Secure Web

Contents

Neue Features in Secure Web

June 6, 2024

> **Hinweis:**
>
> Secure Hub, Secure Mail, Secure Web und die Citrix Workspace-App unterstützen Android 6.x und iOS 11.x ab Juni 2020 nicht.

Was ist neu in der aktuellen Version

Secure Web für iOS 24.3.0

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Was ist neu in früheren Releases

Secure Web für Android 24.3.0

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Secure Web für iOS 24.2.0

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Secure Web für Android 24.1.0

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Secure Web für Android 23.10.0

Unterstützung für den dunklen Modus Ab Version 23.10.0 unterstützt Secure Web den dunklen Modus auf Android-Geräten. Um den dunklen Modus einzustellen, gehen Sie in der App zu **Einstellungen** > **App-Design** und wählen Sie die Option **Dunkler Modus**.

Secure Web 23.9.0

Secure Web für iOS Secure Web für iOS 23.9.0 unterstützt iOS 17. Ein Upgrade von Secure Web auf Version 23.9.0 gewährleistet, dass Geräte, die auf iOS 17 aktualisiert werden, weiter unterstützt werden.

Secure Web 23.8.0

Secure Web für Android Secure Web für Android 23.8.0 unterstützt Android 14. Ein Upgrade von Secure Web auf Version 23.8.0 gewährleistet, dass Geräte, die auf Android 14 aktualisiert werden, weiter unterstützt werden.

Secure Web 23.7.0

Secure Web für Android In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Secure Web 23.5.0

Secure Web für Android In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Secure Web 23.3.5

Secure Web für Android In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Secure Web 23.2.0

Secure Web für Android und iOS In diesem Release wurden einige Probleme behoben, um die allgemeine Leistung und Stabilität zu verbessern.

Secure Web 22.9.0

Secure Web für Android Secure Web unterstützt jetzt Android 13.

Secure Web 22.9.1

Secure Web für iOS Dieses Release enthält Bugfixes.

Secure Web 22.9.0

Secure Web für iOS Secure Web unterstützt jetzt iOS 16.

Secure Web 22.6.0

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web 22.3.0

Secure Web für iOS **Google Analytics**: Citrix Secure Mail verwendet Google Analytics zum Sammeln von App-Statistiken und Analysedaten für Nutzungsinformationen, um die Produktqualität zu verbessern. Citrix sammelt oder speichert keine anderen persönlichen Benutzerinformationen. Weitere Informationen zum Deaktivieren von Google Analytics für Secure Mail finden Sie unter Deaktivieren von Google Analytics

Secure Web für Android **Google Analytics**: Citrix Secure Mail verwendet Google Analytics zum Sammeln von App-Statistiken und Analysedaten für Nutzungsinformationen, um die Produktqualität zu verbessern. Citrix sammelt oder speichert keine anderen persönlichen Benutzerinformationen. Weitere Informationen zum Deaktivieren von Google Analytics für Secure Mail finden Sie unter Deaktivieren von Google Analytics

Secure Web 22.2.0

Secure Web für iOS Dieses Release enthält Bugfixes.

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web 21.12.0

Secure Web für iOS **Unterstützung für FIDO2-basierte Authentifizierung.** Ab diesem Release unterstützt Citrix Secure Web die Authentifizierung bei Websites, die FIDO2 verwenden. Sie können sich bei Websites, die FIDO2 unterstützen, biometrisch, per Touch oder mit einem Passcode authentifizieren. Die WKWebView-Engine unterstützt die FIDO2-basierte Authentifizierung in Secure Web.

Secure Web für Android **Unterstützung für FIDO2-basierte Authentifizierung.** Ab diesem Release unterstützt Citrix Secure Web die Authentifizierung bei Websites, die FIDO2 verwenden. Sie können sich bei Websites, die FIDO2 unterstützen, biometrisch, per Touch oder mit einem Passcode authentifizieren.

Secure Web 21.11.0

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web 21.10.5

Secure Web für iOS Dieses Release enthält Bugfixes.

Secure Web für Android Dieses Release enthält Bugfixes.

> **Hinweis:**
>
> Die Unterstützung für Android 7 endete für Secure Web Oktober 2021.

Secure Web 21.10.0

Secure Web für Android

- **Unterstützung für Android 12**. Ab diesem Release wird Secure Web auf Geräten unterstützt, auf denen Android 12 ausgeführt wird.
- Secure Web erfüllt die aktuellen API-Anforderungen für API-Level 30 (Android 11) von Google Play.

Secure Web 21.9.1

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web 21.9.0

Secure Web für iOS Dieses Release enthält Bugfixes.

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web 21.8.5

Secure Web für Android Unterstützung von Android 12 Beta 4 auf bereits registrierten Geräten. Secure Web unterstützt jetzt Android 12 Beta 4. Wenn Sie ein Upgrade auf Android 12 Beta 4 planen, müssen Sie zunächst Secure Hub auf Version 21.7.1 aktualisieren. Secure Hub 21.7.1 ist die erforderliche Mindestversion für das Upgrade auf Android 12 Beta 4. Dieses Release gewährleistet ein nahtloses Upgrade von Android 11 auf Android 12 Beta 4 für bereits registrierte Benutzer.

> **Hinweis:**
>
> Citrix ist bestrebt, Android 12 vom 1. Tag an zu unterstützen. Nachfolgende Versionen von Secure Mail erhalten weitere Updates, um Android 12 vollständig zu unterstützen.

Secure Web 21.8.0

> **Hinweis:**
>
> Secure Web 21.8.0 wird nur unter iOS 12.1 und höher unterstützt. Es gibt keine Updates für Secure Web, das auf Geräten mit iOS Version 12 oder früher ausgeführt wird.

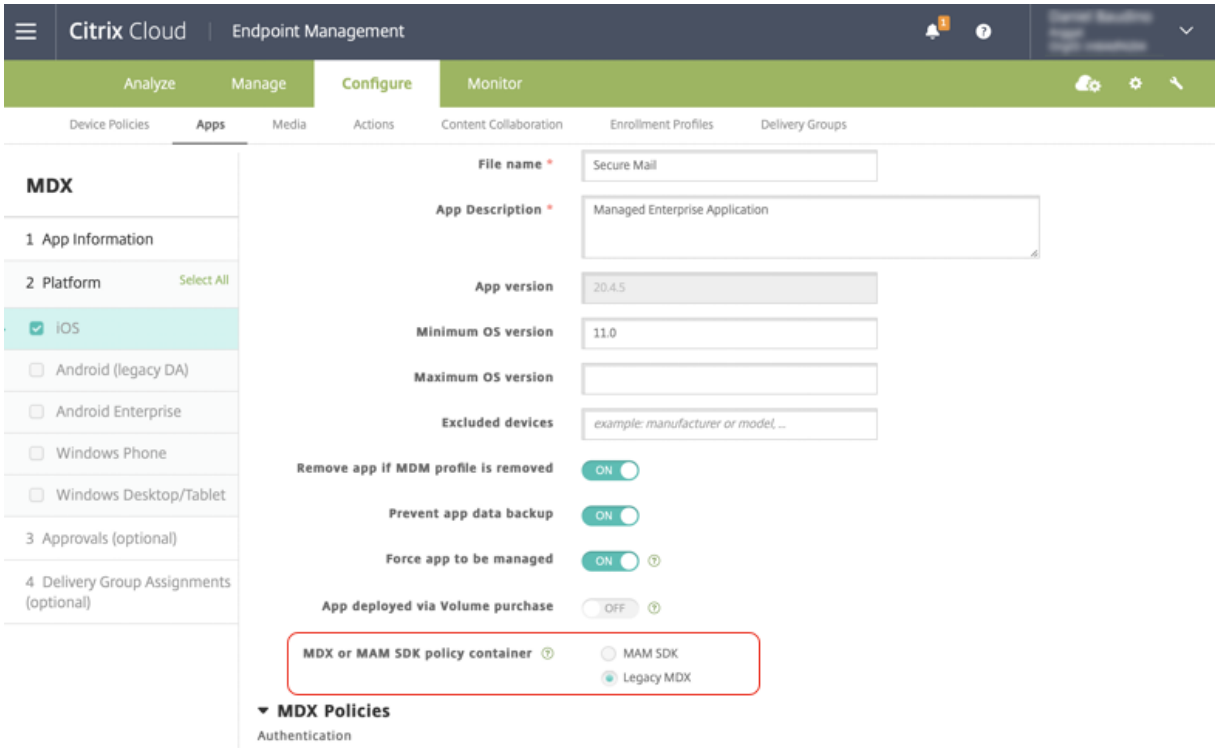
Secure Web für iOS

Dualmodus für Secure Web Das MAM-SDK zur Mobilanwendungsverwaltung ersetzt Bereiche der MDX-Funktionalität, die von der iOS-Plattform nicht bereitgestellt werden. Die MDX-Technologie erreicht das Ende des Lebenszyklus (EOL) im März 2022.

Citrix Secure Web wird mit dem MDX- und dem MAM-SDK-Framework veröffentlicht, um auf das für März 2022 geplante MDX-EOL vorzubereiten. Um die Verwaltung Ihrer Unternehmensanwendungen fortzusetzen, müssen Sie das MAM-SDK integrieren. Citrix empfiehlt den Wechsel zum **MAM-SDK**. Der Dualmodus soll den Übergang der Secure Web-App zum neuen MAM-SDK-Modell ermöglichen.

Mit der Dualmodus-Funktion können Sie Apps entweder wie bisher mit MDX (jetzt **Legacy-MDX**) verwalten oder zum neuen **MAM-SDK** wechseln. 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 von **Legacy-MDX** in **MAM-SDK** ändern.
Es wird empfohlen, nicht von **MAM-SDK** zu **Legacy-MDX** zu wechseln, da Sie beim Umstellen die App dann neu installieren müssen. 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.

Wenn Sie den Modus **MAM-SDK** auswählen, wechseln die Apps automatisch zum MAM SDK-Framework und die Geräterichtlinien werden ohne weitere Aktion der Administratoren aktualisiert.

> **Hinweis:**
>
> Wenn Sie von **Legacy-MDX** zu **MAM-SDK** wechseln, muss die Richtlinie **Netzwerkzugriff** entweder in **Tunnel - Web-SSO** oder **Uneingeschränkt** geändert werden.

Voraussetzungen

Stellen Sie sicher, dass folgende Anforderungen erfüllt sind, um das Dualmodus-Feature erfolgreich bereitzustellen:

- Aktualisieren Sie Citrix Endpoint Management auf die Version 10.12 RP2 oder höher bzw. 10.11 RP5 oder höher.
- Aktualisieren Sie Ihre mobilen Apps auf die Version 21.8.0 oder höher.

- Wenn Ihre Organisation Drittanbieter-Apps verwendet, müssen Sie zunächst das MAM-SDK in diese Drittanbieter-Apps integrieren, bevor Sie zum MAM-SDK-Framework wechseln. Alle verwalteten Apps müssen gleichzeitig in das MAM-SDK verschoben werden.

Einschränkungen

- Das MAM-SDK unterstützt nur die plattformbasierte Verschlüsselung und keine MDX-Verschlüsselung.
- Doppelte Richtlinieneinträge werden angezeigt, wenn Sie Citrix Endpoint Management nicht auf Version 10.12 RP2 oder höher oder 10.11 RP5 oder höher aktualisieren. Die doppelten Einträge werden erstellt, wenn die Richtliniendateien unter Version 21.8.0 oder höher ausgeführt werden.
- Wenn Sie zum MAM-SDK-Modus für die App-Verwaltung wechseln, werden einige Features nicht unterstützt oder sind nicht verfügbar. Die Interoperabilität von Apps in verschiedenen Modi wird für Aktionen wie "Öffnen in"sowie "Kopieren/Einfügen"nicht unterstützt. Beispielsweise können Sie Inhalte aus einer App, die im Modus **Legacy-MDX** verwaltet wird, nicht in eine App kopieren, die im Modus **MAM-SDK** verwaltet wird (und umgekehrt). In der folgenden Tabelle finden Sie die Features, die im Modus "MAM-SDK"nicht verfügbar sind:

Feature	Legacy-MDX	MAM SDK
Gemeinsam genutzte Geräte	Ja	Nein
Intune	Ja	Nein
SMIME gemeinsamer Zertifikattresor	Ja	Nein
Abgeleitete Anmeldeinformationen	Ja	Nein
UIWebView-Tunnel	Ja	Nein
Vollständiges VPN	Ja	Nein

- Die folgenden Richtlinien sind veraltet und im Modus "MAM-SDK"nicht verfügbar:
  - Zulässige Secure Web-Domänen
  - Zulässige Wi-Fi-Netzwerke
  - Alternatives Citrix Gateway
  - Zertifikatbezeichnung
  - Citrix-Berichterstellung
  - Explizite Abmeldebenachrichtigung

- Micro-VPN-Sitzung erforderlich
- Kulanzzeitraum für erforderliche Micro-VPN-Sitzung (Minuten)
- Maximum für Berichterstellungsdateicache
- Wi-Fi erforderlich
- Berichte nur über WLAN senden
- Uploadtoken

Hinweis:

> Wenn Sie ein Clientzertifikat für die Authentifizierung bei internen Servern verwenden, müssen Sie dieselbe Clientzertifizierung im Access Gateway verwenden.

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

- Überblick über das MAM-SDK
- Citrix Developer-Dokumentation zur Integration mobiler Anwendungen
- Citrix Blogbeitrag
- SDK-Download bei der Registrierung bei Citrix Downloads

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web 21.7.0

Secure Web für iOS Dieses Release enthält Bugfixes.

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web 21.6.0

Secure Web für iOS Ab diesem Release werden die folgenden Richtlinienoptionen für die Richtlinie **Netzwerkzugriff** nicht mehr unterstützt:

- **Vorherige Einstellungen verwenden**
- **Tunnel - Vollständiges VPN**
- **Tunnel - Vollständiges VPN und Web-SSO**

Wenn Sie die Richtlinien für **Tunnel - Vollständiges VPN** oder **Tunnel - Vollständiges VPN und Web-SSO** verwenden, müssen Sie zur Richtlinie **Tunnel - Web-SSO** wechseln.

> **Hinweis:**
>
> Um die Secure Ticket Authority (STA) zu verwenden, muss die Richtlinie **Netzwerkzugriff** auf **Tunnel - Web-SSO** festgelegt werden.

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web für iOS 21.5.0

Dieses Release enthält Bugfixes.

Secure Web für Android 21.4.5

Dieses Release enthält Bugfixes.

Secure Web 21.3.5

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web 21.3.0

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web 21.2.0

Secure Web für iOS **Überarbeitung der Farben für Secure Web.** Secure Web ist konform mit Citrix Branding-Farbaktualisierungen.

Secure Web für Android

- **Überarbeitung der Farben für Secure Web.** Secure Web ist konform mit Citrix Branding-Farbaktualisierungen.
- **Stabile Funktionsfähigkeit auf faltbaren Geräten.** Secure Web für Android enthält Fixes, um ein stabiles Funktionieren auf faltbaren Geräten zu gewährleisten.

Secure Web 21.1.5

Secure Web für iOS Dieses Release enthält Bugfixes.

Secure Web 21.1.0

Dieses Release enthält Bugfixes.

Secure Web 20.12.0

Secure Web für iOS Dieses Release enthält Bugfixes.

Secure Web 20.11.0

Dieses Release enthält Bugfixes.

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 Bugfixes.

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 für Android-Version von Secure Web. Das MAM-SDK zur Mobilanwendungsverwaltung ersetzt Bereiche der MDX-Funktionalität, die von den iOS- und Android-Plattformen nicht bereitgestellt werden. Die MDX-Technologie erreicht das Ende des Lebenszyklus (EOL) im September 2021. 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 finden Sie in den folgenden Artikeln:

- Überblick über das MAM-SDK
- Citrix Developer-Abschnitt zur Geräteverwaltung
- Citrix Blogbeitrag
- SDK-Download bei der Registrierung bei 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 zunächst das MAM-SDK in diese Drittanbieter-Apps integrieren, bevor Sie zum MAM-SDK-Framework wechseln. Alle verwalteten Apps müssen gleichzeitig in das MAM-SDK verschoben werden.

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

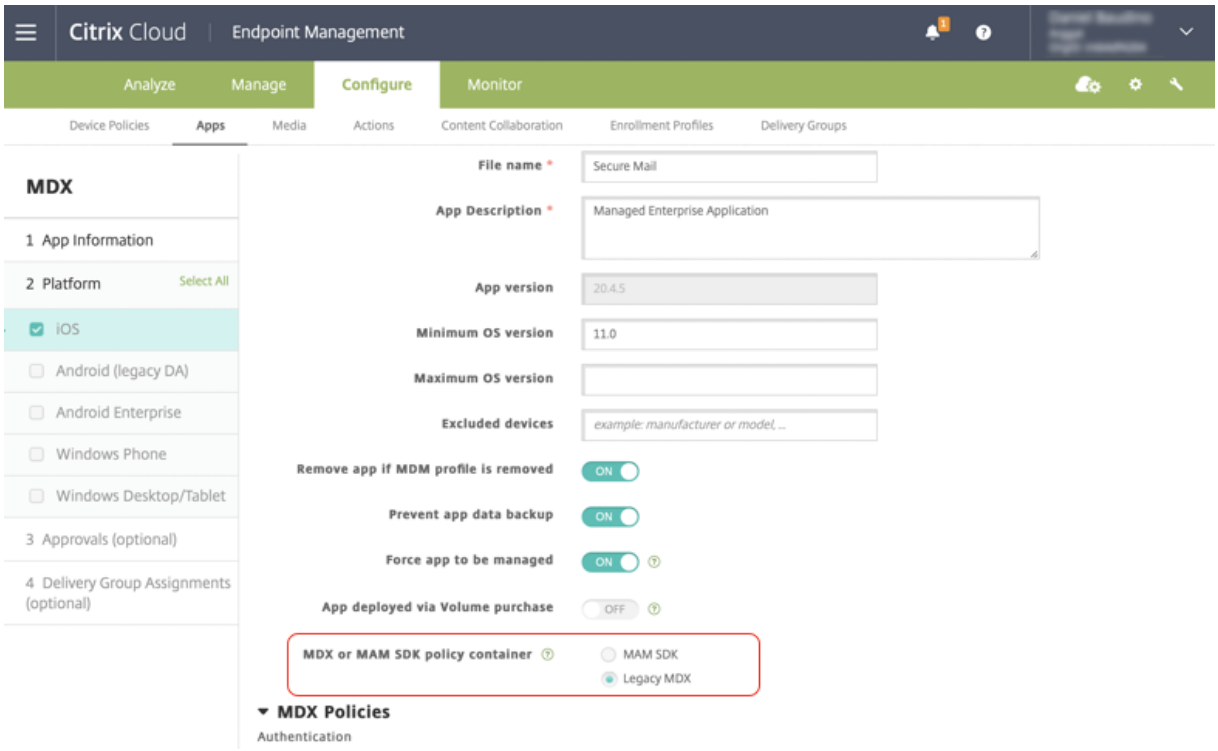
Einschränkungen

- Das MAM-SDK wird 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 Mail angezeigt.

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 Bugfixes.

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 Bugfixes.

Secure Web 20.5.0

Dieses Release enthält Bugfixes.

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 Fehlerbehebungen.

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. Die Verschlüsselungsverwaltung ist aktiviert. Alle vorhandenen verschlüsselten Anwendungsdaten auf Benutzergeräten gehen nahtlos in einen Zustand über, 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 eine Betriebssystemversion aus, die größer oder gleich der angegebenen Version ist.
- Debuggerzugriff: Für die App ist das Debugging nicht aktiviert.
- Gerät mit Jailbreak: Auf Geräten mit Jailbreak wird die App nicht ausgeführt.
- Gerätepasscode: Der 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: Auf Geräten mit Rooting wird die App nicht ausgeführt.
- Gerätesperre: Der Gerätepasscode ist aktiviert.
- Gerät verschlüsselt: Eine App wird auf einem verschlüsselten Gerät ausgeführt.

Secure Web 19.9.5

Dieses Release enthält Bugfixes.

Secure Web 19.9.0

Secure Web für iOS Secure Web für iOS unterstützt iOS 13.

Secure Web für Android Dieses Release enthält Bugfixes.

Secure Web für Android 19.8.5

Secure Web für Android unterstützt Android Q.

Secure Web 19.8.0

Dieses Release enthält Bugfixes.

Secure Web 19.7.5

Secure Web für iOS Dieses Release enthält Leistungsverbesserungen und Bugfixes.

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 Bugfixes.

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 Bugfixes.

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

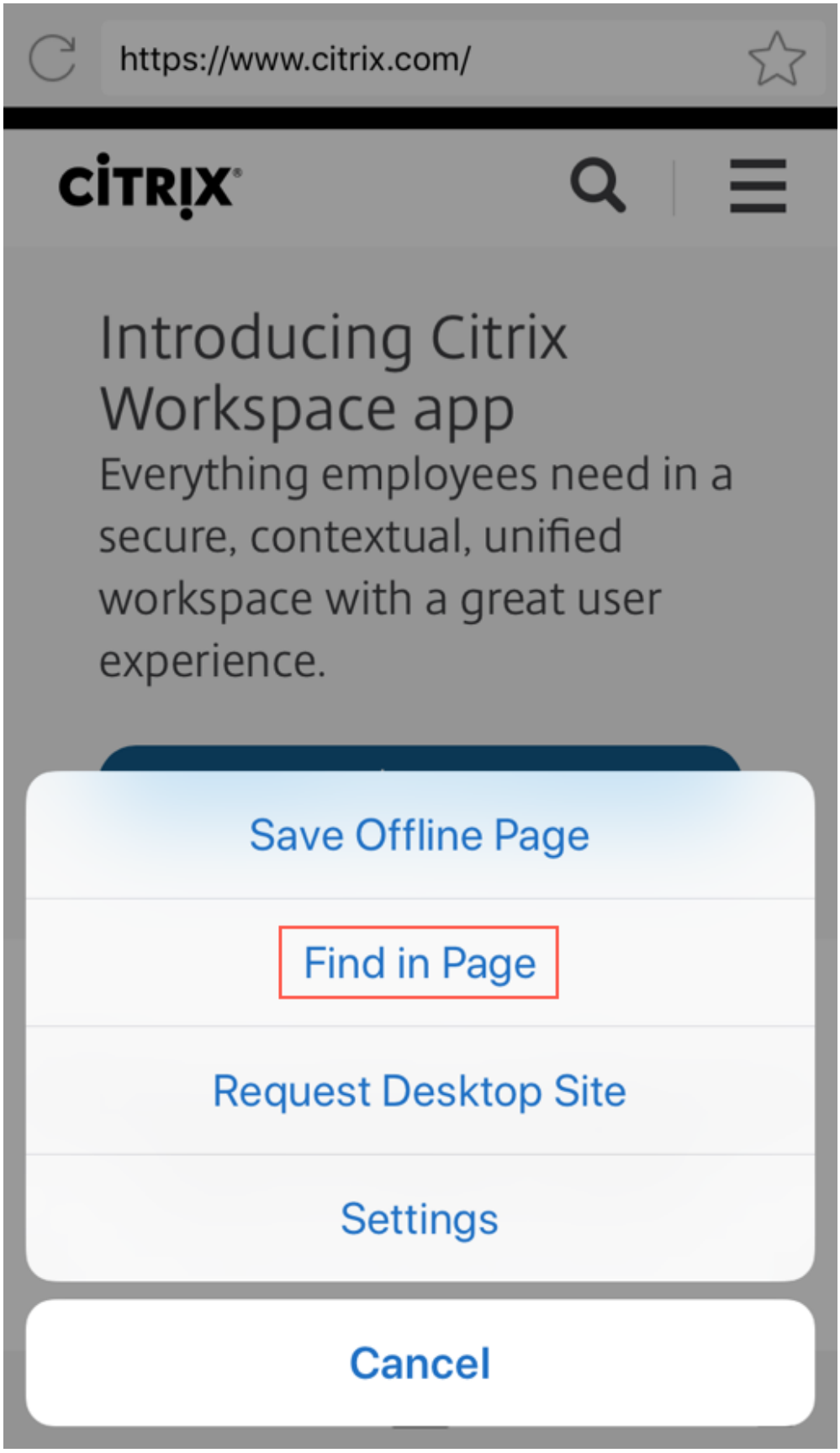
Diese Releases enthalten Leistungsverbesserungen und Bugfixes.

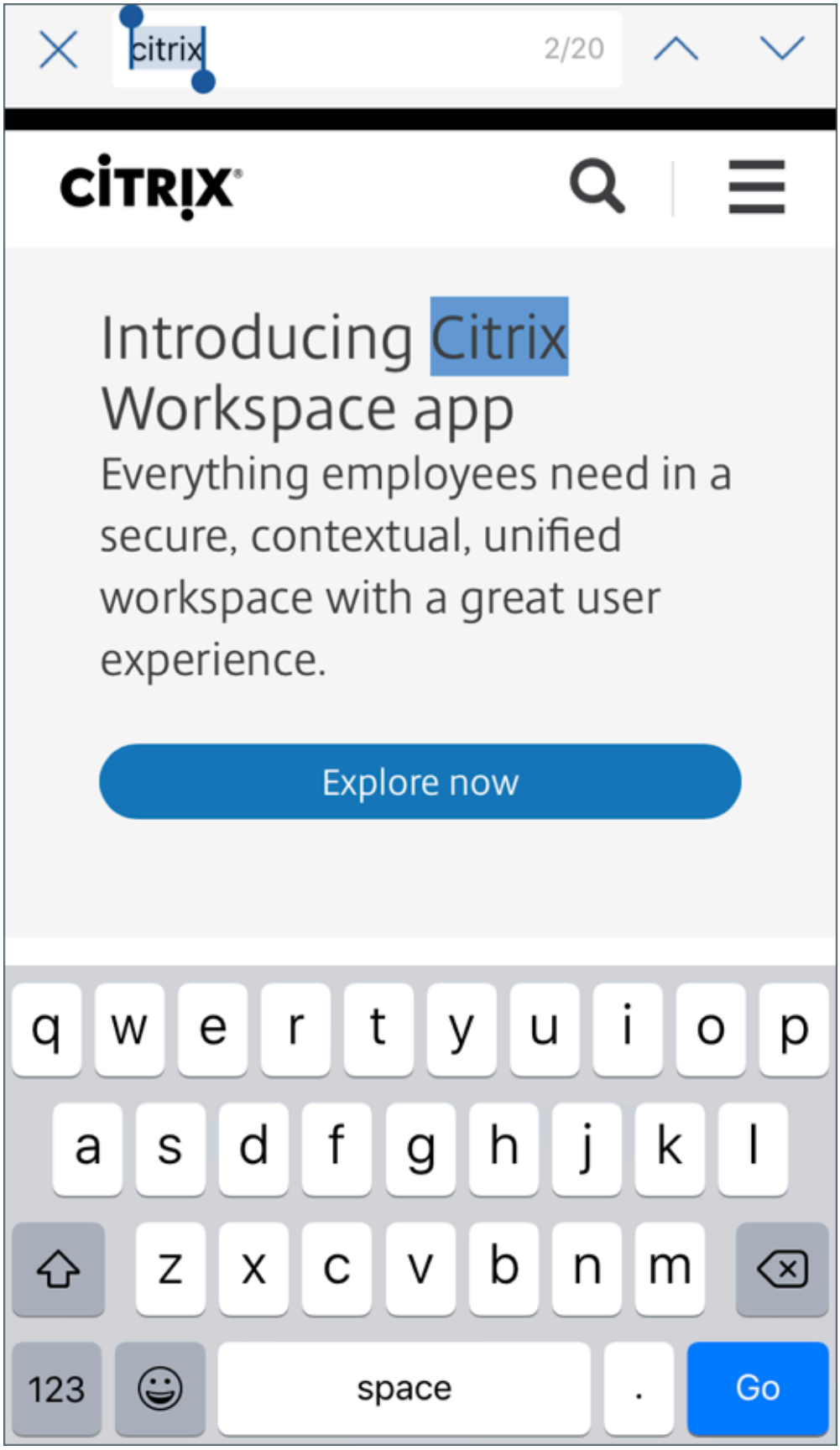
Secure Web 10.8.65

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 werden die Kopf- und Fußzeilenleisten ausgeblendet, während Sie nach oben scrollen, sodass beim Anzeigen von Webseiten mehr Informationen auf Ihrem mobilen Bildschirm angezeigt werden.

Secure Web 10.8.60

- Unterstützung für die polnische Sprache

Secure Web 10.8.35

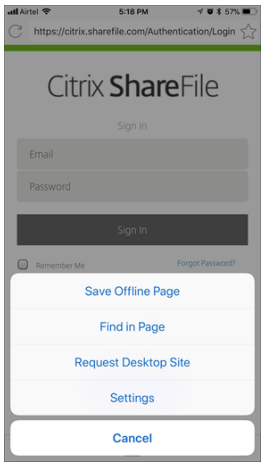
- **Zum Aktualisieren ziehen.** In Secure Web für Android können Benutzer mit der Funktion "Zum Aktualisieren ziehen"die Daten auf dem Bildschirm aktualisieren.

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. Weitere Informationen 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

June 6, 2024

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

Secure Web für iOS 24.3.0

Behobene Probleme

Secure Web reagiert nicht mehr, wenn Endbenutzer versuchen, die App auf iPad-Geräten zu öffnen. Dieses Problem ist spezifisch für Geräte, auf denen die iPad-Version 17.3.1 und höher ausgeführt wird. [XMHELP-4541]

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Web für Android 24.3.0

Behobene Probleme

Der Public Key Infrastructure (PKI)-Server erhält viele Anfragen von Secure Web zum Abrufen eines neuen Zertifikats, auch wenn das vorhandene Zertifikat noch nicht abgelaufen ist. Dieses Problem ist spezifisch für Android 14-Geräte. [XMHELP-4552]

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Web für iOS 24.2.0

Dieses Release enthält keine bekannten oder behobenen Probleme.

Secure Web für Android 24.1.0

Dieses Release enthält keine bekannten oder behobenen Probleme.

Secure Web für iOS 23.9.0

Dieses Release enthält keine bekannten oder behobenen Probleme.

Secure Web für Android 23.8.0

Dieses Release enthält keine bekannten oder behobenen Probleme.

Secure Web für Android 23.7.0

Dieses Release enthält keine bekannten oder behobenen Probleme.

Secure Web für Android 23.5.0

Dieses Release enthält keine bekannten oder behobenen 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

February 28, 2024

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:

- **Tunnel - Web-SSO:** Verbindungen, die einen Tunnel zum internen Netzwerk benötigen, können "Tunnel - Web-SSO"verwenden, eine Variante eines clientlosen VPNs. Diese Konfiguration ist der Standard für die Richtlinie **Bevorzugter VPN-Modus**. "Tunnel - Web-SSO"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.

> **Hinweis:**
>
> Die MDX-Technologie erreicht das Ende des Lebenszyklus (EOL) im September 2021. Um die Verwaltung Ihrer Unternehmensanwendungen fortzusetzen, müssen Sie das MAM-SDK integrieren. Der vollständige VPN-Tunnel wird im Legacy-MDX-Modus nicht unterstützt.

- Die Richtlinie **VPN-Moduswechsel zulassen** ermöglicht bei Bedarf den automatischen Wechsel zwischen den Modi "Vollständiger VPN-Tunnel"und "Tunnel - Web-SSO". 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 Modus "Tunnel –Web-SSO". HTTP-Authentifizierungsaufforderungen mit Single Sign-On werden hingegen eher bedient, wenn der Modus "Tunnel - Web-SSO"verwendet wird.

- **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
Tunnel – Web-SSO	HTTP	Nein	Ja	Nein	Nein	Nein
Tunnel – Web-SSO	HTTPS	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	HTTP	Nein	Ja	Nein	Nein	Nein
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

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 Modus “Tunnel - Web-SSO”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	Secure Web für iOS	Secure Web für Android
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. Sie können den Benutzeragenten in den Secure Web-Protokollen überprüfen. Um die Secure Web-Protokolle abzurufen, navigieren Sie zu **Secure Hub** > **Hilfe** > **Problem melden**. Wählen Sie Secure Web aus der Liste der Apps aus. Sie erhalten eine E-Mail, die die gezippten Protokolldateien im Anhang enthält.

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 Secure Access, 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.

Überprüfen der SSL-Verbindung

Stellen Sie sicher, dass die SSL-Zertifikatkette ordnungsgemäß konfiguriert ist. Mit dem SSL Certificate Checker können Sie nach fehlenden Stamm- oder Zwischenzertifizierungsstellen suchen, die nicht auf Mobilgeräten verknüpft oder installiert sind.

Viele Serverzertifikate werden von mehreren hierarchisch strukturierten Zertifizierungsstellen (ZS) signiert und bilden daher eine Kette. Diese Zertifikate müssen Sie verknüpfen. Informationen zum Installieren oder Verknüpfen Ihrer Zertifikate finden Sie unter Installieren, Verknüpfen und Aktualisieren von Zertifikaten.

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:

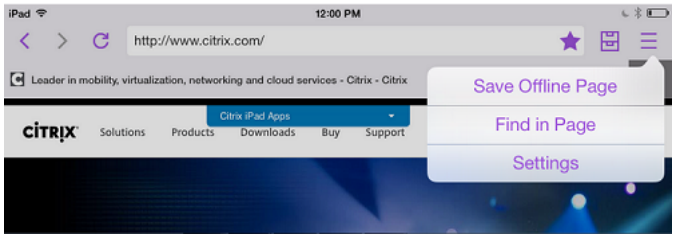
- Popups blockieren

  > 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.

> **Hinweis:**
>
> - Citrix Files für XenMobile erreichte am 1. Juli 2023 das Ende des Lebenszyklus (EOL). Weitere Informationen finden Sie unter Ende des Lebenszyklus und veraltete Apps

Schutz von iOS-Daten

December 7, 2021

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**. Bei Upgrades gehen Sie wie unter Durchführen eines Upgrades von MDX- oder Unternehmensapps beschrieben vor.
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**. Upgrade-Informationen finden Sie unter Apps hinzufügen.

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:

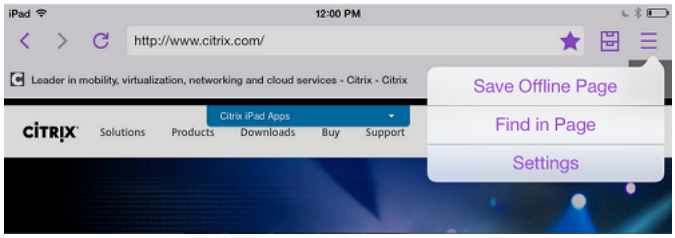
- Popups blockieren

  > 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.