CITRIX

# Secure Web

# Contents



 

# Nouveautés dans Secure Web

March 7, 2019

## Nouveautés de la version 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. Ils peuvent cliquer sur des liens depuis Secure Mail pour Android, 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 blanche puissent communiquer avec Secure Web.

## Nouveautés dans les versions précédentes

Les versions 18.11.5 à 19.1.5 de Secure Web incluent des corrections de bogues et des améliorations des performances.

### 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 18.10.5

Les versions 18.9.0 à 18.10.5 de Secure Web incluent des corrections de bogues et des améliorations des performances.

### 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 séparé à l'aide d'applications d'entreprise Android dans Secure Mail. Pour de plus amples informations, consultez la section Android Entreprise 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

March 7, 2019

### Problèmes connus et résolus dans la version 19.2.0

Il n'existe pas de problème connu ou résolu dans la version 19.2.0.

### Problèmes connus et résolus dans les versions précédentes

#### Problème résolu dans la version 19.1.5

- Dans Secure Web pour iOS, vous ne pouvez pas télécharger un fichier PDF avec l'extension .dwg. [CXM-60509]

#### Problèmes connus et résolus dans la version 19.1.0

Il n'existe pas de problèmes connus ou résolus dans la version 19.1.0

#### Problème connu dans la version 18.12.0

- Dans Secure Web pour iOS, les vidéos intégrées provenant de sites Web externes tels que CNBC ne sont pas visibles. [CXM-59576]

#### Problème connu dans la version 18.11.5

- Dans Secure Web pour iOS, si une vidéo est lue à l'aide de UIWebView, le lecteur multimédia se bloque lorsque la vidéo est affichée en plein écran plusieurs fois. [CXM-58800]

 

**Problèmes résolus dans la version 18.11.0**

- Dans Secure Web pour iOS, vous ne pouvez pas imprimer de fichiers avec AirPrint. Secure Web pour iOS ne prend pas en charge AirPrint. [CXM-56001]
- Dans Secure Web pour iOS, certains sites Web ne sont pas correctement dimensionnés, ce qui entraîne un zoom avant de la page Web. [CXM-58283]
- Dans Secure Web pour iOS, des caractères spéciaux apparaissent par intermittence lorsque vous affichez certains sites Web en turc. [CXM-58412]

**Problèmes connus dans la version 10.8.60**

- Dans Secure Web pour iOS, les sites internes ne sont pas accessibles à partir de l'environnement Workspace, alors que les sites externes le sont. [CXM-55921]

Les problèmes suivants sont résolus dans Secure Web. La liste comprend les problèmes liés à MDX qui affectent Secure Web.

**Problèmes résolus dans la version 10.8.65**

- Dans Secure Web pour iOS, les sites internes ne sont pas accessibles à partir de l'environnement Workspace, alors que les sites externes le sont. [CXM-55921]

**Problèmes résolus dans la version 10.8.60**

- Secure Web pour iOS se bloque lors du lancement à partir de Secure Hub lors d'une nouvelle installation.[CXM-55417]

**Problèmes résolus dans la version 10.8.55**

- Dans Secure Web pour iOS, l'icône de rotation apparaît bien que certaines pages Web aient été chargées avec succès sur l'appareil. [CXM-52889]

**Problèmes résolus dans la version 10.8.50**

- Lorsque la stratégie Échange de documents est définie sur Restreint, Secure Web cesse de fonctionner après avoir tenté de télécharger un fichier. [CXM-48447]
- Secure Web pour iOS se bloque lors de la soumission des identifiants de connexion. Ce problème se produit par intermittence lorsque Secure Web tente de publier des données depuis une page Web sécurisée vers une page Web non sécurisée. [CXM-52977]

 

#### Problèmes résolus dans la version 10.8.45

- Lorsqu'un fichier auto-config proxy avec dnsResolve défini est configuré en mode Tunnel complet, la navigation sur Secure Web est sensiblement lente. [CXM-49567]
- Lorsque vous effectuez un zoom avant par pincement, Secure Web pour Android actualise la page Web. [CXM-53026]

#### Problèmes résolus dans la version 10.8.40

Dans Secure Web pour iOS, le passage en mode Bureau entraîne un rendu incorrect de la page Web. Ce problème se produit par intermittence lorsque vous passez en mode Mobile. [CXM-52847]

#### Problèmes résolus dans la version 10.8.26

Le problème suivant a été résolu dans la version 10.8.26 :

- En raison d'une mise à jour vers Chrome 67 ou version ultérieure, des problèmes se produisent lorsque les utilisateurs accèdent à des sites intranet via Secure Web pour Android lors de l'utilisation de la navigation sécurisée. Pour de plus amples informations, consultez cet article du centre de connaissances. [CXM-52186]

#### Problèmes résolus dans la version 10.8.10

##### Secure Web pour iOS

Après la mise à jour de Secure Web pour iOS vers la version 10.7.25, les utilisateurs ne peuvent pas rejoindre de réunions Skype. Au lieu de cela, l'App Store s'ouvre pour l'application Lync. [CXM-46336]

##### Secure Web pour Android

Sur les appareils qui utilisent l'API WebView, y compris Secure Web pour Android, vous ne pouvez pas joindre d'images à partir d'une galerie bien que la stratégie MDX Bloquer la galerie soit **désactivée**. [CXM-41475]

## Intégration et déploiement de Secure Web

January 25, 2019

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 Worx, 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, veuillez consulter la section À propos des 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 :**

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

**Stratégie MDX Liste d'exclusion de split tunneling inverse dans Citrix Endpoint Management :**
Vous configurez la stratégie de mode de split tunneling inverse avec la plage Exclusion. 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 |

 

| 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 change-ment de mot de passe |
|---|---|---|---|---|---|---|
| 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 Activer la mise en cache du mot de passe Web est définie sur Activé. | Non | Oui ; requis pour mettre en cache les in-formations 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, consultez https://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 du fichier PAC testé sont .txt ou .pac.

   Le fichier PAC devrait 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.

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, ainsi que par les ports par défaut et les ports autres que ceux 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 pouvait 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 d'informations, consultez ce billet de blog.

#### Suffixes DNS

Sur Android, si aucun suffixe DNS n'est configuré, le VPN peut échouer. Pour de plus amples informations sur la configuration de suffixes DNS, reportez-vous à 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 UIWebView 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

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 apparait 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

À l'aide de 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) qui 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/, puis supprimez tous les dossiers dans 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 que vous allez 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 doit s'afficher complètement.
8. Compressez 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/ReadingListArc
   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 Citrix Secure Mail sans qu'aucune authentification supplémentaire ne soit requise.
- Dans iOS, les utilisateurs peuvent ouvrir un lien dans Secure Web à partir d'une application de messagerie native en insérant **ctxmobilebrowser://** au début de l'adresse URL. À titre d'exemple, pour ouvrir le lien `example.com` dans une application de messagerie native, utilisez l'adresse URL ctxmobilebrowser://example.com.
- 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 HTML 5.
- 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

February 19, 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 obtenir des informations détaillées sur la protection de données Secure Mail, consultez 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 une mise à niveau, consultez la section Mettre à niveau les applications MDX ou d'entreprise.
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 une mise à niveau, voir 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.

 

 

**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