

- Le trafic vers le site intranet [example2.net](#) est transmis par proxy via des serveurs proxy internes.
- Le trafic externe est transmis par proxy via des serveurs proxy internes. Les règles de proxy bloquent le trafic externe vers [Facebook.com](#).

## Pour configurer un tunnel VPN complet avec PAC

### 1. Validez et testez le fichier PAC.

Remarque :

Pour de plus amples informations sur la création et l'utilisation de fichiers PAC, accédez à [findproxyforurl.com/](#).

Validez votre fichier PAC à l'aide d'un outil de validation PAC tel que [Pacparser](#). Lorsque vous lisez votre fichier PAC, assurez-vous que les résultats Pacparser sont conformes à vos attentes. Si le fichier PAC contient une erreur de syntaxe, les appareils mobiles ignorent le fichier PAC de manière silencieuse. (Un fichier PAC est uniquement stocké dans la mémoire des appareils mobiles.)

Un fichier PAC est traité de haut en bas et le traitement s'arrête lorsqu'une règle correspond à la requête actuelle.

Testez l'URL du fichier PAC avec un navigateur Web avant d'entrer une valeur dans le champ **PAC/Proxy** de Endpoint Management. Assurez-vous que l'ordinateur peut accéder au réseau sur lequel le fichier PAC est situé.

<https://webserver.local/GenericPAC.pac>

<https://webserver.local/GenericPAC.pac>

Les extensions PAC testées sont .txt ou .pac.

Le fichier PAC doit afficher son contenu dans le navigateur Web.

Important :

Chaque fois que vous mettez à jour le fichier PAC utilisé avec Secure Web, informez les utilisateurs qu'ils doivent fermer et rouvrir Secure Web.

### 2. Configurez Citrix Gateway :

- Désactivez le split tunneling Citrix Gateway. Si le split tunneling est activé et qu'un fichier PAC est configuré, les règles du fichier PAC remplacent les règles de split tunneling de Citrix ADC. Un proxy ne remplace pas les règles de split tunneling de Citrix ADC.
- Supprimez les stratégies de trafic Citrix Gateway configurées pour le proxy. Cette étape est requise pour assurer le bon fonctionnement de Secure Web. La figure suivante montre un exemple de règles de stratégie à supprimer.

VPN Virtual Server Traffic Policy Binding		
<input type="button" value="Add Binding"/> <input type="button" value="Unbind"/> <input type="button" value="Edit"/>		
Priority	Policy Name	Expression
90	traf_pol_no_proxy_url_based	REQ.HTTP.HEADER CitrixSecureB
100	traf_pol_https_proxy	(REQ.HTTP.HEADER User-Agent C
110	traf_pol_http_proxy	(REQ.HTTP.HEADER User-Agent C

### 3. Configurez les stratégies Secure Web :

- Définissez la stratégie Mode VPN préféré sur **Tunnel VPN complet**.
- Définissez la stratégie Autoriser le basculement vers le mode VPN sur **Désactivé**.
- Configurez la stratégie URL du fichier PAC ou serveur proxy. Secure Web prend en charge HTTP et HTTPS en plus des ports par défaut et non par défaut. Pour HTTPS, l'autorité de certification racine doit être installée sur l'appareil si le certificat est auto-signé ou non fiable.

Veillez à tester l'adresse URL ou l'adresse du serveur proxy dans un navigateur Web avant de configurer la stratégie.

Exemple d'URL de fichier PAC :

`http[s]://example.com/proxy.pac`

`http[s]://10.10.0.100/proxy.txt`

Exemple de serveurs proxy (port obligatoire) :

`myhost.example.com:port`

`10.10.0.100:port`

Remarque :

si vous configurez un fichier PAC ou un serveur proxy, ne configurez pas PAC dans les paramètres de proxy du système pour le Wi-Fi.

- Définissez la stratégie Activer la mise en cache du mot de passe Web sur **Activé**. Cette dernière gère le SSO pour les sites HTTPS.

Citrix ADC peut effectuer l'authentification unique (SSO) pour les proxys internes si le proxy prend en charge la même infrastructure d'authentification.

### Limitations de prise en charge de fichier PAC

Secure Web ne prend pas en charge :

- Le basculement d'un serveur proxy à une autre. L'évaluation du fichier PAC peut renvoyer plusieurs serveurs proxy pour un nom d'hôte. Secure Web utilise uniquement le premier serveur proxy renvoyé.
- Les protocoles tels que FTP et Gopher dans un fichier PAC.
- Les serveurs proxy SOCKS dans un fichier PAC.
- Le protocole WPAD.

Secure Web ignore la fonction alert du fichier PAC de façon à ce que Secure Web puisse analyser un fichier PAC ne contenant pas ces appels.

### Stratégies Secure Web

Lors de l'ajout de Secure Web, tenez compte des stratégies MDX qui sont spécifiques à Secure Web. Pour tous les appareils mobiles pris en charge :

#### Sites Web autorisés ou bloqués

Secure Web ne filtre pas les liens Web. Vous pouvez utiliser cette stratégie pour configurer une liste spécifique de sites autorisés ou bloqués. Vous configurez des modèles d'adresse URL afin de limiter les sites Web que le navigateur est autorisé à ouvrir, sous forme de liste séparée par des virgules. Un signe plus (+) ou moins (-) précède chaque modèle dans la liste. Le navigateur compare une URL avec les modèles dans l'ordre indiqué jusqu'à ce qu'une correspondance soit trouvée. Lorsqu'une correspondance est trouvée, le préfixe détermine l'action suivante :

- Un préfixe - indique au navigateur de bloquer l'URL. Dans ce cas, l'URL est traitée comme si l'adresse du serveur Web ne peut pas être résolue.
- Un préfixe + autorise le traitement de l'URL.
- Si aucun préfixe (+ ou -) n'est fourni avec le modèle, + (autoriser) est la valeur par défaut.
- Si l'URL ne correspond à aucun modèle dans la liste, elle est autorisée.

Pour bloquer toutes les autres URL, ajoutez un signe moins suivi d'un astérisque (-\*) à la fin de la liste. Par exemple :

- La valeur de stratégie `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` autorise les URL HTTP avec le domaine `mycorp.com`, mais bloque celles provenant d'un autre domaine, autorise les URL HTTPS et FTP de n'importe quel domaine, et bloque toutes les autres URL.
- La valeur de la stratégie `+http://*.training.lab/*,+https://*.training.lab/*,-*` autorise les utilisateurs à ouvrir n'importe quel site dans le domaine `Training.lab` (intranet) via HTTP ou HTTPS. Cependant, cette valeur ne leur permet pas d'ouvrir des URL publiques, telles que Facebook, Google, Hotmail, etc, quel que soit le protocole utilisé.

La valeur par défaut est vide (toutes les URL sont autorisées).

### **Bloquer les fenêtres contextuelles**

Les fenêtres contextuelles sont de nouveaux onglets que les sites Web ouvrent sans votre autorisation. Cette stratégie détermine si Secure Web autorise les fenêtres contextuelles. Si ce paramètre est défini sur Activé, Secure Web empêche les sites Web d'ouvrir des fenêtres contextuelles. La valeur par défaut est Désactivé.

### **Signets pré-chargés**

Définit un ensemble de signets préchargés pour le navigateur Secure Web. La stratégie est une liste séparée par des virgules de tuples contenant le nom du dossier, un nom convivial et une adresse Web. Chaque triplet doit être au format dossier, nom, url où dossier et nom peuvent éventuellement être entourés de guillemets (“”).

À titre d'exemple, les valeurs de stratégies ,”Mycorp, Inc. home page”,<https://www.mycorp.com>, ”MyCorp Links”,Account logon,<https://www.mycorp.com/Accounts> ”MyCorp Links/Investor Relations”,”Contact us”,<https://www.mycorp.com/IR/Contactus.aspx> définissent trois signets. Le premier est un lien principal (aucun nom de dossier) appelé “Mycorp, Inc. home page”. Le second lien est placé dans un dossier “MyCorp Links” intitulé “Account logon”. Le troisième est placé dans le sous-dossier “Investor Relations” du dossier “MyCorp Links” et affiché en tant que “Contact us”.

La valeur par défaut est vide.

### **URL de page d'accueil**

Définit le site Web que Secure Web charge au démarrage. La valeur par défaut est vide (page de démarrage par défaut).

Pour les appareils Android et iOS pris en charge uniquement :

### **Interface utilisateur du navigateur**

Spécifie le comportement et la visibilité des contrôles de l'interface utilisateur du navigateur pour Secure Web. Tous les contrôles de navigation sont normalement disponibles. Cela comprend les contrôles suivant, précédent, barre d'adresses et actualiser/arrêter. Vous pouvez configurer cette stratégie pour restreindre l'utilisation et la visibilité de certains de ces contrôles. La valeur par défaut est Toutes les commandes visibles.

Options :

- **Toutes les commandes visibles.** Toutes les commandes sont visibles et les utilisateurs sont autorisés à les utiliser.

- **Barre d'adresses en lecture seule.** Toutes les commandes sont visibles, mais les utilisateurs ne peuvent pas modifier le champ d'adresse du navigateur.
- **Masquer la barre d'adresses.** Masque la barre d'adresses, mais pas les autres commandes.
- **Masquer toutes les commandes.** Supprime la barre d'outils complète pour offrir une expérience de navigation sans cadre.

### Activer la mise en cache du mot de passe Web

Lorsque les utilisateurs Secure Web entrent des informations d'identification lors de l'accès à une ressource Web ou la demande d'une ressource Web, cette stratégie détermine si Secure Web met en cache de façon silencieuse le mot de passe sur l'appareil. Cette stratégie s'applique aux mots de passe entrés dans les boîtes de dialogue d'authentification et non aux mots de passe entrés dans les formulaires Web.

Si l'option **Activé** est sélectionnée, Secure Web met en cache tous les mots de passe des utilisateurs lors de la demande d'une ressource Web. Si l'option **Désactivé** est sélectionnée, Secure Web ne met pas en cache les mots de passe et supprime les mots de passe en cache existants. La valeur par défaut est **Désactivé**.

Cette stratégie est activée uniquement lorsque vous définissez en parallèle la stratégie Mode VPN préféré sur Tunnel VPN complet pour cette application.

### Serveurs proxy

Vous pouvez également configurer des serveurs proxy pour Secure Web lorsque vous utilisez le mode Navigation sécurisée. Pour plus de détails, consultez cet [billet de blog](#).

### Suffixes DNS

Sur Android, si aucun suffixe DNS n'est configuré, le VPN peut échouer. Pour plus d'informations sur la configuration des suffixes DNS, consultez la section [Prise en charge de requêtes DNS à l'aide de suffixes DNS pour appareils Android](#).

### Préparation des sites intranet pour Secure Web

Cette section est destinée aux développeurs de sites Web ayant besoin de configurer un site intranet pour utiliser Secure Web sous Android et iOS. Les sites intranet conçus pour des navigateurs de bureau devront être modifiés pour fonctionner correctement sur les appareils Android et iOS.

Secure Web dépend de Android WebView et iOS WkWebView pour prendre en charge la technologie Web. Certaines des technologies Web prises en charge par Secure Web sont :

- AngularJS

- ASP .NET
- JavaScript
- jQuery
- WebGL
- WebSockets (uniquement en mode non restreint)

Certaines des technologies Web non prises en charge par Secure Web sont :

- Flash
- Java

Le tableau suivant dresse la liste des fonctionnalités de rendu HTML et des technologies prises en charge par Secure Web. X indique si la fonction est disponible pour une combinaison plate-forme, navigateur et composant.

Technologie	iOS Secure Web	Android 5.x/6.x/7.x Secure Web
Moteur JavaScript	JavaScriptCore	V8
Stockage local	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X
WebGL		X
requestAnimationFrame API		X
API Navigation Timing		X
API Resource Timing		X

Les technologies fonctionnent de la même façon sur tous les appareils ; cependant, Secure Web renvoie différentes chaînes d'agent utilisateur pour différents appareils. Pour déterminer la version de navigateur utilisée pour Secure Web, consultez la chaîne d'agent utilisateur. Depuis Secure Web, accédez à <https://whatsmyuseragent.com/>.

### Dépannage des sites intranet

Pour résoudre les problèmes d'affichage lorsque votre intranet est affiché dans Secure Web, comparez les affichages entre Secure Web et d'autres navigateurs compatibles tiers.



Pour iOS, les navigateurs tiers compatibles à des fins de test sont Chrome et Dolphin.

Pour Android, le navigateur tiers compatible à des fins de test est Dolphin.

Remarque :

Chrome est un navigateur natif d'Android. Ne l'utilisez pas pour la comparaison.

Dans iOS, assurez-vous que les navigateurs prennent en charge le VPN au niveau de l'appareil. Vous pouvez configurer cette prise en charge sur l'appareil en accédant à **Réglages > VPN > Ajouter une configuration VPN**.

Vous pouvez également utiliser des clients VPN disponibles sur l'App Store, tels que [Citrix VPN](#), [Cisco AnyConnect](#) ou [Pulse Secure](#).

- Si l'affichage d'une même page Web est identique sur les deux navigateurs, le problème vient de votre site Web. Mettez à jour votre site et vérifiez qu'il fonctionne correctement avec le système d'exploitation.
- Si le problème d'affichage d'une page Web apparaît uniquement dans Secure Web, contactez le support technique Citrix pour ouvrir un ticket d'assistance. Veuillez indiquer les étapes de résolution des problèmes que vous avez suivies, y compris les navigateurs et types de systèmes d'exploitation testés. Si vous rencontrez des problèmes d'affichage avec Secure Web pour iOS, incluez une archive Web de la page, comme décrit dans les étapes suivantes. Ceci permet à Citrix de résoudre le problème plus rapidement.

### Pour créer un fichier d'archive Web

En utilisant Safari sur macOS 10.9 ou une version ultérieure, vous pouvez enregistrer une page Web en tant que fichier d'archive Web (aussi appelé liste de lecture). Le fichier d'archive Web contient tous les fichiers liés, tels que les images, feuilles de style CSS et JavaScript.

1. Depuis Safari, videz le dossier de **liste de lecture** : dans le **Finder**, cliquez sur le menu **Aller** dans la barre des **menus**, cliquez sur **Aller au dossier**, tapez le nom du chemin d'accès `~/Bibliothèque/Safari/ReadingListArchives/`. Maintenant, supprimez tous les dossiers de cet emplacement.
2. Dans la barre des **menus**, accédez à **Safari > Préférences > Avancées** et activez **Afficher le menu Développement** dans la barre des menus.
3. Dans la barre des **menus**, accédez à **Développement > Agent d'utilisateur** et entrez l'agent d'utilisateur Secure Web : (Mozilla/5.0 (iPad; CPU OS 8\_3 like macOS) AppleWebKit/600.1.4 (KHTML, like Gecko) Mobile/12F69 Secure Web/ 10.1.0(build 1.4.0) Safari/8536.25).
4. Dans Safari, ouvrez le site Web à enregistrer en tant que liste de lecture (fichier d'archive Web).
5. Dans la barre des **menus**, accédez à **Signets > Ajouter à la liste de lecture**. Cette étape peut prendre plusieurs minutes. L'archivage se produit en arrière-plan.

6. Recherchez la liste de lecture archivée : dans la barre des **menus**, cliquez sur **Présentation > Afficher la barre latérale de la liste de lecture**.

7. Vérifiez le fichier d'archive :

- Désactivez la connectivité réseau sur votre Mac.
- Ouvrez le site Web à partir de la liste de lecture.

Le site Web est restitué complètement.

8. Comprimez le fichier d'archive : dans le **Finder**, cliquez sur le menu **Aller** dans la barre des **menus**, cliquez sur **Aller au dossier** et tapez le nom du chemin d'accès ~/Bibliothèque/Safari/ReadingListArchi. Ensuite, compressez le dossier qui a une chaîne hexadécimale aléatoire en tant que nom de fichier. Il s'agit du fichier que vous pouvez envoyer à l'assistance Citrix lorsque vous ouvrez un ticket d'assistance.

## Fonctionnalités Secure Web

Secure Web utilise des technologies d'échange de données mobiles pour créer un tunnel VPN dédié aux utilisateurs pour accéder aux sites Web internes et externes et tous les autres sites Web. Ceux-ci incluent les sites contenant des informations confidentielles dans un environnement sécurisé par les stratégies de votre organisation.

L'intégration de Secure Web avec Secure Mail et Citrix Files offre une expérience utilisateur transparente au sein du conteneur Endpoint Management sécurisé. Voici quelques exemples de fonctionnalités d'intégration :

- Lorsque les utilisateurs touchent des liens **mailto**, un nouveau message s'ouvre dans Secure Mail sans qu'aucune authentification supplémentaire ne soit requise.
- **Autoriser l'ouverture des liens dans Secure Web tout en assurant la sécurité des données.** Avec Secure Web pour iOS et Android, un tunnel VPN dédié permet aux utilisateurs d'accéder en toute sécurité aux sites contenant des informations sensibles. Ils peuvent cliquer sur des liens depuis Secure Mail, depuis Secure Web ou depuis une application tierce. Le lien s'ouvre dans Secure Web et les données restent sécurisées. Les utilisateurs peuvent ouvrir un lien interne avec le schéma `ctxmobilebrowser://` dans Secure Web. Secure Web transforme le préfixe `ctxmobilebrowser://` en `http://..`. Pour ouvrir un protocole HTTPS, Secure Web transforme `ctxmobilebrowsers://` en `https://`.

Cette fonctionnalité dépend d'une stratégie MDX d'interaction des applications appelée **Échange de documents entrants**. Par défaut, la stratégie est définie sur **Sans restriction**. Ce paramètre permet aux URL de s'ouvrir dans Secure Web. Vous pouvez modifier le paramètre de stratégie afin que seules les applications que vous incluez dans une liste verte puissent communiquer avec Secure Web.

- Lorsque les utilisateurs cliquent sur un lien intranet dans un e-mail, Secure Web accède à ce site sans authentification supplémentaire requise.

- Les utilisateurs peuvent charger des fichiers dans Citrix Files qu'ils téléchargent à partir du Web dans Secure Web.

Les utilisateurs de Secure Web peuvent également effectuer les actions suivantes :

- Bloquer les fenêtres contextuelles.

Remarque :

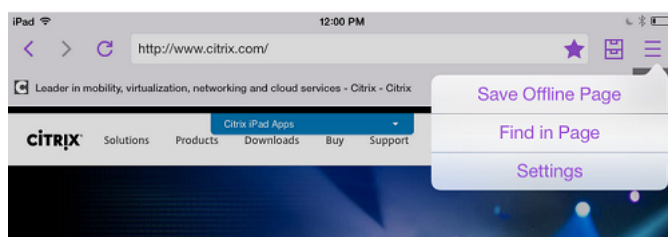
La majorité de la mémoire de Secure Web est consommée par le rendu des fenêtres contextuelles, par conséquent le blocage des fenêtres publicitaires dans les paramètres permet d'améliorer les performances.

- Placer en signet leurs sites favoris.
- Télécharger des fichiers.
- Enregistrer des pages hors connexion.
- Enregistrer automatiquement des mots de passe.
- Effacer le cache/l'historique/les cookies.
- Désactiver les cookies et le stockage local HTML5.
- Partager des appareils avec d'autres utilisateurs en toute sécurité.
- Effectuer des recherches dans la barre d'adresses.
- Autoriser les applications Web qu'ils exécutent dans Secure Web à déterminer leur position.
- Exporter et importer les paramètres.
- Ouvrir les fichiers directement dans Citrix Files sans avoir à les télécharger. Pour activer cette fonctionnalité, ajoutez **ctx-sf** à la stratégie URL autorisées dans Endpoint Management.
- Dans iOS, utilisez des actions tactiles 3D pour ouvrir un nouvel onglet et accéder aux pages en mode déconnecté, à des sites favoris et à des téléchargements directement à partir de l'écran d'accueil.
- Dans iOS, télécharger des fichiers de n'importe quelle taille et les ouvrir dans Citrix Files ou d'autres applications.

Remarque :

Si vous placez Secure Web en arrière-plan, le téléchargement s'arrêtera.

- Recherchez un terme dans la page affichée à l'aide de la fonction **Rechercher dans la page**.



Secure Web prend également en charge le texte dynamique, ce qui signifie qu'il affiche la police que les utilisateurs ont définie sur leurs appareils.

## Protection des données iOS

June 11, 2019

Les entreprises qui doivent satisfaire aux exigences du ASD (Australian Signals Directorate) en matière de protection des données peuvent utiliser la nouvelle stratégie **Activer la protection des données iOS** pour Secure Mail et Secure Web. Par défaut, les stratégies sont définies sur **Désactivé**.

Lorsque la stratégie **Activer la protection des données iOS** est définie sur **Activé** pour Secure Web, Secure Web utilise un niveau de protection de classe A pour tous les fichiers du sandbox. Pour plus d'informations sur la protection des données Secure Mail, reportez-vous à la section [Australian Signals Directorate Data Protection](#). Si vous activez cette stratégie, la classe de protection des données la plus élevée est utilisée. Il n'est donc pas nécessaire de spécifier également la stratégie **Classe de protection des données minimum**.

Pour modifier la stratégie **Activer la protection des données iOS** :

1. Utilisez la console Endpoint Management pour charger les fichiers MDX Secure Web et Secure Mail sur Endpoint Management : pour une nouvelle application, accédez à **Configurer > Applications > Ajouter**, puis cliquez sur **MDX**. Pour obtenir une mise à niveau, reportez-vous à la section [Mettre à niveau les applications MDX ou Enterprise](#).
2. Utilisez la console Endpoint Management pour charger les fichiers MDX sur Endpoint Management : pour une nouvelle application, accédez à **Configurer > Applications > Ajouter**, puis cliquez sur **MDX**. Pour obtenir une mise à niveau, reportez-vous à la section [Ajouter des applications](#).
3. Pour Secure Mail, accédez aux paramètres d'**application**, localisez la stratégie **Activer la protection des données iOS** et définissez-la sur **Activé**. Les appareils exécutant des systèmes d'exploitation plus anciens ne sont pas affectés lorsque cette stratégie est activée.
4. Pour Secure Web, accédez au Paramètres d'**application**, localisez la stratégie **Activer la protection des données iOS** et définissez-la sur **Activé**. Les appareils exécutant des systèmes d'exploitation plus anciens ne sont pas affectés lorsque cette stratégie est activée.

5. Configurez les stratégies applicatives et enregistrez vos paramètres pour déployer l'application sur le magasin d'applications Endpoint Management.

## Fonctionnalités Secure Web

June 19, 2020

Secure Web utilise des technologies d'échange de données mobiles pour créer un tunnel VPN dédié aux utilisateurs pour accéder aux sites Web internes et externes et tous les autres sites Web. Ceux-ci incluent les sites contenant des informations confidentielles dans un environnement sécurisé par les stratégies de votre organisation.

L'intégration de Secure Web avec Secure Mail et Citrix Files offre une expérience utilisateur transparente au sein du conteneur Endpoint Management sécurisé. Voici quelques exemples de fonctionnalités d'intégration :

- Lorsque les utilisateurs touchent des liens mailto, un nouveau message s'ouvre dans Secure Mail sans qu'aucune authentification supplémentaire ne soit requise.
- **Autoriser l'ouverture des liens dans Secure Web tout en assurant la sécurité des données.** Avec Secure Web pour iOS et Android, un tunnel VPN dédié permet aux utilisateurs d'accéder en toute sécurité aux sites contenant des informations sensibles. Ils peuvent cliquer sur des liens depuis Secure Mail, depuis Secure Web ou depuis une application tierce. Le lien s'ouvre dans Secure Web et les données restent sécurisées. Les utilisateurs peuvent ouvrir un lien interne avec le schéma `ctxmobilebrowser(s)` dans Secure Web. Secure Web transforme le préfixe `ctxmobilebrowser://` en `http://..`. Pour ouvrir un protocole HTTPS, Secure Web transforme `ctxmobilebrowsers://` en `https://`.

Cette fonctionnalité dépend d'une stratégie MDX d'interaction des applications appelée **Échange de documents entrants**. Par défaut, la stratégie est définie sur **Sans restriction**. Ce paramètre permet aux URL de s'ouvrir dans Secure Web. Vous pouvez modifier le paramètre de stratégie afin que seules les applications que vous incluez dans une liste verte puissent communiquer avec Secure Web.

- Lorsque les utilisateurs cliquent sur un lien intranet dans un e-mail, Secure Web accède à ce site sans authentification supplémentaire requise.
- Les utilisateurs peuvent charger des fichiers dans Citrix Files qu'ils téléchargent à partir du Web dans Secure Web.

Les utilisateurs de Secure Web peuvent également effectuer les actions suivantes :

- Bloquer les fenêtres contextuelles.

Remarque :

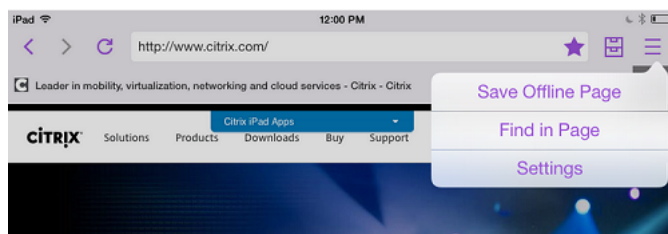
La majorité de la mémoire de Secure Web est consommée par le rendu des fenêtres contextuelles, par conséquent le blocage des fenêtres publicitaires dans les paramètres permet d'améliorer les performances.

- Placer en signet leurs sites favoris.
- Télécharger des fichiers.
- Enregistrer des pages hors connexion.
- Enregistrer automatiquement des mots de passe.
- Effacer le cache/l'historique/les cookies.
- Désactiver les cookies et le stockage local HTML5.
- Partager des appareils avec d'autres utilisateurs en toute sécurité.
- Effectuer des recherches dans la barre d'adresses.
- Autoriser les applications Web qu'ils exécutent dans Secure Web à déterminer leur position.
- Exporter et importer les paramètres.
- Ouvrir les fichiers directement dans Citrix Files sans avoir à les télécharger. Pour activer cette fonctionnalité, ajoutez **ctx-sf** à la stratégie URL autorisées dans Endpoint Management.
- Dans iOS, utilisez des actions tactiles 3D pour ouvrir un nouvel onglet et accéder aux pages en mode déconnecté, à des sites favoris et à des téléchargements directement à partir de l'écran d'accueil.
- Dans iOS, télécharger des fichiers de n'importe quelle taille et les ouvrir dans Citrix Files ou d'autres applications.

Remarque :

Si vous placez Secure Web en arrière-plan, le téléchargement s'arrêtera.

- Recherchez un terme dans la page affichée à l'aide de la fonction **Rechercher dans la page**.



Secure Web prend également en charge le texte dynamique, ce qui signifie qu'il affiche la police que les utilisateurs ont définie sur leurs appareils.



**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States  
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).