citrix

Secure Web

Contents

Neue Features in Secure Web

November 21, 2020

> **Hinweis:**
>
> Die Unterstützung für die Android 6.x- und iOS 11.x-Versionen von Secure Hub, Secure Mail, Secure Web und Citrix Workspace-App endet im Juni 2020.

Neue Features in der aktuellen Version

Secure Web 20.11.0

Dieses Release enthält Fehlerbehebungen.

Was ist neu in früheren Releases

Secure Web 20.10.5

Secure Web für Android

Unterstützung für AndroidX-Bibliotheken. Gemäß der Empfehlung von Google unterstützt Secure Web die **AndroidX**-Bibliotheken, die ein Ersatz für die **android.support**-Bibliothekspakete sind.

Secure Web 20.10.0

Secure Web für Android

Secure Web unterstützt die aktuellen API-Anforderungen von Google Play für Android 10.

Secure Web 20.9.5

Secure Web für iOS

Dieses Release enthält Fehlerbehebungen.

Secure Web 20.9.0

Secure Web für Android

> **Hinweis:**
>
> Support für Android 6.x endete am 15. September 2020.

Secure Web 20.8.5

Secure Web für Android

Secure Web für Android unterstützt Android 11.

Secure Web 20.8.0

Secure Web für Android

Dualmodus (Vorschau) für Android-Version von Secure Web. Ein MAM-SDK zur Mobilanwendungsverwaltung ist verfügbar, um Bereiche der MDX-Funktionalität zu ersetzen, die nicht von den iOS- und Android-Plattformen abgedeckt sind. Die MDX-Technologie soll das Ende des Lebenszyklus (EOL) im September 2021 erreichen. Um die Verwaltung Ihrer Unternehmensanwendungen fortzusetzen, müssen Sie das MAM-SDK integrieren.

Ab Version 20.8.0 werden Android-Apps mit MDX und dem MAM-SDK veröffentlicht, in Vorbereitung des zuvor erwähnten Endes des Lebenszyklus für MDX. Der MDX-Dualmodus soll den Übergang vom Legacy-MDX Toolkit auf neue MAM-SDKs erleichtern. Mit dem Dualmodus können Sie Apps entweder wie gehabt mit MDX Toolkit (jetzt **Legacy-MDX**) verwalten oder zum neuen MAM-SDK wechseln.

Sobald Sie das MAM-SDK zur App-Verwaltung verwenden, implementiert Citrix weitere Änderungen, ohne erforderliche Aktion der Administratoren.

Weitere Informationen zum MAM-SDK (Vorschau) finden Sie in den folgenden Artikeln:

- Überblick über das MAM-SDK
- Citrix Developer-Abschnitt zur Geräteverwaltung
- Citrix Blogbeitrag
- SDK-Download bei der Registrierung für Citrix Downloads

Voraussetzungen

Stellen Sie Folgendes sicher, um das Dualmodus-Feature erfolgreich bereitzustellen:

- Aktualisieren Sie Citrix Endpoint Management auf die Versionen 10.12 RP2 und höher oder 10.11 RP5 und höher.
- Aktualisieren Sie Ihre mobilen Apps auf die Version 20.8.0 oder höher.
- Aktualisieren Sie die Richtliniendatei auf Version 20.8.0 oder höher.
- Wenn Ihre Organisation Drittanbieter-Apps verwendet, müssen Sie das MAM-SDK in diese Drittanbieter-Apps integrieren, bevor Sie zur MAM-SDK-Option für Ihre mobilen Produktivitätsapps von Citrix wechseln. Alle verwalteten Apps müssen gleichzeitig in das MAM-SDK verschoben werden.

> **Hinweis:**
>
> Das MAM-SDK wird für alle cloudbasierten Kunden unterstützt.

Einschränkungen

- Das MAM-SDK wird nur für Apps unterstützt, die unter der Android Enterprise-Plattform in Ihrer Citrix Endpoint Management-Bereitstellung veröffentlicht wurden. Bei den neu veröffentlichten Apps ist die Standardverschlüsselung die plattformbasierte Verschlüsselung.
- Das MAM-SDK unterstützt nur die plattformbasierte Verschlüsselung und keine MDX-Verschlüsselung.
- Wenn Sie Citrix Endpoint Management nicht aktualisieren und die Richtliniendateien für die mobilen Apps auf Version 20.8.0 und höher ausgeführt werden, werden doppelte Einträge der Netzwerkrichtlinie für Secure Web erstellt.

Wenn Sie Secure Web in Citrix Endpoint Management konfigurieren, können Sie mit dem Dualmodus Apps entweder wie gehabt mit MDX Toolkit (jetzt **Legacy-MDX**) verwalten oder zum neuen **MAM-SDK** wechseln. Citrix empfiehlt den Wechsel zum **MAM-SDK**, da MAM-SDKs modularer aufgebaut sind und Ihnen ermöglichen sollen, nur eine Teilmenge der MDX-Funktionalität Ihrer Organisation zu verwenden. Dies reduziert den In-Binary- und Laufzeitaufwand einer App.

Sie erhalten die folgenden Optionen für Richtlinieneinstellungen im **Richtliniencontainer für MDX oder MAM SDK**:

- **MAM-SDK**
- **Legacy-MDX**

In der Richtlinie **Richtliniencontainer für MDX oder MAM SDK** können Sie Ihre Option nur von **Legacy-MDX** in “MAM-SDK” ändern. Ein Wechsel von “MAM-SDK” zu **Legacy-MDX** ist nicht zulässig. Anschließend müssen Sie die App neu veröffentlichen. Der Standardwert ist “Legacy-MDX”. Stellen Sie sicher, dass Sie für Secure Mail und Secure Web auf einem Gerät denselben Richtlinienmodus festlegen. Sie können nicht zwei verschiedene Modi auf demselben Gerät ausführen.

Secure Web 20.7.5

Dieses Release enthält Fehlerbehebungen.

Secure Web 20.7.0

Unterstützung für Multitasking. Verwenden Sie in Secure Web für iOS zwei Apps gleichzeitig mit Multitasking. Um diese Funktion zu aktivieren, ziehen Sie eine App aus dem Dock. Schieben Sie sie an den rechten oder linken Rand des Bildschirms, um den Bildschirm zu teilen und für zwei Apps zu aktivieren.

Aktuelle Informationen zu mobilen Produktivitätsapps finden Sie im Artikel Aktuelle Ankündigungen.

Secure Web 20.6.0

Dieses Release enthält Fehlerbehebungen.

Secure Web 20.5.0

Dieses Release enthält Fehlerbehebungen.

Secure Web 20.4.5

Navigieren zu Lesezeichen auf neuen Registerkarten. In Secure Web für iOS können Sie Lesezeichen anzeigen, bearbeiten und dahin navigieren, wenn Sie eine neue Registerkarte öffnen.

Secure Web 19.10.5 bis 20.4.0

Diese Releases enthalten Fixes für Bugs.

Secure Web 19.10.0

Secure Web iOS und Android unterstützen die Verschlüsselungsverwaltung. Mit der Verschlüsselungsverwaltung können Sie moderne Geräteplattformsicherheit nutzen und gleichzeitig sicherstellen, dass das Gerät in einem ausreichenden Zustand bleibt, um die Plattformsicherheit effektiv zu nutzen. Durch die Verschlüsselungsverwaltung eliminieren Sie die Redundanz der lokalen Datenverschlüsselung, da die Dateisystemverschlüsselung von der iOS- oder Android-Plattform bereitgestellt wird. Um dieses Feature zu aktivieren, müssen Administratoren in der Citrix Endpoint Management-Konsole die MDX-Richtlinie **Verschlüsselungstyp** auf **Plattformverschlüsselung mit Durchsetzen der Compliance** festlegen.

Mit der Verschlüsselungsverwaltung können Sie moderne Geräteplattformsicherheit nutzen und gleichzeitig sicherstellen, dass das Gerät in einem ausreichenden Zustand bleibt, um die Plattformsicherheit effektiv zu nutzen. Durch die Verschlüsselungsverwaltung eliminieren Sie die Redundanz der lokalen Datenverschlüsselung, da die Dateisystemverschlüsselung von der iOS- oder Android-Plattform bereitgestellt wird. Um dieses Feature zu aktivieren, müssen Administratoren in der Citrix Endpoint Management-Konsole die MDX-Richtlinie **Verschlüsselungstyp** auf **Plattformverschlüsselung mit Durchsetzen der Compliance** festlegen.

Verschlüsselungstyp

Um die Verschlüsselungsverwaltung zu verwenden, legen Sie in der Citrix Endpoint Management-Konsole die Richtlinie **Verschlüsselungstyp** auf **Plattformverschlüsselung mit Durchsetzen der Compliance** fest. Dies ermöglicht die Verschlüsselungsverwaltung und alle vorhandenen verschlüsselten Anwendungsdaten auf Benutzergeräten nahtlos in einen Zustand übergehen, der vom Gerät und nicht von MDX verschlüsselt wird. Während dieser Umstellung wird die App für eine einmalige Datenmigration angehalten. Bei erfolgreicher Migration wird die Verantwortung für die Verschlüsselung lokal gespeicherter Daten von MDX auf die Geräteplattform übertragen. MDX überprüft weiterhin die Compliance des Geräts bei jedem App-Start. Dieses Feature funktioniert sowohl in MDM + MAM- als auch in Nur-MAM-Umgebungen.

Wenn Sie die Richtlinie **Verschlüsselungstyp** auf **Plattformverschlüsselung mit Durchsetzen der Compliance** festlegen, ersetzt die neue Richtlinie die vorhandene MDX-Verschlüsselung.

Weitere Informationen zu den MDX-Richtlinien für die Verschlüsselungsverwaltung in Secure Web finden Sie im Abschnitt **Verschlüsselung** unter:

- MDX-Richtlinien für mobile Produktivitätsapps für iOS
- MDX-Richtlinien für mobile Produktivitätsapps für Android

Verhalten für nicht richtlinientreue Geräte

Wenn ein Gerät unter die Mindestanforderungen für die Compliance fällt, können Sie mit der Richtlinie **Verhalten für nicht richtlinientreue Geräte** wählen, welche Aktion ausgeführt wird:

- **App zulassen** — Zulassen, dass die App normal ausgeführt wird.
- **App nach Warnung zulassen** — Benutzer warnen, dass eine App die Mindestanforderungen für die Compliance nicht erfüllt. Das Ausführen der App zulassen. Dies ist der Standardwert.
- **App blockieren** — Das Ausführen der App wird blockiert.

Die folgenden Kriterien bestimmen, ob ein Gerät die Mindestanforderungen für die Compliance erfüllt.

Auf Geräten mit iOS:

- iOS 10: Die App führt Betriebssystemversion aus, die größer oder gleich der angegebenen Version ist.
- Debuggerzugriff: Für die App ist das Debugging nicht aktiviert.
- Gerät mit Jailbreak: Die App wird nicht auf einem Gerät mit Jailbreak ausgeführt.
- Gerätepasscode: Gerätepasscode ist aktiviert.
- Datenfreigabe: Die Datenfreigabe ist für die App nicht aktiviert.

Auf Geräten mit Android:

- Android SDK 24 (Android 7 Nougat): Die App führt eine Betriebssystemversion aus, die größer oder gleich der angegebenen Version ist.
- Debuggerzugriff: Für die App ist das Debugging nicht aktiviert.
- Gerät mit Rooting: Eine App wird nicht auf einem Gerät mit Rooting ausgeführt.

- Gerätesperre: Der Gerätepasscode ist aktiviert.
- Gerät verschlüsselt: Die App wird auf einem verschlüsselten Gerät ausgeführt.

Secure Web 19.9.5

Dieses Release enthält Fehlerbehebungen.

Secure Web 19.9.0

Secure Web für iOS

Secure Web für iOS unterstützt iOS 13.

Secure Web für Android

Dieses Release enthält Fehlerbehebungen.

Secure Web für Android 19.8.5

Secure Web für Android unterstützt Android Q.

Secure Web 19.8.0

Dieses Release enthält Fehlerbehebungen.

Secure Web 19.7.5

Secure Web für iOS

Dieses Release enthält Leistungsverbesserungen und Fehlerbehebungen.

Secure Web für Android

Ab diesem Release wird Secure Web für Android nur auf Geräten unterstützt, auf denen Android 6 und höher ausgeführt wird.

Secure Web 19.3.0 bis 19.6.5

Diese Releases enthalten Leistungsverbesserungen und Fehlerbehebungen.

Secure Web 19.2.0

Zulassen, dass Links in Secure Web unter Wahrung der Datensicherheit geöffnet werden. In Secure Web können Benutzer über einen dedizierten VPN-Tunnel sicher auf Sites mit vertraulichen Informationen zugreifen. Dieses Feature war bereits für Secure Web für iOS verfügbar. Mit diesem Release wird das Feature auch für Android unterstützt. Weitere Informationen finden Sie unter Secure Web-Features.

Secure Web-Versionen 18.11.5 bis 19.1.5

Diese Releases enthalten Leistungsverbesserungen und Fehlerbehebungen.

Secure Web 18.11.0

In Secure Web für iOS wird die Sitecachegrößenliste nicht mehr gemeldet und nicht mehr in den App-Einstellungen angezeigt. Die standardmäßige Cachingfunktionalität ist unverändert.

Secure Web 18.9.0 bis 18.10.5

Diese Releases enthalten Leistungsverbesserungen und Fehlerbehebungen.

Secure Web 10.8.65

Die folgenden Features sind neu in Secure Web 10.8.65:

- **Zum Aktualisieren ziehen.** In Secure Web für iOS können Benutzer mit der Funktion “Zum Aktualisieren ziehen” die Daten auf dem Bildschirm aktualisieren.
- **Suchen mit der Option “Auf Seite suchen”.** Mit der Option **Auf Seite suchen** können Sie umgehend nach Zeichenfolgen suchen. Diese Option hebt die Schlüsselwörter bei der Suche hervor und zeigt die gesamten Treffer auf der rechten Seite der Symbolleiste an. Beim Neustart behält diese Funktion die zuletzt gesuchten Schlüsselwörter bei.
- **Zum Ausblenden der Kopf- und Fußzeilenzeilen nach oben scrollen.** In Secure Web für iOS sind die Kopf- und Fußzeilenleisten ausgeblendet, während Sie nach oben scrollen. Auf diese Weise können beim Betrachten von Webseiten weitere Informationen auf Ihrem mobilen Bildschirm angezeigt werden.

Secure Web 10.8.60

- Unterstützung für die polnische Sprache

Secure Web 10.8.35

- **Zum Aktualisieren ziehen.** In Secure Web für Android können Benutzer mit der Funktion “Zum Aktualisieren ziehen” die Daten auf dem Bildschirm aktualisieren.

Secure Web 10.8.15

- **Secure Web unterstützt Android Enterprise (zuvor “Android for Work”)**. Sie können ein separates Arbeitsprofil erstellen, indem Sie Android Enterprise-Apps in Secure Mail verwenden. Einzelheiten finden Sie unter Android Enterprise in Secure Mail.
- **Secure Web für Android kann Webseiten im Desktopmodus wiedergeben**. Wählen Sie im Überlaufmenü die Option **Desktopsite anfordern**. Secure Web zeigt dann die Desktopversion der Website an.

Secure Web 10.8.10

- **Secure Web für iOS kann Webseiten im Desktopmodus wiedergeben.** Wählen Sie im Hamburgermenü die Option **Desktopsite anfordern**. Secure Web zeigt dann die Desktopversion der Website an.

Secure Web 10.8.5

Secure Mail und Secure Web für iOS und Android haben überarbeitete Schriftarten, Farben und andere UI-Verbesserungen. Die visuelle Neugestaltung bietet eine reichere Benutzererfahrung und reiht sich perfekt in die Markenästhetik der gesamten App-Suite von Citrix ein.

Bekannte und behobene Probleme

November 21, 2020

Citrix unterstützt Upgrades von den letzten zwei Versionen der mobilen Produktivitätsapps.

Secure Web 20.11.0

In diesem Release gibt es keine bekannten oder behobene Probleme.

Secure Web 20.10.5

Secure Web für Android

In diesem Release gibt es keine bekannten oder behobene Probleme.

Secure Web 20.10.0

Secure Web für Android

In diesem Release gibt es keine bekannten oder behobene Probleme.

Bekannte und behobene Probleme in älteren Versionen

Bekannte und behobene Probleme in älteren Versionen von Secure Web finden Sie unter Bekannte und behobene Probleme in älteren Versionen.

Integrieren und Bereitstellen von Secure Web

July 2, 2020

Das generelle Verfahren zum Integrieren und Bereitstellen von Secure Web ist folgendes:

1. Zum Aktivieren von SSO für das interne Netzwerk konfigurieren Sie Citrix Gateway.

   Für HTTP-Datenverkehr bietet Citrix ADC Single Sign-On für alle von Citrix ADC unterstützten Proxy-Authentifizierungstypen. Für HTTPS-Verkehr ermöglicht die Richtlinie für die Kennwortzwischenspeicherung, dass Secure Web Authentifizierungen durchführen und SSO für den Proxyserver über MDX bereitstellen kann. MDX unterstützt nur Standard-, Digest- und NTLM-Proxyauthentifizierung. Das Kennwort wird mit MDX zwischengespeichert und im freigegebenen Endpoint Management-Tresor, einem sicheren Speicher für vertrauliche Anwendungsdaten, gespeichert. Weitere Informationen zur Citrix Gateway-Konfiguration finden Sie unter Citrix Gateway.

2. Laden Sie Secure Web herunter.
3. Legen Sie fest, wie Benutzerverbindungen mit dem internen Netzwerk konfiguriert werden.
4. Zum Hinzufügen von Secure Web zu Endpoint Management führen Sie die gleichen Schritte wie bei anderen MDX-Apps aus und konfigurieren Sie dann die MDX-Richtlinien. Informationen zu Secure Web-spezifischen Richtlinien finden Sie unter Secure Web-Richtlinien.

Konfigurieren von Benutzerverbindungen

Secure Web unterstützt die folgenden Konfigurationen für Benutzerverbindungen:

- **Secure Browse:** Verbindungen, die einen Tunnel zum internen Netzwerk benötigen, können eine Variante eines clientlosen VPNs (Secure browse) verwenden. Diese Konfiguration ist der Standard für die Richtlinie **Bevorzugter VPN-Modus**. Die Einstellung "Secure Browse" wird für Verbindungen empfohlen, die Single Sign-On (SSO) erfordern.
- **Vollständiger VPN-Tunnel:** Verbindungen, die einen Tunnel zum internen Netzwerk benötigen, können einen vollständigen VPN-Tunnel verwenden, der mit der Richtlinie **Bevorzugter VPN-Modus** konfiguriert wird. Die Einstellung "Vollständiger VPN-Tunnel" wird für Verbindungen empfohlen, die Clientzertifikate oder End-To-End-SSL für Ressourcen im internen Netzwerk einsetzen. Vollständiger VPN-Tunnel unterstützt beliebige Protokolle über TCP und kann mit Windows- und Mac-Computern sowie iOS- und Android-Geräten verwendet werden.
- Die Richtlinie **VPN-Moduswechsel zulassen** ermöglicht bei Bedarf den automatischen Wechsel zwischen den Modi "Vollständiger VPN-Tunnel" und "Secure Browse". Standardmäßig ist diese Richtlinie deaktiviert. Wenn die Richtlinie aktiviert ist, werden Netzwerkanfragen, die fehlschlagen, weil eine Authentifizierungsanfrage nicht im bevorzugten VPN-Modus verarbeitet werden konnte, in dem anderen Modus erneut versucht. Beispielsweise können im vollständigen VPN-Tunnel-Modus Serveraufforderungen für Clientzertifikate erfüllt werden, aber nicht im Secure Browse-Modus. Ähnlich werden HTTP-Authentifizierungsaufforderungen mit Single Sign-On eher bedient, wenn "Secure Browse" verwendet wird.
- **Vollständiger VPN-Tunnel mit PAC:** Sie können eine PAC-Datei (Proxy Automatic Configuration) mit einem vollständigen VPN-Tunnel für iOS- und Android-Geräte verwenden. Eine PAC-Datei enthält Regeln, die festlegen, wie Webbrowser einen Proxy für den Zugriff auf eine URL auswählen. Mit Regeln in einer PAC-Datei kann die Handhabung von internen und externen Sites festgelegt werden. Secure Web analysiert die Regeln in der PAC-Datei und sendet die Proxyserverinformationen an Citrix Gateway.
- Die Leistung des vollständigen VPN-Tunnels bei Verwendung einer PAC-Datei ist mit dem Modus "Secure Browse" vergleichbar. Weitere Informationen über die PAC-Konfiguration finden Sie unter Vollständiger VPN-Tunnel mit PAC.
- **Reverse-Split-Tunnel:** Im Modus **REVERSE** umgeht der Datenverkehr für Intranet-Anwendungen den VPN-Tunnel, während der andere Datenverkehr den VPN-Tunnel durchläuft. Diese Richtlinie kann verwendet werden, um den gesamten nicht lokalen LAN-Verkehr zu protokollieren.

Konfigurationsschritte für Reverse-Split-Tunneling

Führen Sie folgende Schritte aus, um den Modus "Reverse-Split-Tunneling" auf dem Citrix Gateway zu konfigurieren:

1. Navigieren Sie zur Richtlinie **Richtlinien > Sitzung**.

2. Wählen Sie die Secure Hub-Richtlinie aus und navigieren Sie zu **Clienterlebnis > Split-Tunnel**.
3. Wählen Sie **REVERSE** aus.

MDX-Richtlinie “Ausschlussliste für Reverse-Split-Tunneling”

Sie konfigurieren die Richtlinie für das Reverse-Split-Tunneling in Citrix Endpoint Management mit einer Ausschlussliste. Es handelt sich um eine kommagetrennte Liste von DNS-Suffixen und FQDNs. Die Liste enthält die URLs, deren Datenverkehr über das lokale Netzwerk (LAN) des Geräts (anstelle von Citrix ADC) gesendet werden muss.

In der folgenden Tabelle wird aufgeführt, wann Secure Web die Benutzer zur Eingabe der Anmeldeinformationen auf der Basis der Konfiguration und des Sitetyps auffordert:

Verbindungsmodus	Sitetyp	Kennwort zwischenspeichern	SSO für Citrix Gateway konfiguriert	Für Secure Web sind Anmeldeinformationen beim ersten Zugriff auf eine Website erforderlich	Für Secure Web sind Anmeldeinformationen bei weiteren Zugriffen auf die Website erforderlich	Für Secure Web sind Anmeldeinformationen nach Kennwortänderung erforderlich
Secure Browse	HTTP	Nein	Ja	Nein	Nein	Nein
Secure Browse	HTTPS	Nein	Ja	Nein	Nein	Nein
Vollständiges VPN	HTTP	Nein	Ja	Nein	Nein	Nein

Verbindungsmodus	Sitetyp	Kennwort zwischenspeichern	SSO für Citrix Gateway konfiguriert	Für Secure Web sind Anmeldeinformationen beim ersten Zugriff auf eine Website erforderlich	Für Secure Web sind Anmeldeinformationen bei weiteren Zugriffen auf die Website erforderlich	Für Secure Web sind Anmeldeinformationen nach Kennwortänderung erforderlich
Vollständiges VPN	HTTPS	Ja, wenn die Secure Web-MDX-Richtlinie “Webkennwort-caching aktivieren” auf “Ein” festgelegt ist.	Nein	Ja; Zum Zwischenspeichern der Anmeldeinformationen in Secure Web erforderlich	Nein	Ja

Vollständiger VPN-Tunnel mit PAC

> Wichtig:
>
> Wenn Secure Web mit einer PAC-Datei und Citrix ADC für den Proxybetrieb konfiguriert ist, tritt bei Secure Web ein Timeout auf. Entfernen Sie die für den Proxy konfigurierten Citrix Gateway-Datenverkehrsrichtlinien, bevor Sie einen vollständigen VPN-Tunnel mit PAC verwenden.

Bei der Konfiguration von Secure Web für einen vollständigen VPN-Tunnel mit der PAC-Datei oder dem Proxyserver sendet Secure Web den gesamten Datenverkehr zum Proxy über Citrix Gateway. Citrix Gateway leitet den Datenverkehr dann gemäß den Proxykonfigurationsregeln weiter. In dieser Konfiguration werden PAC-Datei bzw. Proxyserver von Citrix Gateway nicht beachtet. Der Datenfluss ist der gleiche wie beim vollständigen VPN-Tunnel ohne PAC-Datei.

Die folgende Abbildung zeigt den Datenfluss, wenn Secure Web-Benutzer zu einer Website navigieren:

In diesem Beispiel wird durch die Datenverkehrsregeln Folgendes festgelegt:

- Citrix Gateway stellt eine direkte Verbindung zur Intranetsite `example1.net` her.

- Der Datenverkehr zur Intranetsite `example2.net` wird per Proxy durch interne Proxyserver geleitet.
- Der externe Datenverkehr wird per Proxy durch interne Proxyserver geleitet. Proxyregeln blockieren externen Datenverkehr zu `Facebook.com`.

Konfigurieren eines vollständigen VPN-Tunnels mit PAC

1. Überprüfen und Testen der PAC-Datei.

   > Hinweis:
   >
   > Weitere Informationen zum Erstellen und Verwenden von PAC-Dateien finden Sie unter https://findproxyforurl.com/.

   Überprüfen Sie die PAC-Datei mit einem PAC-Validierungstool wie Pacparser. Stellen Sie beim Lesen der PAC-Datei sicher, dass die Pacparser-Ergebnisse Ihren Erwartungen entsprechen. Wenn die PAC-Datei einen Syntaxfehler enthält, wird sie von mobilen Geräten automatisch ignoriert. (PAC-Dateien werden auf mobilen Geräten nur im Arbeitsspeicher gespeichert.)

   PAC-Dateien werden von oben nach unten verarbeitet, die Verarbeitung endet, wenn eine Regel der aktuellen Abfrage entspricht.

   Testen Sie die URL der PAC-Datei mit einem Webbrowser, bevor Sie sie in das Feld **PAC/Proxy** von Endpoint Management eingeben. Stellen Sie sicher, dass der Computer auf den Speicherort der PAC-Datei im Netzwerk zugreifen kann.

   ```
   https://webserver.local/GenericPAC.pac
   https://webserver.local/GenericPAC.pac
   ```

   Getestete PAC-Dateierweiterungen sind .txt oder .pac.

   Der Inhalt der PAC-Datei muss im Webbrowser angezeigt werden.

   > Wichtig:
   >
   > Wenn Sie die mit Secure Web verwendete PAC-Datei aktualisieren, teilen Sie den Benutzern mit, dass sie Secure Web schließen und wieder öffnen müssen.

2. Konfigurieren von Citrix Gateway:

   - Deaktivieren Sie Split-Tunneling in Citrix Gateway. Falls Split-Tunneling aktiviert und eine PAC-Datei konfiguriert ist, haben die Regeln der PAC-Datei Vorrang vor den Citrix ADC-Split-Tunneling-Regeln. Ein Proxy hat keinen Vorrang vor den Citrix ADC-Split-Tunneling-Regeln.
   - Entfernen Sie die für den Proxy konfigurierten Citrix Gateway-Datenverkehrsrichtlinien. Dieser Schritt ist erforderlich, damit Secure Web einwandfrei funktioniert. In der folgenden Abbildung sehen Sie Beispiele für Regeln, die entfernt werden müssen.

3. Konfigurieren von Secure Web-Richtlinien:

    - Legen Sie die Richtlinie “Bevorzugter VPN-Modus” auf **Vollständiger VPN-Tunnel** fest.
    - Legen Sie die Richtlinie “VPN-Moduswechsel zulassen” auf **Aus** fest.
    - Konfigurieren Sie die URL für die PAC-Datei oder eine Proxyserverrichtlinie. Secure Web unterstützt HTTP und HTTPS sowie Standardports und andere Ports. Für HTTPS muss die Stammzertifizierungsstelle auf dem Gerät installiert sein, wenn das Zertifikat selbstsigniert oder nicht vertrauenswürdig ist.

      Testen Sie die URL oder Proxyserveradresse in einem Webbrowser, bevor Sie die Richtlinie konfigurieren.

      Beispiel für URLs in PAC-Datei:

      ```
      http[s]://example.com/proxy.pac
      http[s]://10.10.0.100/proxy.txt
      ```

      Beispiel für Proxyserver (Port ist erforderlich):

      ```
      myhost.example.com:port
      ```

      ```
      10.10.0.100:port
      ```

      > Hinweis:
      >
      > Wenn Sie eine PAC-Datei oder einen Proxyserver konfigurieren, konfigurieren Sie PAC nicht in den Systemproxyeinstellungen für Wi-Fi.

    - Legen Sie die Richtlinie “Webkennwortcaching aktivieren” auf **Ein** fest. Die Kennwortzwischenspeicherung handhabt Single Sign-On für HTTPS-Sites.

      Citrix ADC kann Single Sign-On für interne Proxys abwickeln, wenn der Proxy die gleiche Authentifizierungsinfrastruktur unterstützt.

Einschränkungen bei der Unterstützung für PAC-Dateien

Secure Web unterstützt Folgendes nicht:

- Failover von einem Proxyserver zu einem anderen. Bei der PAC-Dateiauswertung können mehrere Proxyserver für einen Hostnamen zurückgegeben werden. Secure Web verwendet nur den ersten zurückgegebenen Proxyserver.
- Protokolle wie FTP und gopher in einer PAC-Datei.
- SOCKS-Proxyserver in einer PAC-Datei.
- Web Proxy AutoDiscovery Protocol (WPAD).

Secure Web ignoriert die PAC-Dateifunktion “alert”, sodass es PAC-Dateien analysieren kann, die diese Aufrufe nicht enthalten.

Secure Web-Richtlinien

Wenn Sie Secure Web hinzufügen, berücksichtigen Sie die folgenden Secure Web-spezifischen MDX-Richtlinien. Für alle unterstützten Mobilgeräte:

Zugelassene oder blockierte Websites

Secure Web filtert Weblinks normalerweise nicht. Sie können mit dieser Richtlinie eine spezifische Liste zugelassener oder blockierter Sites konfigurieren. Dazu konfigurieren Sie URL-Muster in einer durch Trennzeichen getrennte Liste und beschränken so die Websites, die der Browser öffnen kann. Ein Pluszeichen (+) oder Minuszeichen (-) wird jedem Muster in der Liste vorangestellt. Der Browser vergleicht eine URL mit den Mustern in der aufgelisteten Reihenfolge, bis eine Übereinstimmung gefunden wird. Wenn eine Übereinstimmung gefunden wird, bestimmt das Präfix die Aktion wie folgt:

- Bei einem Minuszeichen (-) blockiert der Browser die URL. In diesem Fall wird die URL behandelt, als könne die Adresse des Webservers nicht aufgelöst werden.
- Bei einem Pluszeichen (+) wird die URL normal verarbeitet.
- Wenn weder ein + noch ein - dem Muster vorangestellt sind, wird ein + angenommen und der Zugriff zugelassen.
- Wenn die URL mit keinem Muster in der Liste übereinstimmt, wird sie zugelassen.

Wenn alle anderen URLs blockiert werden sollen, setzen Sie an den Schluss der Liste ein Minuszeichen gefolgt von einem Sternchen (-*). Beispiel:

- Durch den Richtlinienwert `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` werden HTTP-URLs innerhalb der Domäne `mycorp.com` zugelassen während alle anderen blockiert werden, alle HTTPS- und FTP-URLs sind zugelassen und alle anderen URLs werden blockiert.
- Der Richtlinienwert `+http://*.training.lab/*,+https://*.training.lab/*,-*` ermöglicht Benutzern, beliebige Websites in der Domäne Training.lab (Intranet) über HTTP oder HTTPS zu öffnen. Der Richtlinienwert lässt Benutzer öffentliche URLs wie Facebook, Google und Hotmail – unabhängig von dem Protokoll.

Der Standardwert ist leer (alle URLs zugelassen).

Popups blockieren

Popups sind neue Registerkarten, die von Websites ohne Ihre Genehmigung geöffnet werden. Mit dieser Richtlinie legen Sie fest, ob Secure Web Popups zulässt. Bei der Einstellung “Ein” verhindert Secure Web das Öffnen von Popups. Der Standardwert ist Aus.

Vorab geladene Lesezeichen

Definiert einen vorab geladenen Satz Lesezeichen für den Secure Web-Browser. Die Richtlinie ist eine durch Trennzeichen getrennte Liste mit Tupel, die einen Ordnernamen, einen Anzeigenamen und die Webadresse einschließt. Jedes Tripel muss das Format "Ordner, Name, URL" haben, wobei Ordner und Name von Anführungszeichen (") umschlossen sein können.

Die Richtlinienwerte `,"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` definieren drei Lesezeichen: Der erste Link ist ein primärer Link (kein Ordnername) mit dem Namen "Mycorp, Inc. home page". Der zweite Link wird in einem Ordner mit dem Namen "MyCorp Links" platziert und trägt die Bezeichnung "Account logon". Der dritte Link wird im Unterordner "Investor Relations" des Ordners "MyCorp Links" platziert und als "Contact us" angezeigt.

Der Standardwert ist leer.

Homepage-URL

Definiert die Website, die beim Starten von Secure Web geladen wird. Der Standardwert ist leer (Standardstartseite).

Nur für unterstützte Android- und iOS-Geräte:

Browserbenutzeroberfläche

Gibt das Verhalten und die Sichtbarkeit der Steuerelemente der Browserbenutzeroberfläche für Secure Web an. Normalerweise sind alle Browsersteuerelemente verfügbar. Dies schließt die Steuerelemente für Weiter, Zurück, Adressleiste sowie Aktualisieren und Stopp ein. Sie können mit dieser Richtlinie die Verwendung und Sichtbarkeit einiger dieser Steuerelemente einschränken. Der Standardwert ist Alle Steuerelemente sichtbar.

Optionen:

- **Alle Steuerelemente sichtbar.** Alle Steuerelemente sind sichtbar und die Verwendung durch Benutzer ist nicht eingeschränkt.
- **Schreibgeschützte Adressleiste.** Alle Steuerelemente sind sichtbar, aber Benutzer können das Adressfeld des Browsers nicht bearbeiten.
- **Adressleiste ausblenden.** Die Adressleiste wird ausgeblendet. Die anderen Steuerelemente werden angezeigt.
- **Alle Steuerelemente ausblenden.** Die gesamte Symbolleiste wird ausgeblendet und das Browserfenster ohne Rahmen angezeigt.

Webkennwortcaching aktivieren

Diese Richtlinie bestimmt, ob Secure Web Kennwörter auf Geräten zwischenspeichert, wenn Benutzer von Secure Web ihre Anmeldeinformationen zum Zugreifen auf oder Anfordern von Webressourcen eingeben. Diese Richtlinie gilt für Kennwörter, die in Authentifizierungsdialogfelder eingegeben werden, und nicht für Kennwörter, die in Webformulare eingegeben werden.

Wenn **Ein** festgelegt wird, speichert Secure Web alle Kennwörter zwischen, die Benutzer beim Anfordern einer Webressource eingeben. Wenn Aus festgelegt wird, speichert Secure Web Kennwörter nicht zwischen und entfernt bereits zwischengespeicherte Kennwörter. Der Standardwert ist **Aus**.

Diese Richtlinie ist nur aktiviert, wenn Sie für diese App auch die Richtlinie "Bevorzugter VPN-Modus" auf Vollständiger VPN-Tunnel festlegen.

Proxyserver

Sie können auch Proxyserver für Secure Web konfigurieren, wenn der Secure Browse-Modus aktiviert ist. Weitere Informationen finden Sie in diesem Blogbeitrag.

DNS-Suffixe

Wenn DNS-Suffixe auf Android nicht konfiguriert sind, schlägt das VPN möglicherweise fehl. Weitere Informationen zum Konfigurieren von DNS-Suffixen finden Sie unter Supporting DNS Queries by Using DNS Suffixes for Android Devices.

Vorbereiten von Intranetsites für Secure Web

Dieser Abschnitt richtet sich an Website-Entwickler, die eine Intranetsite für die Verwendung mit Secure Web für iOS und Android vorbereiten müssen. Bei für Desktop-Browser entwickelten Intranetsites sind Änderungen erforderlich, damit sie ordnungsgemäß auf Android- und iOS-Geräten funktionieren.

Secure Web stützt sich auf Android WebView und iOS WkWebView für die Unterstützung von Webtechnologie. Beispiele für von Secure Web unterstützte Internet-Technologien:

- AngularJS
- ASP.NET
- JavaScript
- jQuery
- WebGL
- WebSockets (nur im uneingeschränkten Modus)

Beispiele für von Secure Web nicht unterstützte Internet-Technologien:

- Flash
- Java

In der folgenden Tabelle werden die von Secure Web unterstützten HTML-Rendering-Features und -Technologien aufgelistet. Ein X bedeutet, dass das Feature für eine Plattform-/Browser-/Komponentenkombination verfügbar ist.

Technologie	iOS Secure Web	Android 5.x/6.x/7.x Secure Web
JavaScript-Engine	JavaScriptCore	V8
Lokaler Speicher	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X
WebGL		X
requestAnimationFrame API		X
Navigation Timing API		X
Resource Timing API		X

Die Technologien funktionieren geräteübergreifend gleich, doch Secure Web gibt verschiedene Benutzeragentzeichenfolgen für verschiedene Geräte zurück. Die für Secure Web verwendete Browserversion können Sie anhand der Zeichenfolge des Benutzeragents ermitteln. Navigieren Sie über Secure Web zu https://whatsmyuseragent.com/.

Problembehandlung bei Intranetsites

Zum Beheben von Rendering-Problemen bei der Anzeige der Intranetsite in Secure Web vergleichen Sie das Rendering der Website in Secure Web und einem kompatiblen Drittanbieter-Browser.

Für iOS sind Chrome und Dolphin kompatible Drittanbieter-Browser für Tests.

Für Android ist Dolphin der kompatible Drittanbieter-Browser für Tests.

> Hinweis:
>
> Chrome ist ein systemeigener Android-Browser. Verwenden Sie ihn nicht für den Vergleich.

Stellen Sie in iOS sicher, dass die Browser auf Geräteebene über VPN-Support verfügen. Diese Einstellung können Sie unter **Einstellungen > VPN > VPN-Konfiguration hinzufügen** auf dem Gerät konfigurieren.

Sie können auch VPN-Client-Apps wie Citrix VPN, Cisco AnyConnect oder Pulse Secure verwenden, die im App Store verfügbar sind.

- Ist das Rendering bei beiden Browsern gleich, liegt das Problem bei der Website. Aktualisieren Sie die Website und stellen Sie sicher, dass sie in dem Betriebssystem einwandfrei funktioniert.
- Wenn das Problem auf einer Webseite nur in Secure Web auftritt, wenden Sie sich an den Citrix Support zum Öffnen eines Supporttickets. Geben Sie die Problembehandlungsschritte und die getesteten Webbrowser und Betriebssysteme an. Wenn in Secure Web für iOS Wiedergabeprobleme auftreten, fügen Sie dieser Seite mit den folgenden Schritten ein Webarchiv hinzu. Auf diese Weise kann Citrix das Problem beheben.

Erstellen einer Webarchivdatei

In Safari unter macOS 10.9 oder höher können Sie eine Webseite als Webarchivdatei (Leseliste) speichern. Die Webarchivdatei enthält alle verknüpften Dateien wie Images, CSS und JavaScript.

1. Leeren Sie in Safari den Ordner der **Leseliste**: Klicken Sie im **Finder** in der **Menüleiste** auf **Gehe zu**, wählen Sie **Gehe zum Ordner**, geben Sie den Pfadnamen ~/Library/Safari/ReadingListArchives/ ein. Löschen Sie nun alle Ordner an diesem Speicherort.
2. Gehen Sie in der **Menüleiste** zu **Safari > Einstellungen > Erweitert** und aktivieren Sie in der Menüleiste **Menü “Entwickler” anzeigen**.
3. Klicken Sie in der **Menüleiste** auf **Entwickler > User Agent** und geben Sie den User Agent für Secure Web ein: (Mozilla/5.0 (iPad; CPU OS 8_3 wie macOS) AppleWebKit/600.1.4 (KHTML, wie Gecko) Mobile/12F69 Secure Web/ 10.1.0 (Build 1.4.0) Safari/8536.25).
4. Öffnen Sie in Safari die Website, die Sie als Leseliste (Webarchivdatei) speichern möchten.
5. Klicken Sie in der **Menüleiste** auf **Lesezeichen > Zur Leseliste hinzufügen**. Dieser Schritt kann einige Zeit dauern. Die Archivierung erfolgt im Hintergrund.
6. Navigieren Sie zur archivierten Leseliste: Klicken Sie in der **Menüleiste** auf **Darstellung > Seitenleiste für Leseliste einblenden**.
7. Überprüfen Sie die Archivdatei:
   - Deaktivieren Sie die Netzwerkverbindung zum Mac.
   - Öffnen Sie die Website über die Leseliste.

     Die Website wird komplett gerendert.

8. Komprimieren Sie die Archivdatei: Klicken Sie im **Finder** in der **Menüleiste** auf **Gehe zu**, wählen Sie **Gehe zum Ordner**, geben Sie den Pfadnamen ~/Library/Safari/ReadingListArchives/ ein. Komprimieren Sie dann den Ordner mit einer zufälligen Hex-Zeichenfolge als Dateiname. Diese Datei können Sie an den Citrix Support senden, wenn Sie ein Supportticket öffnen.

Secure Web-Features

Secure Web verwendet Technologien für den Austausch von mobilen Daten zum Erstellen eines dedizierten VPN-Tunnels, damit Benutzer in einer durch die Richtlinien Ihres Unternehmens gesicherten Umgebung auf interne und externe Websites zugreifen können. Die Websites umfassen Websites mit sensiblen Informationen in einer Umgebung, die durch die Richtlinien Ihrer Organisation geschützt ist.

Die Integration von Secure Web in Secure Mail und Citrix Files bietet eine nahtlose Benutzererfahrung innerhalb des sicheren Endpoint Management-Containers. Hier sehen Sie einige Beispiele der Integrationsfeatures:

- Wenn Benutzer auf einen **mailto**-Link tippen, wird eine neue E-Mail-Nachricht in Secure Mail geöffnet, ohne dass sie sich erneut authentifizieren müssen.
- **Zulassen, dass Links in Secure Web unter Wahrung der Datensicherheit geöffnet werden**. In Secure Web für iOS und Android können Benutzer über einen dedizierten VPN-Tunnel sicher auf Sites mit vertraulichen Informationen zugreifen. Sie können über Secure Mail, Secure Web oder eine Drittanbieter-App auf Links klicken. Die Links werden in Secure Web geöffnet und die Daten werden sicher eingebunden. Die Benutzer können einen internen Link öffnen, der das ctxmobilebrowser-Schema in Secure Web hat. Dabei transformiert Secure Web das Präfix `ctxmobilebrowser://` in `http://`. Für HTTPS-Links transformiert Secure Web `ctxmobilebrowsers://` in `https://`.

Das Feature wird von der MDX-App-Interaktionsrichtlinie **Eingehender Dokumentaustausch** gesteuert. Die Richtlinie ist standardmäßig auf **Uneingeschränkt** festgelegt. Mit dieser Einstellung können URLs in Secure Web geöffnet werden. Sie können die Richtlinieneinstellung so ändern, dass nur Apps in einer von Ihnen angelegten Positivliste mit Secure Web kommunizieren können.

- Wenn Benutzer auf einen Intranet-Link in einer E-Mail-Nachricht klicken, wechselt Secure Web ohne weitere Authentifizierung zu der Site.
- Benutzer können Dateien in Citrix Files hochladen, die sie mit Secure Web aus dem Internet heruntergeladen haben.

Secure Web-Benutzer können zudem die folgenden Aktionen ausführen:

- Popups blockieren

> Hinweis:
>
> Ein Großteil des Speichers von Secure Web wird für die Wiedergabe von Popups verwendet, sodass die Leistung oft durch das Blockieren von Popups in “Einstellungen” erhöht werden kann.

- Lesezeichen für bevorzugte Sites erstellen
- Dateien herunterladen
- Seiten offline speichern
- Kennwörter automatisch speichern
- Cache, Verlauf und Cookies löschen
- Blockieren von Cookies und lokalem HTML5-Speicher:
- Geräte sicher mit anderen Benutzern teilen
- Über die Adressleiste suchen
- Zulassen, dass mit Secure Web ausgeführte Web-Apps auf ihren Standort zugreifen
- Einstellungen exportieren und importieren
- Dateien direkt in Citrix Files öffnen, ohne sie herunterzuladen. Zum Aktivieren dieses Features fügen Sie der Richtlinie “Zulässige URLs” in Endpoint Management den Parameter **ctx-sf** hinzu.
- Verwenden Sie in iOS 3D-Touchaktionen zum Öffnen einer neuen Registerkarte und zum Zugriff auf Offlineseiten und Favoriten sowie für direkte Downloads vom Homebildschirm.
- In iOS: Herunterladen von Dateien jeder Größe und Öffnen in Citrix Files oder anderen Apps

  > Hinweis:
  >
  > Beim Verschieben von Secure Web in den Hintergrund wird der Download angehalten.

- Nach einem Begriff in der aktuellen Seitenansicht mit **Auf Seite suchen** suchen

Secure Web unterstützt auch dynamischen Text und zeigt daher die Schriftart an, die Benutzer auf ihrem Gerät festlegen.

Schutz von iOS-Daten

November 21, 2020

In Unternehmen, in denen die australischen Datenschutzanforderungen des Australian Signals Directorate (ASD) erfüllt werden müssen, können die neuen **Richtlinien zum Aktivieren des iOS-Datenschutzes** für Secure Mail und Secure Web verwendet werden. Die Standardeinstellung der Richtlinien ist **Aus**.

Wenn Sie **iOS-Datenschutz aktivieren** für Secure Web auf **Ein** festlegen, wird in Secure Web die Schutzklasse A für alle Dateien in der Sandbox verwendet. Weitere Informationen zum Datenschutz in Secure Mail finden Sie unter Datenschutz gemäß Australian Signals Directorate. Wenn Sie diese Richtlinie aktivieren, wird die höchste Datenschutzklasse verwendet, die Richtlinie **Mindestdatenschutzklasse** muss nicht zusätzlich festgelegt werden.

Zum Ändern der Richtlinie **iOS-Datenschutz aktivieren** gehen Sie folgendermaßen vor:

1. Laden Sie mit der Endpoint Management-Konsole die MDX-Dateien für Secure Web and Secure Mail in Endpoint Management: Bei neuen Apps navigieren Sie zu **Konfigurieren > Apps > Hinzufügen** und klicken Sie auf **MDX**. Informationen zu Upgrades finden Sie unter Durchführen eines Upgrades von MDX- oder Unternehmensapps.
2. Laden Sie mit der Endpoint Management-Konsole die MDX-Dateien in Endpoint Management: Bei neuen Apps navigieren Sie zu **Konfigurieren > Apps > Hinzufügen** und klicken Sie auf **MDX**. Informationen zu Upgrades finden Sie unter Hinzufügen von Apps.
3. Navigieren Sie für Secure Mail zu den **App**-Einstellungen und legen Sie die Richtlinie **iOS-Datenschutz aktivieren** auf **Ein** fest. Auf Geräte mit älteren Betriebssystemversionen hat die Aktivierung dieser Richtlinie keine Auswirkungen.
4. Navigieren Sie für Secure Web zu den **App**-Einstellungen und legen Sie die Richtlinie **iOS-Datenschutz aktivieren** auf **Ein** fest. Auf Geräte mit älteren Betriebssystemversionen hat die Aktivierung dieser Richtlinie keine Auswirkungen.
5. Konfigurieren Sie die App-Richtlinien wie gewohnt und speichern Sie die Einstellungen, um die App im Endpoint Management App Store bereitzustellen.

Secure Web-Features

April 20, 2020

Secure Web verwendet Technologien für den Austausch von mobilen Daten zum Erstellen eines dedizierten VPN-Tunnels, damit Benutzer in einer durch die Richtlinien Ihres Unternehmens gesicherten Umgebung auf interne und externe Websites zugreifen können. Die Websites umfassen Websites mit sensiblen Informationen in einer Umgebung, die durch die Richtlinien Ihrer Organisation geschützt ist.

Die Integration von Secure Web in Secure Mail und Citrix Files bietet eine nahtlose Benutzererfahrung innerhalb des sicheren Endpoint Management-Containers. Hier sehen Sie einige Beispiele der Integrationsfeatures:

- Wenn Benutzer auf einen mailto-Link tippen, wird eine neue E-Mail-Nachricht in Secure Mail geöffnet, ohne dass sie sich erneut authentifizieren müssen.

- **Zulassen, dass Links in Secure Web unter Wahrung der Datensicherheit geöffnet werden**. In Secure Web für iOS und Android können Benutzer über einen dedizierten VPN-Tunnel sicher auf Sites mit vertraulichen Informationen zugreifen. Sie können über Secure Mail, Secure Web oder eine Drittanbieter-App auf Links klicken. Die Links werden in Secure Web geöffnet und die Daten werden sicher eingebunden. Die Benutzer können einen internen Link öffnen, der das bzw. die ctxmobilebrowser-Schema(s) in Secure Web hat. Dabei transformiert Secure Web das Präfix `ctxmobilebrowser://` in `http://`. Für HTTPS-Links transformiert Secure Web `ctxmobilebrowsers://` in `https://`.

Das Feature wird von der MDX-App-Interaktionsrichtlinie **Eingehender Dokumentaustausch** gesteuert. Die Richtlinie ist standardmäßig auf **Uneingeschränkt** festgelegt. Mit dieser Einstellung können URLs in Secure Web geöffnet werden. Sie können die Richtlinieneinstellung so ändern, dass nur Apps in einer von Ihnen angelegten Positivliste mit Secure Web kommunizieren können.

- Wenn Benutzer auf einen Intranet-Link in einer E-Mail-Nachricht klicken, wechselt Secure Web ohne weitere Authentifizierung zu der Site.
- Benutzer können Dateien in Citrix Files hochladen, die sie mit Secure Web aus dem Internet heruntergeladen haben.

Secure Web-Benutzer können zudem die folgenden Aktionen ausführen:

- Popups blockieren

  > Hinweis:
  >
  > Ein Großteil des Speichers von Secure Web wird für die Wiedergabe von Popups verwendet, sodass die Leistung oft durch das Blockieren von Popups in “Einstellungen” erhöht werden kann.

- Lesezeichen für bevorzugte Sites erstellen
- Dateien herunterladen
- Seiten offline speichern
- Kennwörter automatisch speichern
- Cache, Verlauf und Cookies löschen
- Blockieren von Cookies und lokalem HTML5-Speicher:
- Geräte sicher mit anderen Benutzern teilen
- Über die Adressleiste suchen
- Zulassen, dass mit Secure Web ausgeführte Web-Apps auf ihren Standort zugreifen
- Einstellungen exportieren und importieren
- Dateien direkt in Citrix Files öffnen, ohne sie herunterzuladen. Zum Aktivieren dieses Features fügen Sie der Richtlinie “Zulässige URLs” in Endpoint Management den Parameter **ctx-sf** hinzu.

- Verwenden Sie in iOS 3D-Touchaktionen zum Öffnen einer neuen Registerkarte und zum Zugriff auf Offlineseiten und Favoriten sowie für direkte Downloads vom Homebildschirm.
- In iOS: Herunterladen von Dateien jeder Größe und Öffnen in Citrix Files oder anderen Apps

  > Hinweis:
  >
  > Beim Verschieben von Secure Web in den Hintergrund wird der Download angehalten.

- Nach einem Begriff in der aktuellen Seitenansicht mit **Auf Seite suchen** suchen

Secure Web unterstützt auch dynamischen Text und zeigt daher die Schriftart an, die Benutzer auf ihrem Gerät festlegen.

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