Mobile Produktivitätsapps

Contents

Mobile Produktivitätsapps - Zeitachse für Releases

December 7, 2021

Die mobilen Produktivitätsapps von Citrix werden alle zwei Wochen veröffentlicht. Die genauen Daten können sich zwar ändern, Sie können jedoch anhand dieses Zweiwochentakts planen. Außerdem möchten wir Ihnen die Verwaltung von App-Bereitstellungen und -Updates erleichtern.

Info zum schrittweisen Releaseprozess von Secure Mail und Secure Web

Wenn neue Versionen von Secure Mail und Secure Web verfügbar sind, werden die Releases in Phasen veröffentlicht:

- Secure Mail- und Secure Web-Updates sind für einen zunehmenden Prozentsatz von iOS- und Android-Benutzern innerhalb einer Woche (sieben Tage) im App Store und im Google Play Store verfügbar.
- Bei neuen Downloads von Secure Mail und Secure Web für iOS ist die neue Version innerhalb dieser Woche verfügbar. Bei neuen Downloads von Secure Mail und Secure Web für Android wird die vorherige Version eine Woche lang ausgeführt, bis das neue Release 100 Prozent der Benutzer erreicht hat.
- Einige Features werden schrittweise für Benutzer eingeführt.

Voraussetzungen für die Verwaltung von Featureflags

Wenn in einer Produktionsumgebung ein Problem mit Secure Hub oder Secure Mail auftritt, kann das betroffene Feature im App-Code deaktiviert werden. Hierfür verwenden wir Featureflags und den Drittanbieterdienst “LaunchDarkly”. Sie müssen das Aktivieren des Datenverkehrs über LaunchDarkly nur dann konfigurieren, wenn Sie den ausgehenden Datenverkehr durch eine Firewall oder einen Proxyserver blockieren. In diesem Fall aktivieren Sie den Datenverkehr über LaunchDarkly Ihren Richtlinienanforderungen entsprechend über bestimmte URLs oder IP-Adressen. Weitere Informationen zum Ausschluss von Domänen vom Tunneling, der in MDX ab mobile Produktivitätsapps 10.6.15 unterstützt wird, finden Sie in der Dokumentation zum MDX Toolkit. Antworten auf häufig gestellte Fragen (FAQs) zu Featureflags und LaunchDarkly finden Sie in diesem Artikel im Support Knowledge Center.

> **Hinweis:**
> Vorankündigungen zu Features von Citrix Endpoint Management, die schrittweise ausgemustert werden, finden Sie unter Einstellung von Features und Plattformen.

Unterstützung für mobile Produktivitätsapps

February 28, 2024

Benutzer, die automatische Updates aktiviert haben, erhalten die aktuelle Version aus dem App-Store. Die aktuelle Version der mobilen Produktivitätsapps ist wie folgt:

- 23.10.0 (Secure Web für Android)
- 23.9.0 (Secure Mail und Secure Web für iOS)
- 23.8.2 (Secure Mail für Android)

Citrix unterstützt Upgrades von den letzten zwei Versionen der mobilen Produktivitätsapps. Die letzten zwei Versionen der mobilen Produktivitätsapps sind Folgende:

- 23.8.1 (Secure Mail für Android)
- 23.8.0 (Secure Web für Android)
- 23.7.0 (Secure Mail für Android und Secure Mail für iOS)
- 23.5.0 (Secure Mail für iOS und Secure Web für Android)
- 23.2.0 (Secure Web für iOS)
- 22.9.1 (Secure Web für iOS)

> **Wichtig:**
>
> Die MDX-Verschlüsselung hat am 1. September 2020 das Ende des Lebenszyklus (EOL) erreicht. Für Geräte, die in der Legacygeräteverwaltung (DA) registriert sind:
>
> - Wenn Sie keine MDX-Verschlüsselung verwenden, ist keine Aktion erforderlich.
> - Wenn Sie die MDX-Verschlüsselung verwenden, migrieren Sie Android-Geräte zu Android Enterprise. Geräte mit Android 10 müssen sich mit Android Enterprise registrieren bzw. erneut registrieren. Diese betrifft auch Android-Geräte im Nur-MAM-Modus. Siehe Migration von der Geräteverwaltung zu Android Enterprise.

Unterstützte Betriebssysteme

Mobile Produktivitäts-Apps unterstützen die folgenden Betriebssysteme:

Produktname	Betriebssystem	Mindestversion für Bereitstellung	Aktuelle Version
Secure Hub	Android	7.x	14.x
	iOS	12.x	17.x

Produktname	Betriebssystem	Mindestversion für Bereitstellung	Aktuelle Version
Secure Mail	Android	8.x	14.x
	iOS	13.x	17.x
Secure Web	Android	8.x	14.x
	iOS	13.x	17.x

Die aktuellen Versionen der mobilen Produktivitätsapps sind mit der aktuellen Version sowie den zwei vorherigen Versionen von Citrix Endpoint Management kompatibel. Weitere Informationen zu Betriebssystemen mit Unterstützung für Citrix Endpoint Management finden Sie unter Unterstützte Gerätebetriebssysteme.

Für die aktuelle Version der mobilen Produktivitätsapps ist die aktuelle Version von Secure Hub erforderlich. Halten Sie Secure Hub auf dem neuesten Stand.

> **Hinweis:**
>
> Zu jedem Zeitpunkt unterstützt Citrix nur die neuesten und die beiden vorherigen Versionen (N, N-1 und N-2) der Android- und iOS-Betriebssysteme.

Weitere Überlegungen und Einschränkungen

Vorankündigungen zu Features von Citrix Endpoint Management, die schrittweise ausgemustert werden, finden Sie unter Einstellung von Features und Plattformen.

Secure Mail

- Endpoint Management bietet derzeit keine Unterstützung für NetScaler 12.0.41.16 aufgrund eines Problems mit Secure Ticket Authority (STA) und Secure Mail. Das Problem wurde in NetScaler 12.0 Build 41.22 behoben.
- Die Unterstützung für Secure Mail für Exchange 2007 und Lotus Notes 8.5.3 wurde am 30. September 2017 eingestellt (EOL).
- Für die optimale Leistung beim Senden von Citrix Files-Anlagen empfiehlt sich die Verwendung der aktuellen Version von Citrix Files. Citrix Files wird für Windows nicht unterstützt.
- In Umgebungen mit IBM Notes müssen Sie den IBM Domino Traveler-Server, Version 9.0, konfigurieren. Weitere Informationen finden Sie unter Integration von Exchange Server oder IBM Notes Traveler-Server.

> **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

Secure Web

Installieren Sie die neueste Version von Android WebView auf den Geräten. Die Benutzer können Android WebView aus dem Google Play Store herunterladen.

QuickEdit

QuickEdit bleibt als mobile Produktivitätsapp verfügbar. Das zuvor angekündigte Ende des Lebenszyklus (EOL) am 1. September 2018 findet nicht statt.

Citrix Content Collaboration für Endpoint Management

Benutzer greifen über den öffentlichen App-Store auf Citrix Content Collaboration für Endpoint Management ab Version 6.5 zu.

ShareConnect

ShareConnect hat das Ende des Lebenszyklus (EOL) am 30. Juni 2020 erreicht. Weitere Informationen finden Sie unter Ende des Lebenszyklus und veraltete Apps.

Citrix Secure Notes und Citrix Secure Tasks

Citrix Secure Notes und Citrix Secure Tasks haben das Ende des Lebenszyklus (EOL) am 31. Dezember 2018 erreicht. Weitere Informationen finden Sie unter Ende des Lebenszyklus und veraltete Apps.

Administratoraufgaben und -überlegungen

October 31, 2022

In diesem Artikel werden die Aufgaben und Überlegungen erläutert, die für Administratoren von mobilen Produktivitätsapps relevant sind.

Featureflags verwalten

Wenn in einer Produktionsumgebung ein Problem mit einer mobilen Produktivitätsapp auftritt, kann das betroffene Feature im App-Code deaktiviert werden. Wir können das Feature für Secure Hub, Secure Mail und Secure Web für iOS und Android deaktivieren. Hierfür verwenden wir Featureflags und den Drittanbieterdienst "LaunchDarkly". Sie müssen das Aktivieren des Datenverkehrs über LaunchDarkly nur dann konfigurieren, wenn Sie den ausgehenden Datenverkehr durch eine Firewall oder einen Proxyserver blockieren. In diesem Fall aktivieren Sie den Datenverkehr über LaunchDarkly Ihren Richtlinienanforderungen entsprechend über bestimmte URLs oder IP-Adressen. Weitere Informationen zur Unterstützung in MDX für den Domänenausschluss vom Tunneling finden Sie in der Dokumentation zum MDX Toolkit.

Sie können den Datenaustausch und die Kommunikation mit LaunchDarkly wie folgt ermöglichen:

Datenverkehr für folgende URLs zulassen

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `firehose.launchdarkly.com`

Erstellen einer Positivliste nach Domäne

Bisher bot Citrix eine Liste mit IP-Adressen an, die verwendet werden konnten, wenn interne Richtlinien eine ausschließliche Auflistung von IP-Adressen erforderten. Nachdem Citrix Infrastrukturverbesserungen vorgenommen hat, werden die öffentlichen IP-Adressen ab 16. Juli 2018 schrittweise abgebaut. Citrix empfiehlt Verwendung einer Positivliste nach Domäne.

IP-Adressen in einer Positivliste auflisten

Wenn Sie IP-Adressen in einer Positivliste auflisten müssen, konsultieren Sie die Liste der aktuellen IP-Adressbereiche unter Liste öffentlicher IP-Adressen von LaunchDarkly. Mithilfe dieser Liste können Sie sicherstellen, dass Ihre Firewallkonfigurationen automatisch anhand der Infrastrukturupdates aktualisiert werden. Einzelheiten zum Status der Änderungen der Infrastruktur finden Sie auf der Statusseite von LaunchDarkly.

> Hinweis:
>
> Öffentliche Store-Apps müssen zur ersten Bereitstellung neu installiert werden. Ein Upgrade einer umschlossenen Unternehmensapp auf eine öffentliche Store-App ist nicht möglich.

> Bei der Bereitstellung in öffentlichen App-Stores brauchen Sie von Citrix entwickelte Apps nicht zu signieren und mit dem MDX Toolkit zu umschließen. Sie können Unternehmensapps und Apps von Drittanbietern mit dem MDX Toolkit umschließen.

LaunchDarkly-Systemanforderungen

- Endpoint Management 10.7 oder höher.
- Stellen Sie sicher, dass die Apps mit den folgenden Diensten kommunizieren können, wenn Sie Split-Tunneling in Citrix ADC auf **OFF** festgelegt haben:
  - LaunchDarkly-Dienst.
  - APNs-Listenerdienst

Unterstützte App-Stores

Die mobilen Produktivitätsapps sind im Apple App Store und in Google Play verfügbar.

In China ist Google Play nicht verfügbar, Secure Hub für Android ist jedoch in den folgenden App-Stores verfügbar:

- https://shouji.baidu.com
- https://apk.hiapk.com
- https://apk.91.com

Aktivieren der Verteilung über öffentliche App-Stores

1. Laden Sie die Datei public-store.mdx je für iOS und Android von der Endpoint Management-Downloadseite herunter.
2. Laden Sie die MDX-Dateien auf die Endpoint Management-Konsole hoch. Die Versionen der mobilen Produktivitätsapps für öffentliche Stores werden weiterhin als MDX-Apps hochgeladen. Laden Sie die Apps nicht als öffentliche Store-Apps auf den Server hoch. Weitere Informationen zu dem Verfahren finden Sie unter Hinzufügen von Apps.
3. Ändern Sie die Standardwerte von Richtlinien gemäß Ihren Sicherheitsvorgaben (optional).
4. Stellen Sie die Apps per Push als erforderlich bereit (optional). Für diesen Schritt muss Ihre Umgebung für die Mobilgeräteverwaltung aktiviert sein.
5. Installieren Sie Apps auf Geräten aus dem App-Store, Google Play oder dem Endpoint Management App Store.
   - Benutzer von Android-Geräten werden zum Installieren der App an den Play Store weitergeleitet. Auf iOS-Geräten wird die App in Bereitstellungen mit MDM installiert. ohne dass Benutzer zum App Store wechseln.

- Wenn die App aus dem App Store oder Play Store installiert wird, wird folgende Aktion ausgeführt. Die App wird zur verwalteten App, sofern die zugehörige MDX-Datei auf den Server hochgeladen wurde. Beim Wechsel zur verwalteten App wird die Eingabe einer Citrix-PIN angefordert. Wenn Benutzer die Citrix-PIN eingeben, wird von Secure Mail der Bildschirm zur Kontokonfiguration angezeigt.

6. Apps sind nur zugänglich, wenn der Benutzer bei Secure Hub registriert und die entsprechende MDX-Datei auf dem Server ist. Ist eine dieser beiden Bedingungen nicht erfüllt, kann der Benutzer die App zwar installieren, jedoch im Anschluss nicht nutzen.

Wenn Sie bereits Apps aus dem Citrix Ready Marketplace in öffentlichen App-Stores verwenden, kennen Sie das Bereitstellungsverfahren schon. Die mobilen Produktivitätsapps verwenden den gleichen Ansatz, den derzeit viele unabhängige Softwarehersteller verwenden. Betten Sie das MDX SDK in die App ein, um die App für den öffentlichen Store vorzubereiten.

> Hinweis:
>
> Die Versionen der Citrix Files-Apps für iOS und Android, die in öffentlichen Stores verfügbar sind, sind jetzt universell. Die Citrix Files-App ist dieselbe für Mobiltelefone und Tablets.

Apple-Pushbenachrichtigungen

Weitere Informationen zum Konfigurieren von Pushbenachrichtigungen finden Sie unter Konfigurieren von Secure Mail für Pushbenachrichtigungen.

Häufig gestellte Fragen (FAQs) zum öffentlichen App-Store

- Kann ich mehrere Exemplare öffentlicher Apps für verschiedene Benutzergruppen bereitstellen? Beispiel: Ich möchte unterschiedliche Richtlinien für verschiedene Benutzergruppen bereitstellen.

  Laden Sie für jede Benutzergruppe eine eigene MDX-Datei hoch. Allerdings darf in diesem Fall ein einzelner Benutzer nicht mehreren Gruppen angehören. Gehörte ein einzelner Benutzer mehreren Gruppen an, würden ihm mehrere Exemplare derselben App zugewiesen. Es können nicht mehrere Exemplare einer öffentlichen Store-App auf demselben Gerät bereitgestellt werden, da die App-ID nicht geändert werden kann.

- Kann ich öffentliche Store-Apps per Push als erforderliche Apps installieren?

  Ja. Die Pushinstallation erfordert MDM, im Nur-MAM-Modus wird sie nicht unterstützt.

- Muss ich Datenverkehrsrichtlinien oder Exchange Server-Regeln, die auf dem Benutzeragent basieren, aktualisieren?

  Zeichenfolgen für alle benutzeragentbasierten Richtlinien und Regeln nach Plattform:

> Wichtig:
>
> Secure Notes und Secure Tasks haben das Ende des Lebenszyklus (End Of Life, EOL) am 31. Dezember 2018 erreicht. Weitere Informationen finden Sie unter Ende des Lebenszyklus und veraltete Apps.

Android

App	Server	User-Agent-Zeichenfolge
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		WorxMail
Citrix Secure Tasks	Exchange	WorxMail
Citrix Secure Notes	Exchange	WorxMail
	Citrix Files	Secure Notes

iOS

App	Server	User-Agent-Zeichenfolge
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		com.citrix.browser
Citrix Secure Tasks	Exchange	WorxTasks
Citrix Secure Notes	Exchange	WorxNotes
	Citrix Files	Secure Notes

- Kann ich App-Updates verhindern?

  Nein. Wenn ein Update im öffentlichen App-Store bereitgestellt wird, erhalten alle Benutzer, die automatische Updates aktiviert haben, das Update.

- Kann ich App-Updates erzwingen?

  Ja, Updates werden über die Update-Kulanzzeitraumrichtlinie erzwungen. Diese Richtlinie wird festgelegt, wenn die neue MDX-Datei für die aktualisierte App-Version in Endpoint Management hochgeladen wird.

- Wie kann ich Apps testen, bevor die Benutzer sie erhalten, wenn ich keine Kontrolle über die Update-Zeitachse habe?

  Ähnlich wie bei Secure Hub stehen Apps während des EAR-Zeitraums (Early Adopter Release) zum Testen auf TestFlight für iOS zur Verfügung. Android-Apps stehen während des EAR-Zeitraums über das Google Play-Betaprogramm zur Verfügung. In diesem Zeitraum können Sie App-Updates testen.

- Was passiert, wenn ich die neue MDX-Datei nicht aktualisiere, bevor ein automatisches Update auf die Benutzergeräte gelangt?

  Die aktualisierte App ist weiterhin mit der älteren MDX-Datei kompatibel. Neue Features, die von einer neuen Richtlinie abhängen, werden nicht aktiviert.

- Wird die App zur verwalteten App, wenn Secure Hub installiert wird, oder muss sie neu registriert werden?

  Benutzer müssen bei Secure Hub registriert sein, damit eine öffentliche Store-App als verwaltete (mit MDX geschützte) App aktiviert wird und verwendet werden kann. Wenn Secure Hub installiert ist aber keine Registrierung vorliegt, können die Benutzer die öffentliche Store-App nicht verwenden.

- Benötige ich ein Apple Enterprise Developer-Konto für öffentliche Store-Apps?

  Nein. Da jetzt Citrix die Zertifikate und Provisioningprofile für die mobilen Produktivitätsapps pflegt, ist zur Bereitstellung der Apps kein Apple Enterprise Developer-Konto erforderlich.

- Gilt das Ende der Unternehmensverteilung für umschlossene Apps, die ich schon bereitgestellt habe?

  Nein, es gilt nur für die mobilen Produktivitätsapps Secure Mail, Secure Web und Citrix Content Collaboration für Endpoint Management, QuickEdit und ShareConnect. Alle umschlossenen Unternehmensapps (interne oder von Drittanbietern), die Sie bereitgestellt haben, können weiterhin umschlossen verwendet werden. Das MDX Toolkit unterstützt weiterhin das Umschließen von Unternehmensapps für App-Entwickler.

- Beim Installieren einer App aus Google Play wird ein Android-Fehler mit dem Fehlercode 505 angezeigt.

  > Hinweis:
  >
  > Die Unterstützung für Android 5.x endete am 31. Dezember 2018.

  Dies ist ein bekanntes Problem bei Google Play und Android 5.x-Versionen. Wenn dieser Fehler auftritt, können Sie veraltete Daten auf dem Gerät, die die Installation der App verhindern, wie folgt löschen:

1. Starten Sie das Gerät neu.

2. Leeren Sie den Cache und löschen Sie die Daten für Google Play über die Geräteeinstellungen.
3. Entfernen Sie als letzten Ausweg das Google-Konto vom Gerät und fügen Sie es wieder hinzu.

Weitere Informationen finden Sie auf dieser Site, wenn Sie nach folgenden Schlüsselwörtern suchen: "Fix Google Play Store Error 505 in Android: Unknown Error Code".

- Wenn eine App in Google Play zur Produktion freigegeben wurde und es keine neue Betaversion gibt, warum wird Beta neben dem App-Namen in Google Play angezeigt?

  Wenn Sie an unserem Early Access Release-Programm teilnehmen, wird neben dem App-Namen immer "Beta"angezeigt. Der Name weist die Benutzer auf ihre Zugriffsebene für eine bestimmte App hin. Der Zusatz "Beta"bedeutet, dass Benutzer die aktuelle Version der App erhalten. Die aktuelle Version kann eine Produktionsversion oder eine Betaversion sein.

- Nach der Installation und dem Öffnen der App wird "App nicht autorisiert"gemeldet, selbst wenn die MDX-Datei in der Endpoint Management-Konsole vorliegt.

  Dieser Fall kann eintreten, wenn der Benutzer die App direkt aus dem App-Store oder aus Google Play installiert und Secure Hub noch nicht aktualisiert hat. Secure Hub muss aktualisiert werden, wenn der Inaktivitätstimer abgelaufen ist. Richtlinien werden aktualisiert, wenn Benutzer Secure Hub öffnen und sich erneut authentifizieren. Die App wird autorisiert, wenn die Benutzer sie das nächste Mal öffnen.

- Benötige ich einen Zugangscode zum Verwenden von Apps? Ich werde zur Eingabe eines Zugangscodes beim Installieren einer App aus dem App Store oder Google Play aufgefordert.

  Wenn Sie eine Aufforderung zur Codeeingabe sehen, sind Sie nicht bei Endpoint Management über Secure Hub registriert. Registrieren Sie sich bei Secure Hub und vergewissern Sie sich, dass die MDX-Datei der App auf dem Server bereitgestellt wurde. Stellen Sie zudem sicher, dass die App verwendet werden kann. Der Zugangscode dient nur zur Citrix-internen Verwendung. Apps erfordern eine Endpoint Management-Bereitstellung zur Aktivierung.

- Kann ich iOS-Apps aus dem öffentlichen Store über VPP oder DEP bereitstellen?

  Endpoint Management ist für die Verteilung öffentlicher, nicht MDX-aktivierter Store-Apps per VPP optimiert. Sie können zwar öffentliche Endpoint Management Store Apps über VPP verteilen, doch ist die Bereitstellung so lange nicht optimal, bis Citrix weitere Verbesserungen an Endpoint Management und dem Secure Hub-Store zur Beseitigung von Einschränkungen vorgenommen hat. Eine Liste der bekannten Probleme bei der Bereitstellung öffentlicher Endpoint Management Store Apps über VPP sowie mögliche Workarounds finden Sie im Citrix Knowledge Center.

MDX-Richtlinien für mobile Produktivitätsapps

Mit den MDX-Richtlinien können Sie Einstellungen konfigurieren, die von Endpoint Management durchgesetzt werden. Die Richtlinien sind für Authentifizierung, Gerätesicherheit, Netzwerkanforderungen und -zugriff, Verschlüsselung, App-Interaktion, App-Einschränkungen usw. Viele MDX-Richtlinien gelten für alle mobilen Produktivitätsapps. Einige Richtlinien sind jedoch App-spezifisch.

Richtliniendateien werden als MDX-Dateien für die öffentlichen Storeversionen der mobilen Produktivitätsapps bereitgestellt. Sie können außerdem Richtlinien in der Endpoint Management-Konsole konfigurieren, wenn Sie eine App hinzufügen.

Ausführliche Beschreibungen der MDX-Richtlinien finden Sie in den folgenden Artikeln:

- Überblick über die MDX-Richtlinien für mobile Produktivitätsapps
- MDX-Richtlinien für mobile Produktivitätsapps für Android
- MDX-Richtlinien für mobile Produktivitätsapps für iOS

In den folgenden Abschnitten werden die mit den Benutzerverbindungen verbundenen MDX-Richtlinien erläutert.

Dualmodus in Secure Mail für Android

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 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 aktuellen MDX Toolkit auf neue MAM-SDKs erleichtern. Der Dualmodus bietet zwei Optionen:

- Sie verwalten Apps weiter mit dem MDX Toolkit (das jetzt Legacy-MDX in der Endpoint Management-Konsole genannt wird).
- Sie verwalten Apps, die das neue MAM-SDK enthalten.

> **Hinweis:**
>
> Wenn Sie das MAM-SDK verwenden, müssen Sie Apps nicht umschließen.

Nach dem Wechsel zum MAM-SDK sind keine weiteren Schritte erforderlich.

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 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

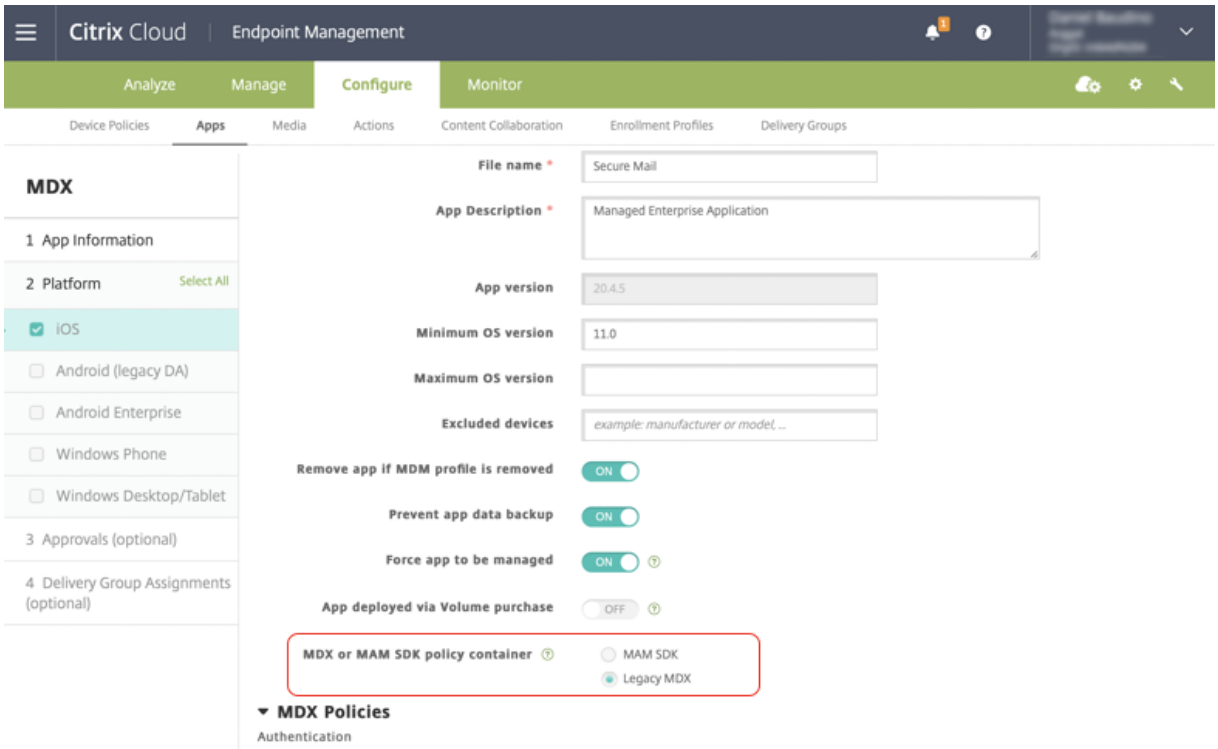
- Das MAM-SDK unterstützt nur Apps, die unter der Android Enterprise-Plattform in Ihrer Citrix Endpoint Management-Bereitstellung veröffentlicht wurden. Bei den neu veröffentlichten Apps ist die Standardverschlüsselung die plattformbasierte Verschlüsselung.
- Das MAM-SDK unterstützt nur die plattformbasierte 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 erstellt.

Wenn Sie Secure Mail in Citrix Endpoint Management konfigurieren, können Sie mit dem Dualmodus Apps entweder wie gehabt mit MDX Toolkit (jetzt Legacy-MDX) verwalten oder für die App-Verwaltung 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 für Ihre Organisation zu verwenden.

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.

Benutzerverbindungen mit dem internen Netzwerk

Verbindungen, die einen Tunnel zum internen Netzwerk benötigen, können einen vollständigen VPN-Tunnel oder eine Variante eines clientlosen VPNs (Tunnel - Web-SSO) verwenden. Dieses Verhalten wird von der Richtlinie “Bevorzugter VPN-Modus”gesteuert. Standardmäßig verwenden Verbindungen “Tunnel - Web-SSO”, und diese Einstellung wird für Verbindungen empfohlen, die Single Sign-On erfordern. Die Einstellung “Vollständiger VPN-Tunnel”wird für Verbindungen empfohlen, die Clientzertifikate oder End-To-End-SSL für Ressourcen im internen Netzwerk einsetzen. Diese Einstellung 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 “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 Serveraufforderungen für Clientzertifikate im vollständigen VPN-Tunnel-Modus 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.

Netzwerkzugangseinschränkungen

Mit der Richtlinie “Netzwerkzugriff”kann der Netzwerkzugriff eingeschränkt werden. Standardmäßig ist der Zugriff auf Secure Mail nicht beschränkt, d. h. es gelten keine Einschränkungen für den Netzwerkzugriff. Apps haben uneingeschränkten Zugriff auf Netzwerke, mit denen das Gerät verbunden ist. Für den Zugriff auf Secure Web ist standardmäßig ein Tunnel zum internen Netzwerk erforderlich, daher wird pro Anwendung ein VPN-Tunnel zum internen Netzwerk für den gesamten Netzwerkzugriff zusammen mit Citrix ADC-Split-Tunneling-Einstellungen verwendet. Sie können den Zugriff blockieren, sodass die App sich verhält, als hätte das Gerät keine Netzwerkverbindung.

Blockieren Sie nicht die Richtlinie “Netzwerkzugriff”, wenn Sie Features wie AirPrint, iCloud sowie Facebook- und Twitter-APIs zulassen.

Die Richtlinie “Netzwerkzugriff”interagiert auch mit der Richtlinie “Hintergrundnetzwerkdienste”. Weitere Informationen finden Sie unter Integration von Exchange Server oder IBM Notes Traveler-Server.

Endpoint Management-Clienteigenschaften

Clienteigenschaften enthalten Informationen, die direkt in Secure Hub auf den Geräten der Benutzer bereitgestellt werden. Clienteigenschaften befinden sich in der Endpoint Management-Konsole unter **Einstellungen > Client > Clienteigenschaften**.

Mit Clienteigenschaften werden Einstellungen wie die Folgenden konfiguriert:

Benutzerkennwortcaching

Die Clienteigenschaft “Benutzerkennwortcaching”ermöglicht die lokale Zwischenspeicherung des Active Directory-Kennworts auf dem Mobilgerät. Wenn Sie “Benutzerkennwortcaching”aktivieren, werden die Benutzer aufgefordert, eine Citrix-PIN oder einen Passcode festzulegen.

Inaktivitätstimer

Der Inaktivitätstimer definiert die Dauer (in Minuten), die ein Gerät inaktiv sein darf, bevor Benutzer für den Zugriff auf eine App zur Eingabe der Citrix-PIN bzw. des Passcodes aufgefordert werden. Zum

Aktivieren dieser Einstellung für eine MDX-App müssen Sie die Richtlinie "App-Passcode"auf **Ein** festlegen. Wenn die Richtlinie "App-Passcode"auf **Aus** festgelegt ist, werden Benutzer für eine vollständige Authentifizierung an Secure Hub umgeleitet. Wenn Sie diese Einstellung ändern, tritt der neue Wert erst in Kraft, wenn ein Benutzer das nächste Mal zur Authentifizierung aufgefordert wird.

Citrix PIN-Authentifizierung

Die Citrix-PIN vereinfacht die Benutzerauthentifizierung. Mit der PIN können Clientzertifikate gesichert oder Active Directory-Anmeldeinformationen lokal auf einem Gerät gespeichert werden. Wenn Sie PIN-Einstellungen konfigurieren, melden sich Benutzer wie folgt an:

1. Wenn Benutzer Secure Hub zum ersten Mal starten, werden sie zur Eingabe einer PIN aufgefordert, die die Active Directory-Anmeldeinformationen zwischenspeichert.
2. Beim nächsten Start einer mobilen Produktivitätsapp, wie zum Beispiel Secure Mail, geben Benutzer nur die PIN ein und melden sich an.

Verwenden Sie die Clienteigenschaften zum Aktivieren der Authentifizierung durch die PIN, zum Angeben des PIN-Typs, der PIN-Stärke und -Länge sowie zum Ändern der Anforderungen.

Authentifizierung per Touch ID bzw. Fingerabdruck

Die Authentifizierung per Fingerabdruck ("Touch-ID-Authentifizierung") bei iOS-Geräten ist eine Alternative zur Citrix PIN. Das Feature ist nützlich, wenn für umschlossene Apps (außer Secure Hub) eine Offlineauthentifizierung, etwa nach Ablaufen des Inaktivitätstimers, erforderlich ist. Sie können dieses Feature für die folgenden Authentifizierungskonfigurationen aktivieren:

- Citrix-PIN + Clientzertifikat
- Citrix-PIN + zwischengespeichertes Active Directory-Kennwort
- Citrix-PIN + Clientzertifikat + zwischengespeichertes Active Directory-Kennwort
- Citrix-PIN ist deaktiviert

Schlägt die Authentifizierung per Fingerabdruck fehl oder bricht der Benutzer die Authentifizierung per Fingerabdruck ab, wird für umschlossene Apps auf die Authentifizierung per Citrix-PIN oder Active Directory-Kennwort zurückgegriffen.

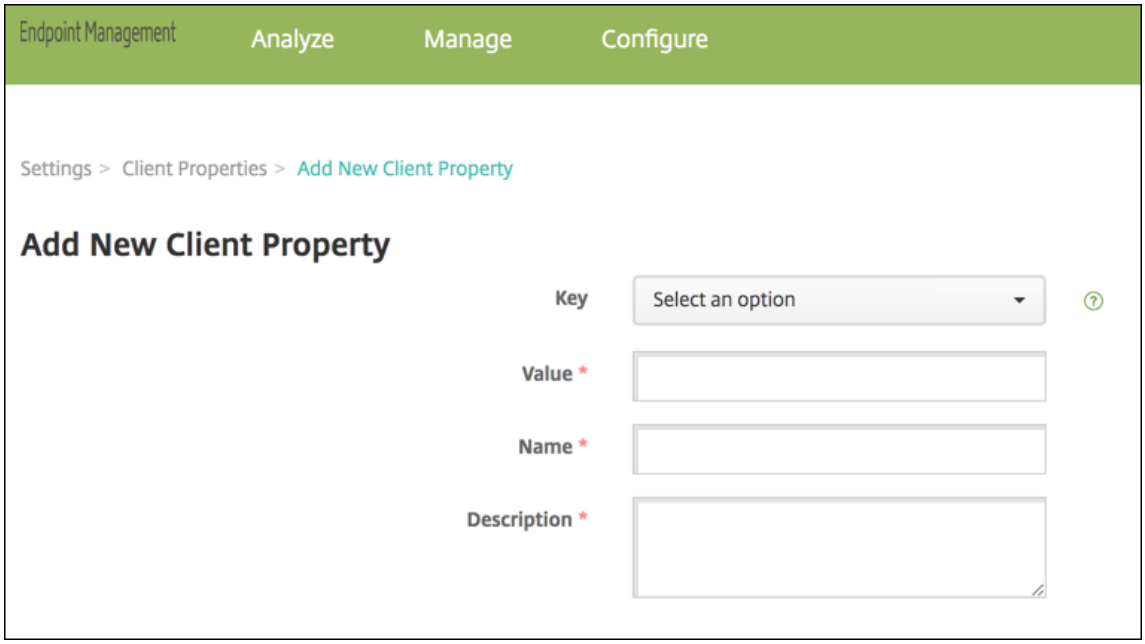
Anforderungen für die Authentifizierung per Fingerabdruck

- iOS-Geräte (Mindestversion 8.1), die die Authentifizierung per Fingerabdruck unterstützen und auf denen mindestens ein Fingerabdruck konfiguriert ist.
- Benutzerentropie muss deaktiviert sein.

Konfigurieren der Authentifizierung per Fingerabdruck

> Wichtig:
>
> Bei aktivierter Benutzerentropie wird die Eigenschaft zur Aktivierung der Touch ID-Authentifizierung ignoriert. Die Benutzerentropie wird über den Schlüssel "Encrypt secrets using the Passcode" aktiviert.

1. Navigieren Sie in der Endpoint Management-Konsole zu **Einstellungen > Client > Clienteigenschaften**.
2. Klicken Sie auf **Hinzufügen**.



3. Fügen Sie den Schlüssel **ENABLE_TOUCH_ID_AUTH** hinzu, legen Sie den **Wert** auf **True** fest und den **Namen der Richtlinie auf Authentifizierung per Fingerabdruck aktivieren**.

Nachdem Sie die Authentifizierung per Fingerabdruck konfiguriert haben, müssen die Benutzer ihre Geräte nicht erneut registrieren.

Informationen zu dem Schlüssel "Encrypt Secrets using Passcode"und Clienteigenschaften im Allgemeinen finden Sie in der Dokumentation zu Endpoint Management unter Clienteigenschaften.

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.

Deaktivieren von Google Analytics

Administratoren können Google Analytics deaktivieren, indem sie die benutzerdefinierte Clienteigenschaft **DISABLE_GA** konfigurieren. Um Google Analytics zu deaktivieren, gehen Sie wie folgt vor:

1. Melden Sie sich bei der Citrix Endpoint Management-Konsole an und navigieren Sie zu **Einstellungen** > **Clienteigenschaften** > **Neue Clienteigenschaft hinzufügen**.
2. Fügen Sie den Wert **DISABLE_GA** zum Feld **Schlüssel** hinzu.
3. Setzt den Wert der Clienteigenschaft auf **true**.

> **Hinweis:**
>
> Wenn Sie den Wert **DISABLE_GA** nicht in der Citrix Endpoint Management-Konsole konfigurieren, sind Google Analytics-Daten aktiv.

Features nach Plattform

September 12, 2023

In den folgenden Tabellen sind die Funktionen für die mobilen Produktivitätsapps von Citrix zusammengefasst. **X** bedeutet, das Feature ist für die Plattform verfügbar. Informationen zu Features von QuickEdit finden Sie in dem Artikel zu Citrix QuickEdit.

Citrix Secure Hub

Feature	iOS	Android
Für Authentifizierung anmelden	X	X
Richtlinieneinhaltung überwachen	X	X
Auf Apps und Desktops zugreifen	X	X
HDX-Apps und Desktops	X	X
Problemprotokolle erstellen und senden	X	X
Screenshots an Protokolle anfügen	X	X

Feature	iOS	Android
Helpdesk in der App kontaktieren	X	X
Citrix Support aus der App heraus kontaktieren	X	X
Absturzerfassung und -analyse	X	X
Offlineauthentifizierung	X	X
Protokolle mit Citrix Secure Mail senden	X	X
Google Analytics	X	X
Hoch- und Querformatmodus	X	X
App-interne Anweisungen zur Herstellung einer Vertrauensstellung mit Apps	X	X
Falls für E-Mail registriert, automatische Registrierung bei Secure Mail (nur MAM)	X	X
Offlineauthentifizierung per Touch ID	X	X
Registrieren mit abgeleiteten Anmeldeinformationen	X	
Biometrische Authentifizierung		X
Verwendung von Workspace App Store	X	X

Citrix Secure Mail

Feature	iOS	Android
E-Mail-Produktivität		
Entwürfe minimieren	X	X
Senden von E-Mails rückgängig machen		X
Verschlüsselungsverwaltung	X	X
Widget für Kalenderagenda		X

Feature	iOS	Android
Kontaktbild in Secure Mail	X	X
Unterstützung für dynamische E-Mails	X	X
Automatische Synchronisierung des Ordners “Entwürfe”	X	X
Anlagen im Ordner **Entwürfe** synchronisieren		X
Senden, Empfangen, Antworten, Allen antworten und E-Mails weiterleiten	X	X
Erstellen, Bearbeiten und Löschen von Entwürfen	X	X
E-Mails markieren	X	X
Ungelesen	X	X
Aller Ordner und Unterordner anzeigen	X	X
Automatisches Speichern von Entwürfen, wenn App in den Hintergrund verschoben wird	X	X
E-Mail in Notizen mit Citrix Secure Notes konvertieren **Wichtig:** Secure Notes hat das Ende des Lebenszyklus (End Of Life, EOL) am 31. Dezember 2018 erreicht. Weitere Informationen finden Sie unter Ende des Lebenszyklus und veraltete Apps.	X	X
E-Mails durchsuchen (lokal und Server)	X	X
E-Mail-Synchronisierungszeitraum auswählen (bis zu 1 Monat oder alle E-Mails)	X	X
Ungelesene E-Mails anzeigen	X	X

Feature	iOS	Android
Sichere Anlagenanzeige/Wiedergabe für Bilder, Videos und Audiodateien	X	X
Mehrere Anlagen	X	X
Antworten und Anlagen anfügen	X	X
Dateien aus Citrix Files anfügen	X	X
Dateien aus eingeschränkten Citrix Files-Zonen und Connectors anfügen	X	X
Anlagenrepository	X	X
Rich-Text bearbeiten	X	X
E-Mail-Benachrichtigung mit Betreff, Vorschau auf gesperrtem Bildschirm	X	X
Beantworten und Löschen von E-Mails und Einladungen über den Benachrichtigungsbildschirm	X	
Foto aufnehmen oder anfügen	X	X
Mehrere Meldungen auswählen	X	X
Anlagen herunterladen	X	X
Inlinebilder laden	X	X
Schnell sortieren	X	X
Senden, Öffnen und Speichern von ZIP-Dateianlagen	X	X
Hoch- und Querformatmodus	X; In der E-Mail-Liste sowie in den Ansichten zum Lesen und Verfassen von E-Mails und für Kalender und Kontakte	X: Nur in den Ansichten zum Verfassen und Lesen von E-Mails
Eingefügter Text behält Formatierungen bei	X	X
SMS von Kontakten	X	X

Feature	iOS	Android
FaceTime von Kontakten	X	
Wegen Verbindungsproblemen oder vollem Postfach nicht gesendete Nachrichten in Postausgang speichern	X	X
Blasenanzeige zuletzt verwendeter Ordner		X
E-Mail durch Ziehen aktualisieren	X	X
Zeitstempel der letzten Aktualisierung	X	X
Streichen nach links bei Nachrichten	X	X
Unterstützung für Microsoft Exchange und IBM Notes Traveler	X	X
Zum Aktualisieren von E-Mail, Kalender und Kontakten tippen	X	X
Einstellungen für Gerätezugriff und Schriftgrad in E-Mail-Ansichten beibehalten	X	X
S/MIME-Signatur und Verschlüsselung	X	X
S/MIME-Zertifikatimport per E-Mail	X	X
S/MIME, Intercede-Integration	X	
S/MIME, Entrust-Integration	X	
Microsoft IRM-Schutz für Nachrichtentext	X	X
Pushbenachrichtigungen	X	X
Pushbenachrichtigungen an Posteingang aktualisieren automatisch alle Ordner einschließlich Kalender	X	
Office 365-Dokumente öffnen	X	X
3D-Touchaktionen	X	

Feature	iOS	Android
Kontextbezogene Symbole auf Sperrbildschirm	X	X
Ordner durchsuchen	X	X
Ordner für VIP-Mail	X	X
Unterstützung für dynamischen Typ	X	X
Erweiterte Ordner beibehalten	X	X
Klassifizierungsmarkierungen für Nachrichten	X	X
Rechtschreibprüfung	X	
Letztes Foto anfügen	X	X
URL-Vorschau	X	X
Citrix Files-Links in Citrix Files öffnen	X	X
Unterstützung für .pass-Dateien	X	
Mehrere E-Mails im Suchmodus auswählen	X	X
Inlinebild einfügen	X	X
Upgrade auf Exchange ActiveSync (EAS) Version 16	X	X
Einschränken der Verwendung unbekannter oder persönlicher Domänen durch Benutzer	X	
Unterstützung für extrabreite Gerätebildschirme		X
Konfigurieren mehrerer Exchange-Konten	X	X
Streichen nach links oder rechts für weitere Aktionen	X	X
Verschlüsseln von Antworten auf E-Mail oder weitergeleiteter E-Mail	X	
E-Mails und eingebettete Bilder drucken	X	

Feature	iOS	Android
Verwenden Sie die Vorschaueinstellung, um zu konfigurieren, wie viele Zeilen des Textkörpers als Vorschau in der Postfachansicht angezeigt werden.	X	
Unterstützung für dynamische E-Mails	X	X
In-App-Vorschau von Anlagen (MS Office oder Bilder)	X	X
Persönliche Kontaktgruppen	X	X
Migration von Benutzernamen auf E-Mail-Adressen (UPN)	X	X
Phishing-E-Mails melden	X	X
Moderne Authentifizierung (OAuth)	X	X
Anlagen drucken	X	
Android Enterprise (Android for Work)	X	
Rich-Text-Signaturen	X	
Pushbenachrichtigungen mit Rich-Media-Inhalt	X	
Feeds	X	X
Verbesserungen beim Anhängen von Fotos	X	X
Gruppenbenachrichtigungen	X	
Slack-Integration (Vorschau)	X	X
Feeds verwalten	X	
Interne Domänen	X	X
Feeds verwalten	X	X
MS Teams-Integration	X	X
Option zur Selbstdiagnose (**Problembehandlung**)		X
Dualmodus (MAM-SDK)	X	X

Feature	iOS	Android
Selbstdiagnosetool		X
Kalender		
Vorschau und Import von ICS-Dateien als Kalenderereignisse		X
Drag & Drop für Kalenderereignisse	X	X
Ansichten für Tag, Woche, Monat und Tagesordnung	X	X
Detaillierte Erinnerungen auf gesperrtem Bildschirm	X	X
Für sechs Monate synchronisieren	X	X
Ereignisse als “privat”festlegen	X	X
Zur Stunde vor erstem Ereignis scrollen	X	
Manuelle Aktualisierungsoptionen	X	X
Festlegen von Erinnerungen	X	X
Durch Tippen Adresse in Kartenanwendung anzeigen	X	X
Wochennummern	X	X
Unterstützung für dynamischen Typ	X	X
Sicherheitsklassifizierungsmarker	X	X
Langes Tippen auf Adressen	X	
Anfang der Arbeitswoche festlegen	X	X
Fokus der Wochenansicht auf ausgewähltes Datum festlegen	X	
Aktuelles Datum immer hervorgehoben	X	X
Kalender-Anlagen im Anlagenrepository	X	X

Feature	iOS	Android
Unterstützung für den persönlichen Kalender	X	X
Konflikte mit persönlichen Kalenderereignissen anzeigen		X
Kalenderereignisse drucken	X	
Tippen auf Telefonnummern und Webadressen in einer Kalenderbetreffzeile	X	
Kalender durchsuchen	X	
Besprechungen		
Antworten, Allen antworten, Besprechung weiterleiten	X	X
Organisatoransicht für Antworten auf Einladungen	X	X
Organisatoransicht für Verfügbarkeit Eingeladener mit empfohlener Verfügbarkeit	X	X
An Online-Meeting durch Tippen teilnehmen **Hinweis:** Für WebEx und Lync müssen Sie Richtlinien in Citrix Endpoint Management konfigurieren, um diese Apps zu aktivieren.	X	X
An Audiokonferenzen durch Tippen teilnehmen	X	X
Online-Meeting, Audiokonferenz in neuer Einladung planen	X	X
ShareFile-Links in neue Einladung einfügen	X	X
Einladungen mit Anlagen weiterleiten	X	X
Verspätungs-E-Mail durch Tippen senden	X	X

Feature	iOS	Android
Besprechungsorganisator durch Tippen antworten	X	X
Allen zu einem Meeting Eingeladenen durch Tippen antworten	X	X
Allen zu einem Meeting Eingeladenen durch Tippen antworten	X	X
Allen zu einem Meeting Eingeladenen durch Tippen mit Anlagen antworten	X	X
Einwahl bei GoToMeeting	X	X
Einladung über Sperrbildschirm oder Benachrichtigungsbildschirm beantworten	X	X
Einwahl bei WebEx- oder Lync-Besprechungen	X	X
Abgelehnte Ereignisse ausblenden	X	X
Mehr als 3 gleichzeitige Termine anzeigen	X	X
Schnellansicht für Eingeladenenstatus	X	X
Löschen, Antworten, Allen antworten, Kommentare hinzufügen bei abgesagten Ereignissen	X	X
Name des Organisators auf weitergeleiteten Einladungen anzeigen	X	X
Gemeinsam genutzte Geräte	X	X
Teilnahme an Skype for Business-Besprechungen	X	X

Feature	iOS	Android
Antworten auf Besprechungs-benachrichtigungen mit “Annehmen”, “Ablehnen”und “Mit Vorbehalt”.	X	X
Antworten auf Benachrichtigungen zu erhaltenen Nachrichten mit “Antworten”und “Löschen”.	X	
Kontakte		
Ordner unter **Kontakte** erstellen		X
2-Wege-Kontaktsynchronisierung	X	X
Detaillierte GAL-Suche für Kontaktinformationen	X	X
Secure Mail-Kontakte in lokale Kontakte exportieren und mit lokalen Kontakten synchronisieren	X	X
Kontakte: Favoriten und Kategorie		X
Steuerung, welche Kontaktfelder exportiert werden	X	X
Kontaktdetails für Secure Mail-externe Kontakte	X	X
Unterstützung für dynamischen Typ	X	X
Kontakte als VIPs kennzeichnen	X	X
Kontakte mit `.vcards` teilen	X	X
Anzeigen von Kontakten mit langem Fingertipp		X
Kontakte exportieren, auch wenn natives E-Mail-Konto vorhanden ist	X	X
Ordner und Unterordner anzeigen	X	

Feature	iOS	Android
Auf dem Gerät konfigurierte Einstellungen		
Unterstützung von iMessage	X	
Erweiterte Optionen zum Steuern von Benachrichtigungen	X	X
Steuerung von Benachrichtigungen auf dem Sperrbildschirm	X	X
Benachrichtigungstöne für E-Mail und Kalender	X	X
Ordner automatisch aktualisieren	X	X
Interne und externe Abwesenheitsbenachrichtigungen einrichten	X	X
Vor Löschen fragen	X	X
Konversationsthread oder chronologische Ansicht	X	X
Anlagen mit Wi-Fi laden	X	X
Anlagen mit Wi-Fi laden als Standard festlegen	X	X
E-Mail-Synchronisierungszeitraum festlegen	X	X
Unbeschränkte Synchronisierung/Synchronisierung aller E-Mails		X
E-Mail-Signatur festlegen	X	X
Kontakte nach Vor- oder Nachnamen sortieren	X	X
Automatisch weiter	X	X
Heimatzeitzone verwenden		X
Vorlagen für schnelle Antworten		X

Feature	iOS	Android
Pushhäufigkeit für E-Mail konfigurieren		X
Einstellungen für Export/Import	X	X
Auf die Taste “Zurück”auf dem Gerät tippen, um die Optionen der unverankerten Aktionstaste auszublenden		X
Microsoft Teams	X	X

Citrix Secure Web

Feature	iOS	Android
Verwenden Sie zwei Apps gleichzeitig mit Multitasking	X	
Herunterladen von Dateien	X	X
Favorit hinzufügen	X	X
Gespeicherte Benutzernamen und Kennwörter löschen	X	X
Löschen von Cache/Verlauf/Cookies	X	X
Popups blockieren	X	X
Offlineseiten speichern	X	X
Suchen in Adressleiste	X	X
Öffnen von heruntergeladen Elementen aus Benachrichtigungen	X	X
Automatisches Speichern von Kennwörtern	X	X
Proxyunterstützung		
Unternehmensproxies	X	X
URL-Sperrlisten und Positivlisten	X	X

Feature	iOS	Android
Verlauf	X	X
Standard-Homepage	X	X
Registerkarten	X	X
Pushbereitstellung von Lesezeichen	X	X
Bildschirmaufnahme blockieren		X
Suche in aktueller Seite	X	X
3D-Touchaktionen	X	
Gemeinsam genutzte Geräte	X	X
Dateimanipulationsschutz für gemeinsam genutzte Geräte	X	
Einstellungen für Export/Import	X	X
Hoch- und Querformatmodus	X	X
Android Enterprise (Android for Work)		X
Zum Aktualisieren des Bildschirminhalts ziehen	X	X
Secure Web als Standardbrowser		X

Citrix Secure Hub

February 28, 2024

Citrix Secure Hub ist das Startpunkt für die mobilen Produktivitätsapps. Benutzer registrieren ihre Geräte in Secure Hub, um Zugriff auf den App-Store zu erhalten. Im App-Store können sie von Citrix entwickelte mobile Produktivitätsapps und Apps von Drittanbietern hinzufügen.

Sie können Secure Hub und andere Komponenten von der Citrix Endpoint Management-Downloadseite herunterladen.

Angaben zu den Systemanforderungen für Secure Hub und die mobilen Produktivitätsapps finden Sie unter Systemanforderungen.

Aktuelle Informationen zu mobilen Produktivitätsapps finden Sie unter Aktuelle Ankündigungen.

In den folgenden Abschnitten werden die neuen Features in aktuellen und früheren Versionen von Secure Hub aufgeführt.

> **Hinweis:**
>
> Unterstützung für die Versionen Android 6.x und iOS 11.x von Secure Hub endete im Oktober 2023.

Was ist neu in der aktuellen Version

Secure Hub für Android 23.12.0

Auf der Anmeldeseite einen Hinweis zur Authentifizierungs-PIN hinzufügen Ab Release 23.12.0 können Sie auf der Anmeldeseite einen Hinweis zur Authentifizierungs-PIN hinzufügen. Dieses Feature ist optional und gilt für Geräte, die für die Zweifaktorauthentifizierung registriert sind. Anhand des Hinweises erfahren Sie, wie Sie auf die PIN zugreifen können.

Sie können einen Hinweis als Text oder Link konfigurieren. Der Hinweistext bietet präzise Informationen zur PIN, während der Link detaillierte Informationen zum Zugriff auf die PIN enthält. Weitere Informationen zum Konfigurieren eines Hinweises finden Sie unter Hinweis über die Citrix Endpoint Management-Konsole konfigurieren.

nFactor-Authentifizierung unterstützt das Single Sign-On-Feature Ab Secure Hub für Android Version 23.12.0 unterstützt die nFactor-Registrierung oder -Anmeldung für Mobile Application Management (MAM) das SSO-Feature (Single Sign-On). Mit diesem Feature können zuvor eingegebene Anmeldeinformationen den MAM-Registrierungs- oder Anmeldevorgang durchlaufen, sodass Benutzer sie nicht erneut manuell eingeben müssen. Weitere Informationen zur nFactor SSO-Eigenschaft finden Sie in der Referenz der Clienteigenschaften in der Dokumentation zu Citrix Endpoint Management.

Unterstützung für das vollständige Löschen im Direktstartmodus Bisher mussten Sie das Gerät entsperren, um einen vollständigen Löschbefehl auf einem neu gestarteten Gerät auszuführen. Jetzt können Sie im Direktstartmodus einen Befehl zum vollständigen Löschen ausführen, auch wenn das Gerät gesperrt ist. Diese Funktion ist aus Sicherheitsgründen hilfreich, insbesondere wenn sich das Gerät im Besitz einer unbefugten Person befindet. Weitere Informationen zum Befehl für das vollständige Löschen finden Sie unter Sicherheitsaktionen in der Citrix Endpoint Management-Dokumentation.

Die Ladegeschwindigkeit des App Store von Secure Hub wurde optimiert Der App Store in Secure Hub wird jetzt schneller als zuvor geladen, sodass Benutzer schneller darauf zugreifen können.

Was ist neu in früheren Releases

Secure Hub für iOS 23.11.0

Auf der Anmeldeseite einen Hinweis zur Authentifizierungs-PIN hinzufügen Ab Release 23.11.0 können Sie auf der Anmeldeseite einen Hinweis zur Authentifizierungs-PIN hinzufügen. Dieses Feature ist optional und gilt für Geräte, die für die Zweifaktorauthentifizierung registriert sind. Anhand des Hinweises erfahren Sie, wie Sie auf die PIN zugreifen können.

Sie können einen Hinweis als Text oder Link konfigurieren. Der Hinweistext bietet präzise Informationen zur PIN, während der Link detaillierte Informationen zum Zugriff auf die PIN enthält. Weitere Informationen zum Konfigurieren eines Hinweises finden Sie unter Hinweis über die Citrix Endpoint Management-Konsole konfigurieren.

nFactor-Authentifizierung unterstützt das Single Sign-On-Feature Ab Secure Hub für iOS Version 23.11.0 unterstützt die nFactor-Registrierung oder -Anmeldung für Mobile Application Management (MAM) das SSO-Feature (Single Sign-On). Mit diesem Feature können zuvor eingegebene Anmeldeinformationen den MAM-Registrierungs- oder Anmeldevorgang durchlaufen, sodass Benutzer sie nicht erneut manuell eingeben müssen.

Weitere Informationen zur nFactor SSO-Eigenschaft finden Sie in der Referenz der Clienteigenschaften in der Dokumentation zu Citrix Endpoint Management.

Secure Hub 23.10.0

Secure Hub für Android

Secure Hub für Android 23.10.0 unterstützt Android 14. Ein Upgrade von Secure Hub auf Version 23.10.0 gewährleistet eine kontinuierliche Unterstützung für Geräte, die auf Android 14 aktualisiert werden.

Secure Hub 23.9.0

Secure Hub für Android

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Secure Hub 23.8.1

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

Secure Hub 23.8.0

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

Secure Hub 23.7.0

Secure Hub für Android

Play Integrity API Die SafetyNet Attestation API wird in Kürze von Google eingestellt und auf die empfohlene Play Integrity API migriert.

Weitere Informationen finden Sie unter Play Integrity API in dem Dokument zu Citrix Endpoint Management.

Einzelheiten zur Einstellung von Produkten und Features finden Sie unter Veraltete und entfernte Produkte und Features in dem Dokument zu Citrix Endpoint Management.

Informationen zur Android-SafetyNet finden Sie unter SafetyNet.

Secure Hub 23.4.0

Secure Hub für iOS

Verbesserte Benutzererfahrung Ab Version 23.4.0 verbessert Secure Hub für iOS die folgenden Aspekte des Benutzererlebnisses:

- Storeerfahrung:

  ⊠ Bisher wurde die Seite “Meine Apps”zuerst angezeigt. In Version 23.4.0 wird die Store-Seite zuerst angezeigt.

  ⊠ Bisher führte der Secure Hub-Store die Aktion zum erneuten Laden jedes Mal aus, wenn Benutzer auf die Store-Option klickten.

  Version 23.4.0 bietet nun eine bessere Benutzererfahrung. Jetzt wird die App neu geladen, wenn Benutzer die App zum ersten Mal starten und wenn sie die App neu starten oder auf dem Bildschirm nach unten wischen.

- Benutzeroberfläche: Bisher war die Option zum Abmelden unten links auf dem Bildschirm. In Version 23.4.0 ist die Option zum Abmelden Teil des Hauptmenüs und befindet sich über der Option "Info".
- Hyperlinks: Bisher wurden die Hyperlinks auf der Detailseite der App als einfacher Text angezeigt. In Version 23.4.0 sind die Hyperlinks anklickbar und unterstrichen, um sie als Links zu markieren.

Wechsel vom MDX- zum MAM-SDK Ab Version 23.4.0 wurde der Wechsel vom älteren MDX- zum MAM-SDK für iOS-Apps im dualen Modus verbessert. Durch diese Funktion wird die Benutzererfahrung bei der Verwendung mobiler Produktivitätsapps verbessert, indem sie Warnmeldungen reduziert und zu Secure Hub wechselt.

Citrix-PIN zum Entsperren von Apps verwenden Bisher gaben Endbenutzer den Gerätepasscode ein, um auf Mobile App Management (MAM) basierende Apps zu entsperren.

Ab Version 23.4.0 können Endbenutzer die Citrix-PIN als Passcode eingeben, um MAM-basierte Apps zu entsperren. Administratoren können die Komplexität des Passcodes mit den Clienteigenschaften auf dem CEM-Server konfigurieren.

Wenn eine App länger als die zulässige Zeit inaktiv ist, können Endbenutzer je nach der vom Administrator festgelegten Konfiguration die Citrix-PIN eingeben, um die App zu entsperren.

Für Secure Hub für Android gibt es zum Konfigurieren des Inaktivitätstimers in MAM-Anwendungen eine separate Clienteigenschaft. Weitere Informationen finden Sie unter Separater Inaktivitätstimer für Android.

Secure Hub 23.4.1

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

Secure Hub 23.4.0

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

Secure Hub 23.2.0

Secure Hub für Android

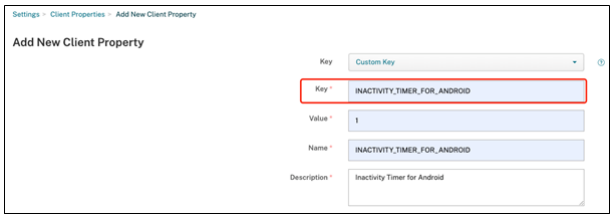
> **Hinweis:**
>
> - Es werden keine Analysedaten für Benutzer in der Europäischen Union (EU), dem Europäischen Wirtschaftsraum (EWR), der Schweiz und dem Vereinigten Königreich (UK) gesammelt.

MDX-VPN im vollständigen Tunnelmodus Das MDX Micro-VPN (vollständiger Tunnelmodus) ist veraltet.

Weitere Informationen finden Sie unter Auslaufende Features in der Dokumentation von Citrix Endpoint Management.

Separater Inaktivitätstimer für Android Bisher war die Clienteigenschaft **Inaktivitätstimer** für Secure Hub für Android und iOS üblich.

Ab Version 23.2.0 kann ein IT-Administrator die neue Clienteigenschaft **Inactivity_Timer_For_Android** verwenden, um den Inaktivitätstimer von iOS zu trennen. Ein IT-Administrator kann den **Wert** des **Inactivity_Timer_For_Android** auf 0 setzen, um den Android-Inaktivitätstimer unabhängig zu deaktivieren. Auf diese Weise funktionieren alle Apps im Arbeitsprofil, einschließlich Secure Hub, nur mit PIN.



Weitere Informationen zum Hinzufügen und Ändern einer Clienteigenschaft finden Sie unter Clienteigenschaften in der XenMobile-Dokumentation.

Secure Hub 22.11.0

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 22.9.0

Secure Hub für Android Diese Version enthält:

- Passcodekomplexität für Gerätepasscode (Android 12+)
- Unterstützung für SDK 31
- Bugfixes

Passcodekomplexität für Gerätepasscode (Android 12+) Die Passcodekomplexität wird gegenüber der benutzerdefinierten Kennwortanforderung bevorzugt. Der Passcodekomplexitätsgrad ist eine der vordefinierten Ebenen. Daher kann der Endbenutzer kein Kennwort mit einem niedrigeren Komplexitätsgrad festlegen.

Die Passcodekomplexität für Geräte mit Android 12+ ist wie folgt:

- **Passcodekomplexität anwenden:** Erfordert ein Kennwort mit einer Komplexitätsstufe, die von der Plattform und nicht von einer benutzerdefinierten Kennwortanforderung definiert wird. Nur für Geräte mit Android 12+ und Secure Hub 22.9 und höher.
- **Komplexitätsgrad:** Vordefinierte Ebenen der Kennwortkomplexität.
  - **Ohne:** Kein Kennwort erforderlich.
  - **Niedrig:** Das Kennwort kann Folgendes sein:
    * Ein Muster
    * Eine PIN mit mindestens vier Ziffern
  - **Mittel:** Das Kennwort kann Folgendes sein:
    * Eine PIN mit mindestens vier Ziffern ohne Sequenzen, die sich wiederholen (4444) oder geordnet sind (1234)
    * Alphabetisch mit mindestens vier Zeichen
    * Alphanumerisch mit mindestens vier Zeichen
  - **Hoch:** Das Kennwort kann Folgendes sein:
    * Eine PIN mit mindestens acht Ziffern ohne Sequenzen, die sich wiederholen (4444) oder geordnet sind (1234)
    * Alphabetisch mit mindestens sechs Zeichen
    * Alphanumerisch mit mindestens sechs Zeichen

> **Hinweise:**
>
> - Für BYOD-Geräte mit Android 12 und höher sind Passcodeeinstellungen wie "Mindestlänge" , "Erforderliche Zeichen", "Biometrische Erkennung"und "Erweiterte Regeln"nicht anwendbar. Verwenden Sie stattdessen Passcodekomplexität.
> - Wenn die Passcodekomplexität für Arbeitsprofil aktiviert ist, muss auch die Passcodekomplexität für die Geräteseite aktiviert werden.

Weitere Informationen finden Sie unter Android Enterprise-Einstellungen in der Dokumentation von Citrix Endpoint Management.

Secure Hub 22.7.0

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 22.6.0

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 22.5.0

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub 22.4.0

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 22.2.0

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 21.11.0

Secure Hub für Android

Unterstützung von Arbeitsprofilen für firmeneigene Geräte Auf Android Enterprise-Geräten können Sie Secure Hub jetzt im Arbeitsprofilmodus für firmeneigene Geräte registrieren. Diese Funktion ist auf Geräten mit Android 11 oder höher verfügbar. Geräte, die zuvor im Modus "Corporate Owned Personally Enabled"(COPE) registriert waren, werden automatisch in den Arbeitsprofilmodus für firmeneigene Geräte migriert, wenn das Gerät von Android 10 auf Android 11 oder höher aktualisiert wird.

Secure Hub 21.10.0

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub für Android **Unterstützung für Android 12**. Ab diesem Release wird Secure Hub auf Geräten unterstützt, auf denen Android 12 ausgeführt wird.

Secure Hub 21.8.0

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub 21.7.1

Secure Hub für Android **Unterstützung von Android 12 auf bereits registrierten Geräten.** Wenn Sie ein Upgrade auf Android 12 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. Dieses Release gewährleistet ein nahtloses Upgrade von Android 11 auf Android 12 für bereits registrierte Benutzer.

> **Hinweis:**
>
> Wenn Secure Hub nicht auf Version 21.7.1 aktualisiert wurde, bevor Sie ein Upgrade auf Android 12 durchführen, muss Ihr Gerät möglicherweise erneut registriert oder auf die Werkseinstellungen zurückgesetzt werden, um die vorherige Funktionalität wiederherzustellen.
>
> Citrix ist bestrebt, Android 12 vom 1. Tag an zu unterstützen und plant weitere Updates für nachfolgende Versionen von Secure Hub, damit auch sie Android 12 vollständig unterstützen.

Secure Hub 21.7.0

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 21.6.0

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 21.5.1

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 21.5.0

Secure Hub für iOS In diesem Release funktionieren mit dem MDX Toolkit bis einschließlich Version 19.8.0 umschlossene Apps nicht mehr. Umschließen Sie Ihre Apps mit dem neuesten MDX Toolkit, um die ordnungsgemäße Funktion wieder herzustellen.

Secure Hub 21.4.0

Überarbeitung der Farben für Secure Hub. Secure Hub ist konform mit Citrix Branding-Farbaktualisierungen.

Secure Hub 21.3.2

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub 21.3.0

Dieses Release enthält Bugfixes.

Secure Hub 21.2.0

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 21.1.0

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 20.12.0

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub für Android Secure Hub für Android unterstützt den Direct Boot-Modus. Weitere Informationen zum Direct Boot-Modus finden Sie in der Android-Dokumentation unter *Developer.android.com*.

Secure Hub 20.11.0

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

Secure Hub 20.10.5

Dieses Release enthält Bugfixes.

Secure Hub 20.9.0

Secure Hub für iOS Secure Hub für iOS unterstützt iOS 14.

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub 20.7.5

Secure Hub für Android

- Secure Hub für Android unterstützt Android 11.
- **Umstieg von Secure Hub 32-Bit auf 64-Bit für Apps.** In Secure Hub Version 20.7.5 endet die Unterstützung für die 32-Bit-Architektur für Apps, und Secure Hub wurde auf 64-Bit aktualisiert. Citrix empfiehlt Kunden, ein Upgrade von 20.6.5 auf Version 20.7.5 durchzuführen. Wenn Benutzer das Upgrade auf Secure Hub Version 20.6.5 überspringen und direkt von 20.1.5 auf 20.7.5 aktualisieren, müssen sie sich neu authentifizieren. Bei der Neuauthentifizierung müssen Sie Anmeldeinformationen eingeben und die Secure Hub PIN zurücksetzen. Secure Hub Version 20.6.5 ist im Google Play Store verfügbar.
- **Installieren von Updates aus dem App Store.** Wenn in Secure Hub für Android Updates für Apps verfügbar sind, wird die App hervorgehoben, und im App Store-Bildschirm wird das Feature **Updates verfügbar** angezeigt.

  Wenn Sie auf **Updates verfügbar** tippen, wird im Store eine Liste der Apps mit ausstehenden Updates angezeigt. Tippen Sie auf **Details** für die App, um die Updates zu installieren. Nachdem die App aktualisiert wurde, ändert sich der Abwärtspfeil unter **Details** in ein Häkchen.

Secure Hub 20.6.5

Secure Hub für Android **Umstieg von 32-Bit auf 64-Bit für Apps.** Secure Hub 20.6.5 ist das letzte Release, das eine 32-Bit-Architektur für mobile Android-Apps unterstützt. In späteren Releases

unterstützt Secure Hub die 64-Bit-Architektur. Citrix empfiehlt Benutzern, ein Upgrade auf Secure Hub Version 20.6.5 durchzuführen, damit Benutzer ohne Neuauthentifizierung auf höhere Versionen aktualisieren können. Wenn Benutzer das Upgrade auf Secure Hub Version 20.6.5 überspringen und stattdessen direkt auf 20.7.5 aktualisieren, müssen sie sich neu authentifizieren. Bei der Neuauthentifizierung müssen Sie Anmeldeinformationen eingeben und die Secure Hub PIN zurücksetzen.

> **Hinweis:**
>
> Release 20.6.5 blockiert nicht die Registrierung von Geräten, auf denen Android 10 im Geräteadministratormodus ausgeführt wird.

Secure Hub für iOS **Aktivieren eines auf iOS-Geräten konfigurierten Proxys.** In Secure Hub für iOS müssen Sie die neue Clienteigenschaft `ALLOW_CLIENTSIDE_PROXY` aktivieren, wenn Sie Benutzern erlauben möchten, Proxyserver zu verwenden, die sie unter **Einstellungen > Wi-Fi** konfigurieren. Weitere Informationen finden Sie unter `ALLOW_CLIENTSIDE_PROXY` in Referenz der Clienteigenschaften.

Secure Hub 20.3.0

> **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.

Secure Hub für iOS

- **Netzwerkerweiterung deaktiviert.** Aufgrund der jüngsten Änderungen an den App Store-Überprüfungsrichtlinien unterstützt Secure Hub ab Release 20.3.0 keine Network Extension (NE) auf Geräten mit iOS. NE hat keine Auswirkungen auf von Citrix entwickelte mobile Produktivitätsapps. Das Entfernen von NE hat jedoch Auswirkungen auf bereitgestellte MDX-umschlossene Unternehmensapps. Endbenutzer können zusätzliche Wechsel zu Secure Hub bemerken, während Komponenten wie Autorisierungstoken, Timer und PIN-Versuche synchronisiert werden. Weitere Informationen finden Sie unter https://support.citrix.com/article/CTX270296.

> **Hinweis:**
>
> Neue Benutzer werden nicht aufgefordert, VPN zu installieren.

- **Unterstützung für verbesserte Registrierungsprofile.** Secure Hub unterstützt die erweiterten Registrierungsprofilfunktionen, die für Citrix Endpoint Management unter Registrierungsprofile angekündigt wurden.

Secure Hub 20.2.0

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub 20.1.5

Diese Version enthält:

- Update für die Formatierung und Anzeige der Datenschutzrichtlinie für Benutzer. Dieses Featureupdate ändert den Registrierungsablauf für Secure Hub.
- Bugfixes.

Secure Hub 19.12.5

Dieses Release enthält Bugfixes.

Secure Hub 19.11.5

Dieses Release enthält Bugfixes.

Secure Hub 19.10.5

Secure Hub für Android **Secure Hub im COPE-Modus registrieren.** Registrieren Sie in Android Enterprise-Geräten Secure Hub im COPE-Modus (Corporate Owned Personally Enabled), wenn Citrix Endpoint Management im COPE-Registrierungsprofil konfiguriert ist.

Secure Hub 19.10.0

Dieses Release enthält Bugfixes.

Secure Hub 19.9.5

Secure Hub für iOS Dieses Release enthält Bugfixes.

Secure Hub für Android **Unterstützte Verwaltung von Keyguard-Funktionen für Android Enterprise-Arbeitsprofile und für vollständig verwaltete Geräte.** Android Keyguard verwaltet die Sperrbildschirme für Gerät und Arbeitsprofil. Nutzen Sie die Geräterichtlinie für die Keyguard-Verwaltung in Citrix Endpoint Management, um die Keyguard-Funktion auf Arbeitsprofilgeräten und auf vollständig verwalteten und dedizierten Geräten zu verwalten. Mit der Keyguard-Verwaltung können Sie festlegen, ob Benutzer vor dem Entsperren des Keyguard-Bildschirms auf Funktionen wie "Trust Agents"und "Sichere Kamera"zugreifen können. Sie können jedoch auch alle Keyguard-Funktionen deaktivieren.

Weitere Informationen zu den Einstellungen dieser Funktion und zum Konfigurieren der Geräterichtlinie finden Sie unter Geräterichtlinie für die Keyguard-Verwaltung.

Secure Hub 19.9.0

Secure Hub für iOS Secure Hub für iOS unterstützt iOS 13.

Secure Hub für Android Dieses Release enthält Bugfixes.

Secure Hub für Android 19.8.5

Dieses Release enthält Bugfixes.

Secure Hub 19.8.0

Secure Hub für iOS Dieses Release enthält Leistungsverbesserungen und Bugfixes.

Secure Hub für Android **Unterstützung für Android Q.** Dieses Release enthält Unterstützung für Android Q. Informieren Sie sich vor dem Upgrade auf die Android Q-Plattform, wie die Veraltung von Google Device Administration-APIs sich auf Geräte mit Android Q auswirkt: Migration von der Gerätevverwaltung zu Android Enterprise. Siehe auch den Blog Citrix Endpoint Management und Android Enterprise im Wandel.

Secure Hub 19.7.5

Secure Hub für iOS Dieses Release enthält Leistungsverbesserungen und Bugfixes.

Secure Hub für Android **Unterstützung für Samsung Knox SDK 3.x.** Secure Hub für Android unterstützt Samsung Knox SDK 3.x. Weitere Informationen zur Migration auf Samsung Knox 3.x finden Sie in der Samsung Knox-Entwicklerdokumentation. Diese Version enthält auch Unterstützung für die neuen Samsung Knox-Namespaces. Weitere Informationen zu Änderungen an alten Samsung Knox-Namespaces finden Sie unter Änderungen an alten Samsung Knox-Namespaces.

> **Hinweis:**
>
> Secure Hub für Android unterstützt Samsung Knox 3.x nicht auf Geräten mit Android 5.

Secure Hub 19.3.5 bis 19.6.6

Diese Releases enthalten Leistungsverbesserungen und Bugfixes.

Secure Hub 19.3.0

Unterstützung für Samsung Knox Platform for Enterprise. Secure Hub für Android unterstützt Knox Platform for Enterprise (KPE) auf Android Enterprise-Geräten.

Secure Hub 19.2.0

Dieses Release enthält Leistungsverbesserungen und Bugfixes.

Secure Hub 19.1.5

Secure Hub für Android Enterprise unterstützt jetzt die folgenden Richtlinien:

- **WiFi-Geräterichtlinie.** Die Wi-Fi-Geräterichtlinie unterstützt jetzt Android Enterprise. Weitere Informationen zu dieser Richtlinie finden Sie unter Wi-Fi-Geräterichtlinie.
- **Benutzerdefinierte XML-Geräterichtlinie.** Die benutzerdefinierte XML-Geräterichtlinie unterstützt jetzt Android Enterprise. Weitere Informationen zu dieser Richtlinie finden Sie unter Benutzerdefinierte XML-Geräterichtlinie.
- **Dateirichtlinie.** Sie können Skriptdateien in Citrix Endpoint Management hinzufügen, um Funktionen auf Android Enterprise-Geräten auszuführen. Weitere Informationen zu dieser Richtlinie finden Sie unter Dateirichtlinie.

Secure Hub 19.1.0

Schriftarten, Farben und weitere Details in der Secure Hub-Benutzeroberfläche verbessert. Die visuelle Neugestaltung bietet eine reichere Benutzererfahrung und reflektiert die Markenästhetik der gesamten Suite mobiler Produktivitätsapps von Citrix.

Secure Hub 18.12.0

Dieses Release enthält Leistungsverbesserungen und Bugfixes.

Secure Hub 18.11.5

- **Einstellungen der Einschränkungsrichtlinie für Geräte für Android Enterprise:** Neue Einstellungen der Einschränkungsrichtlinie für Geräte ermöglichen Benutzern den Zugriff auf folgende Features auf Android Enterprise-Geräten: Statusleiste, Tastensperre für Sperrbildschirm, Kontoverwaltung, Standortfreigabe und Gerätebildschirm eingeschaltet lassen für Android Enterprise-Geräte. Weitere Informationen finden Sie unter Richtlinie für Geräteeinschränkungen.

Secure Hub 18.10.5 bis 18.11.0 beinhaltet Leistungsverbesserungen und Fehlerbehebungen.

Secure Hub 18.10.0

- **Unterstützung für den Samsung DeX-Modus:** Samsung DeX ermöglicht es Benutzern, KNOX-fähige Geräte an ein externes Display anzuschließen, um Anwendungen zu nutzen, Dokumente zu überprüfen und Videos auf einer PC-ähnlichen Oberfläche anzusehen. Informationen zu den Samsung DeX-Geräteanforderungen und zum Einrichten von Samsung DeX finden Sie unter How Samsung DeX works.

  Um die Features des Samsung DeX-Modus in Citrix Endpoint Management zu konfigurieren, aktualisieren Sie die Richtlinie für Geräteeinschränkungen für Samsung Knox. Weitere Informationen finden Sie unter **Samsung KNOX-Einstellungen** in der Richtlinie für Geräteeinschränkungen.

- **Unterstützung für Android SafetyNet:** Sie können Endpoint Management zur Verwendung des **Android SafetyNet**-Features konfigurieren, um die Kompatibilität und Sicherheit von Android-Geräten mit installiertem Secure Hub zu bewerten. Die Ergebnisse können genutzt werden, um automatisierte Aktionen auf den Geräten auszulösen. Weitere Informationen finden Sie unter Android SafetyNet.

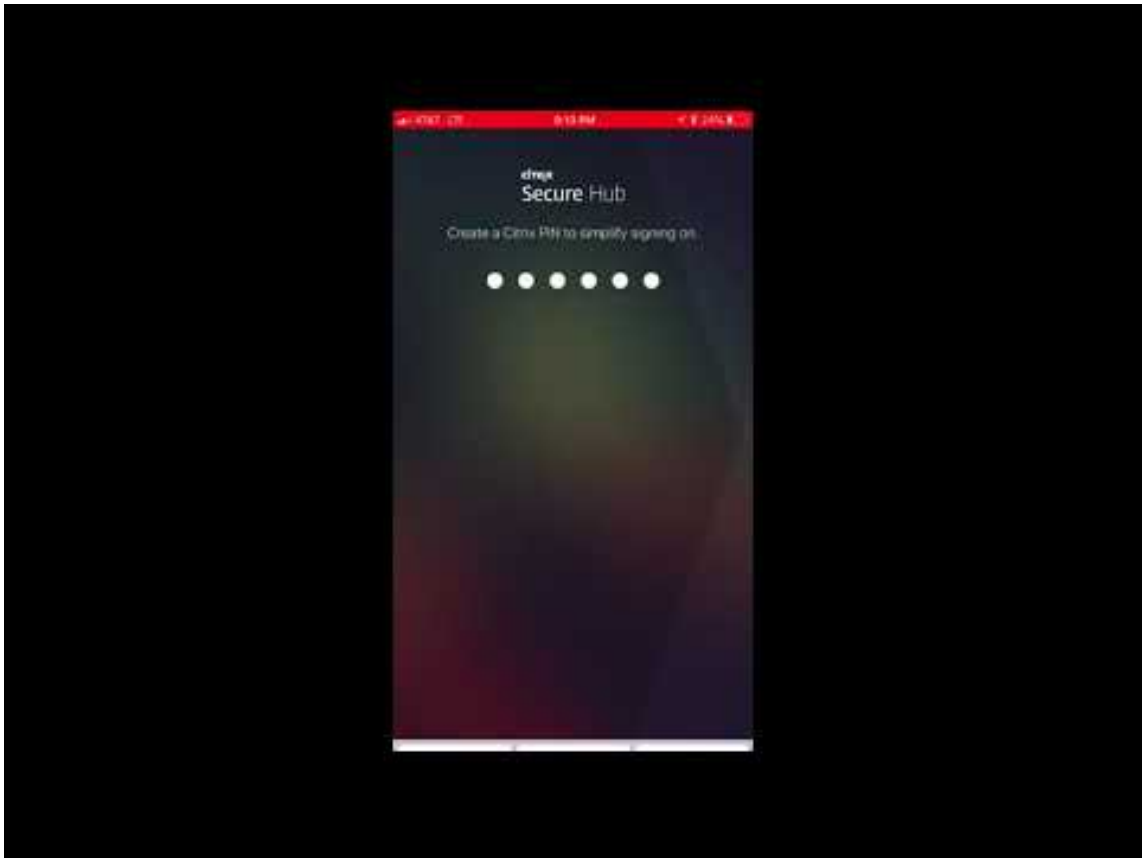
- **Verwendung der Kamera für Android Enterprise-Geräte verhindern:** Mit der neuen Einstellung **Verwenden der Kamera zulassen** für die Richtlinie für Geräteeinschränkungen können Sie verhindern, dass Benutzer die Kamera auf ihren Android Enterprise-Geräten verwenden. Weitere Informationen finden Sie unter Richtlinie für Geräteeinschränkungen.

Secure Hub 10.8.60 bis 18.9.0

Diese Releases enthalten Leistungsverbesserungen und Bugfixes.

Secure Hub 10.8.60

- Unterstützung für die polnische Sprache.
- Unterstützung für Android P.
- Unterstützung für die Verwendung von Workspace App Store.
  Der Secure Hub-Store wird beim Öffnen von Secure Hub nicht mehr angezeigt. Benutzer werden über die Schaltfläche **Apps hinzufügen** zum Workspace-App-Store geleitet. Das folgende Video zeigt, wie ein iOS-Gerät über die Citrix Workspace-App bei Citrix Endpoint Management registriert wird.



> Wichtig:
>
> Dieses Feature steht nur Neukunden zur Verfügung. Wir unterstützen derzeit keine Migration für bestehende Kunden.

Um dieses Feature zu nutzen, konfigurieren Sie Folgendes:

  - Aktivieren Sie die Richtlinien zur Kennwortzwischenspeicherung und Kennwortauthentifizierung. Weitere Informationen zum Konfigurieren dieser Richtlinien finden Sie unter Überblick über die MDX-Richtlinien für mobile Produktivitätsapps.

- Konfigurieren Sie die Active Directory-Authentifizierung als AD oder AD+Cert. Wir unterstützen diese beiden Modi. Weitere Informationen zum Konfigurieren der Authentifizierung finden Sie unter Authentifizierung mit Domäne oder mit Domäne und Sicherheitstoken.
- Workspace-Integration für Endpoint Management aktivieren. Weitere Informationen zur Workspaceintegration finden Sie unter Konfigurieren von Workspaces.

> **Wichtig:**
>
> Nachdem dieses Feature aktiviert wurde, erfolgt der Single Sign-On für Citrix Files über Workspace und nicht über Endpoint Management (früher XenMobile). Es wird empfohlen, die Citrix Files-Integration in der Endpoint Management-Konsole zu deaktivieren, bevor Sie die Workspaceintegration aktivieren.

Secure Hub 10.8.55

- Die Möglichkeit, einen Benutzernamen und ein Kennwort für das Google Zero-Touch- und Samsung Knox Mobile Environment (KME)-Portal mit der Konfigurations-JSON zu übergeben. Einzelheiten finden Sie unter Samsung Knox-Massenregistrierung.
- Wenn Sie Zertifikatpinning aktivieren, können Benutzer sich nicht mit einem selbstsignierten Zertifikat bei Endpoint Management anmelden. Wenn Benutzer versuchen, sich mit einem selbstsignierten Zertifikat bei Endpoint Management anzumelden, werden sie gewarnt, dass das Zertifikat nicht vertrauenswürdig ist.

Secure Hub 10.8.25: Secure Hub für Android unterstützt Android P-Geräte.

> **Hinweis:**
>
> Vor dem Upgrade auf die Android P-Plattform: Stellen Sie sicher, dass Ihre Serverinfrastruktur mit Sicherheitszertifikaten kompatibel ist, die über einen übereinstimmenden Hostnamen in der subjectAltName-Erweiterung (SAN) verfügen. Zum Überprüfen eines Hostnamens muss der Server ein Zertifikat mit einem passenden SAN bereitstellen. Zertifikate, die keinen SAN enthalten, der mit dem Hostnamen übereinstimmt, sind nicht länger vertrauenswürdig. Weitere Informationen finden Sie in der Android-Entwicklerdokumentation.

Secure Hub für iOS-Update am 19. März 2018: Secure Hub Version 10.8.6 für iOS ist verfügbar, um ein Problem mit der VPP-App-Richtlinie zu beheben. Weitere Informationen finden Sie in diesem Citrix Knowledge Center-Artikel.

Secure Hub 10.8.5: Unterstützung für Secure Hub für Android für den COSU-Modus für Android Work (Android for Work). Weitere Informationen finden Sie in der Dokumentation zu Citrix Endpoint Management.

Verwalten von Secure Hub

Sie führen die meisten Verwaltungsaufgaben für Secure Hub bei der Erstkonfiguration von Endpoint Management aus. Um Secure Hub unter iOS und Android zur Verfügung zu stellen, laden Sie Secure Hub in den iOS App Store und den Google Play Store hoch.

Secure Hub aktualisiert auch die meisten MDX-Richtlinien, die in Endpoint Management für die installierten Apps gespeichert sind, wenn sich die Citrix Gateway-Sitzung eines Benutzers nach der Authentifizierung mit Citrix Gateway verlängert.

> **Wichtig:**
>
> Bei Änderungen an einer dieser Richtlinien muss der Benutzer die App löschen und neu installieren, damit die aktualisierte Richtlinie angewendet wird: Sicherheitsgruppe, Verschlüsselung aktivieren und Secure Mail Exchange Server.

Citrix-PIN

Sie können Secure Hub zur Verwendung der Citrix PIN konfigurieren. Die Citrix PIN ist ein Sicherheitsfeature, das in der Endpoint Management-Konsole unter **Einstellungen** > **Clienteigenschaften** aktiviert wird. Durch diese Einstellung müssen sich Benutzer von Mobilgeräten bei Secure Hub anmelden und alle mit MDX umschlossenen Apps über eine persönliche Identifikationsnummer (PIN) aktivieren.

Die Citrix PIN vereinfacht die Benutzerauthentifizierung beim Anmelden an den gesicherten umschlossenen Apps. Benutzer müssen nicht wiederholt die Anmeldeinformationen eingeben, wie ihren Active Directory-Benutzernamen und ihr Kennwort.

Bei der ersten Anmeldung bei Secure Hub müssen die Benutzer ihren Active Directory-Benutzernamen und das Kennwort eingeben. Während der Anmeldung speichert Secure Hub die Active Directory-Anmeldeinformationen oder ein Clientzertifikat auf dem Benutzergerät und fordert die Benutzer dann zur Eingabe einer PIN auf. Wenn Benutzer sich erneut anmeldet, geben sie die PIN ein und erhalten bis zum Ablauf des nächsten Leerlauftimeouts für die aktive Sitzung sicheren Zugriff auf Citrix Apps und den Store. In den zugehörigen Clienteigenschaften können Sie mit der PIN Geheimnisse verschlüsseln und den Passcodetyp sowie Stärke und Länge der PIN festlegen. Einzelheiten finden Sie unter Clienteigenschaften.

Bei aktivierter Authentifizierung per Fingerabdruck (Touch ID) können Benutzer sich per Fingerabdruck anmelden, wenn eine Offlineauthentifizierung aufgrund von Inaktivität in der App erforderlich ist. Bei der Erstanmeldung bei Secure Hub, beim Neustart des Geräts und nach Ablauf des Inaktivitätstimers müssen Benutzer jedoch immer noch eine PIN eingeben. Informationen zum Aktivieren der Authentifizierung per Fingerabdruck finden Sie unter Authentifizierung per Touch ID bzw. Fingerabdruck.

Zertifikatpinning

Secure Hub für iOS und Android unterstützt SSL-Zertifikatpinning. Dieses Feature stellt sicher, dass das Zertifikat Ihrer Firma für die Kommunikation zwischen Clients und Endpoint Management verwendet wird. Auf diese Weise werden Verbindungen von Citrix Clients mit Endpoint Management vermieden, wenn die Installation eines Stammzertifikats auf dem Gerät die SSL-Sitzung gefährdet. Wenn Secure Hub Änderungen am öffentlichen Schlüssel des Servers erkennt, wird die Verbindung verweigert.

Ab Android N lässt das Betriebssystem keine vom Benutzer hinzugefügten Zertifizierungsstellen (ZS) mehr zu. Citrix empfiehlt stattdessen die Verwendung einer öffentlichen Stamm-ZS.

Nach einem Upgrade auf Android N können bei Verwendung privater oder selbstsignierter ZS Probleme auftreten. Verbindungen werden auf Android N-Geräten in folgenden Situationen getrennt:

- Private oder selbstsignierte ZS und die Option für erforderliche vertrauenswürdige ZS für Endpoint Management ist auf **EIN** festgelegt. Weitere Informationen finden Sie unter Geräteverwaltung.
- Private oder selbstsignierte ZS und des Endpoint Management AutoDiscovery Service (ADS) sind nicht erreichbar. Aus Sicherheitsgründen wird die Option "Required Trusted CA"**aktiviert**, wenn ADS nicht erreichbar ist, selbst wenn sie zuvor auf **OFF** festgelegt wurde.

Bevor Sie Geräte registrieren oder Secure Hub aktualisieren, sollten Sie das Zertifikatpinning aktivieren. Die Option ist standardmäßig **Aus** und wird von ADS verwaltet. Wenn Sie Zertifikatpinning aktivieren, können Benutzer sich nicht mit einem selbstsignierten Zertifikat bei Endpoint Management anmelden. Wenn Benutzer versuchen, sich mit einem selbstsignierten Zertifikat anzumelden, werden sie gewarnt, dass das Zertifikat nicht vertrauenswürdig ist. Die Registrierung schlägt fehl, wenn Benutzer das Zertifikat nicht akzeptieren.

Für die Verwendung des Zertifikatpinnings fordern Sie bei Citrix das Hochladen von Zertifikaten auf den Citrix ADS-Server an. Öffnen Sie im Citrix Support-Portal einen Supportfall. Stellen Sie sicher, dass Sie den privaten Schlüssel nicht an Citrix senden. Geben Sie dann die folgenden Informationen an:

- Die Domäne mit den Konten, mit denen Benutzer Geräte registrieren.
- Der vollqualifizierte Domänenname (FQDN) für Endpoint Management.
- Der Name für die Endpoint Management-Instanz. Standardmäßig lautet der Instanzname (Groß-/Kleinschreibung beachten) zdm.
- Benutzer-ID-Typ (entweder UPN oder E-Mail). Standardeinstellung ist UPN.
- Der für die iOS-Registrierung verwendete Port, wenn Sie die standardmäßige Portnummer 8443 geändert haben.
- Der Port, über den Endpoint Management Verbindungen annimmt, wenn Sie die standardmäßige Portnummer 443 geändert haben.

- Vollständige URL von Citrix Gateway.
- E-Mail-Adresse des Administrators (optional).
- PEM-Zertifikate, die der Domäne hinzugefügt werden sollen, müssen öffentliche Zertifikate und dürfen kein privater Schlüssel sein.
- Verfahren mit einem ggf. vorhandenen Serverzertifikat: Ob dieses sofort entfernt werden soll (da es kompromittiert ist) oder bis zum Ablaufen weiterverwendet werden soll.

Ihr Supportfall wird aktualisiert, sobald Ihre Daten und das Zertifikat den Citrix Servern hinzugefügt wurden.

Zertifikat und Authentifizierung mit Einmalkennwort

Sie können Citrix ADC so konfigurieren, dass die Authentifizierung in Secure Hub mit einem Zertifikat und einem Sicherheitstoken, der als Einmalkennwort dient, ausgeführt wird. Diese Konfiguration bietet hohe Sicherheit, die keine Active Directory-Spur auf Benutzergeräten hinterlässt.

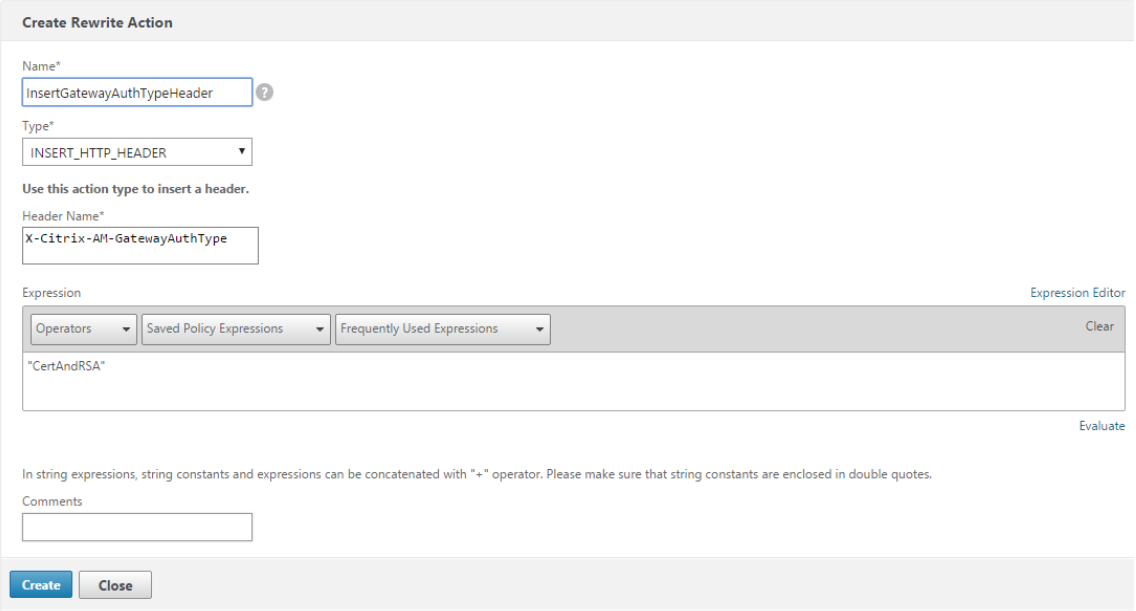
Damit Secure Hub die Authentifizierung per Zertifikat und Einmalkennwort verwendet, fügen Sie eine Rewrite-Aktion und eine Rewrite-Richtlinie in Citrix ADC hinzu, sodass ein benutzerdefinierter Antwortheader der Form **X-Citrix-AM-GatewayAuthType: CertAndRSA** eingefügt wird, um den Citrix Gateway-Anmeldetyp anzugeben.

Normalerweise verwendet Secure Hub den in der Endpoint Management-Konsole konfigurierten Citrix Gateway-Anmeldetyp. Diese Informationen stehen Secure Hub jedoch erst dann zur Verfügung, wenn Secure Hub die erste Anmeldung abgeschlossen hat Daher ist ein benutzerdefinierter Header erforderlich.

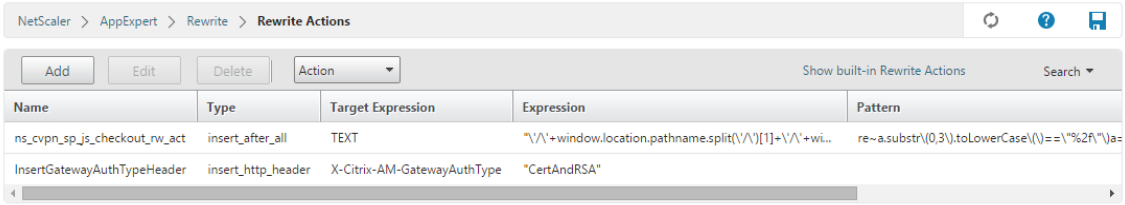
> **Hinweis:**
>
> Wenn für Endpoint Management und Citrix ADC unterschiedliche Anmeldetypen festgelegt sind, hat die Konfiguration von Citrix ADC Vorrang. Weitere Informationen finden Sie unter Citrix Gateway und Endpoint Management.

1. Navigieren Sie in Citrix ADC zu **Configuration > AppExpert > Rewrite > Actions**.
2. Klicken Sie auf **Hinzufügen**.

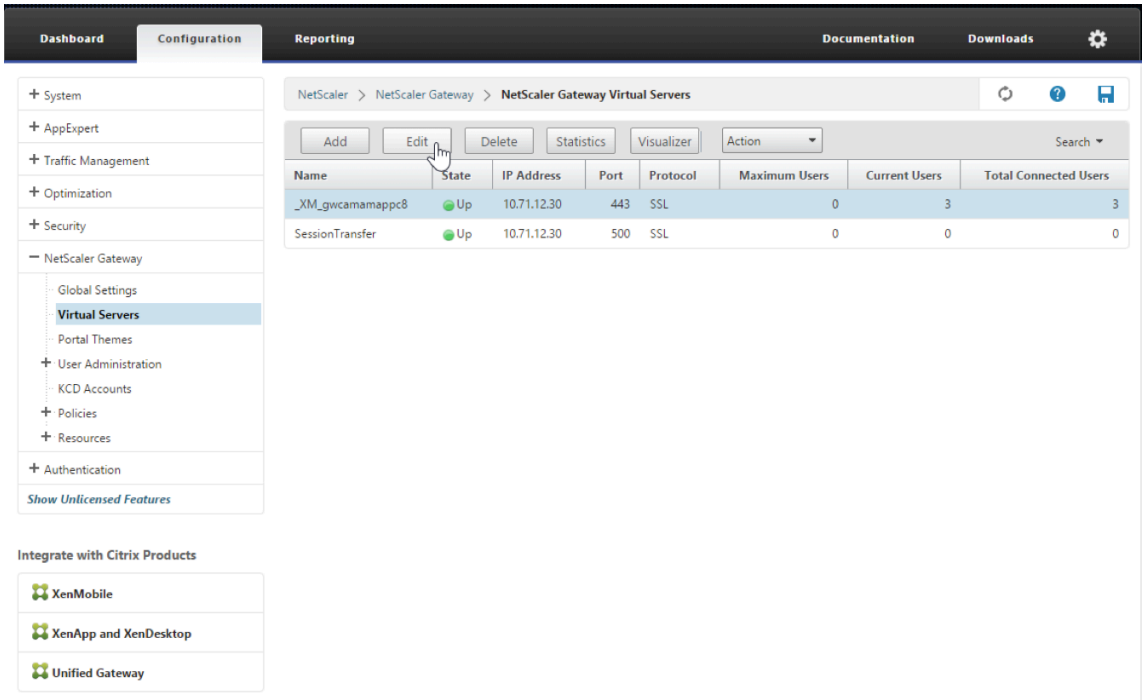
   Der Bildschirm **Create Rewrite Action** wird angezeigt.
3. Nehmen Sie Eingaben in den Feldern vor (siehe Abbildung unten) und klicken Sie auf **Create**.



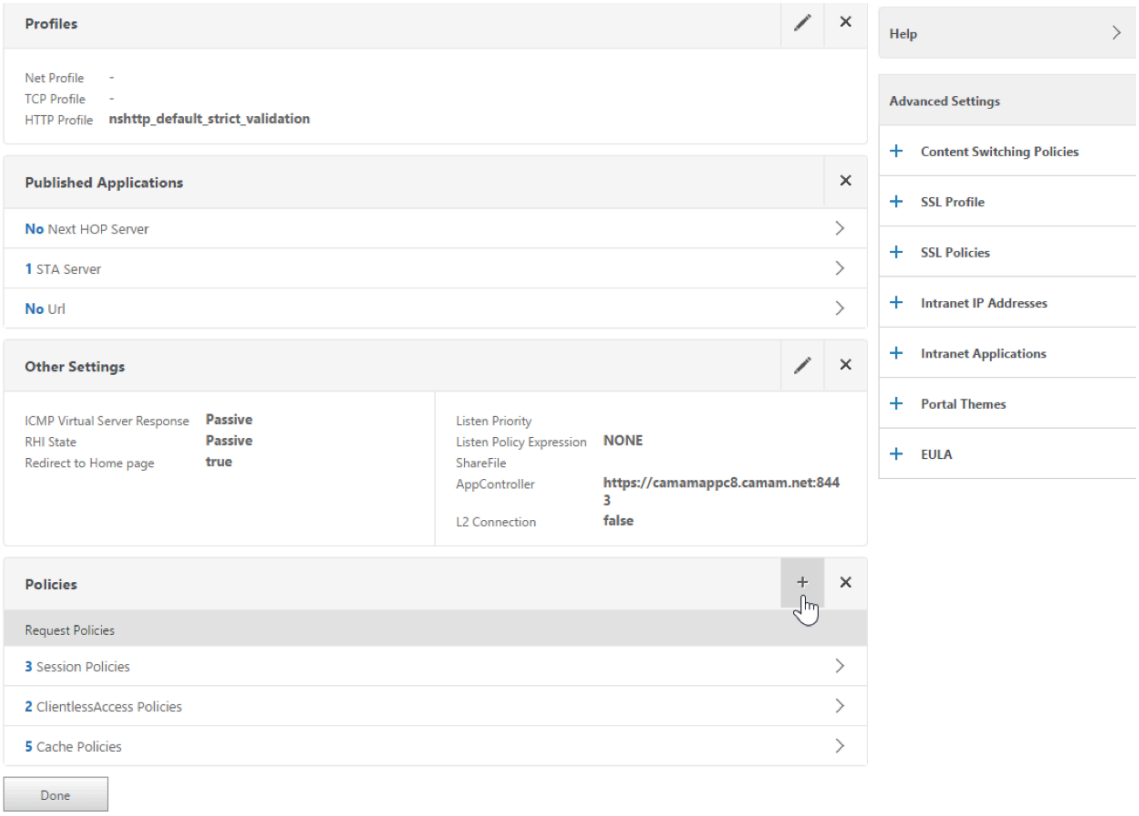
Das folgende Ergebnis wird auf dem Hauptbildschirm **Rewrite Actions** angezeigt.



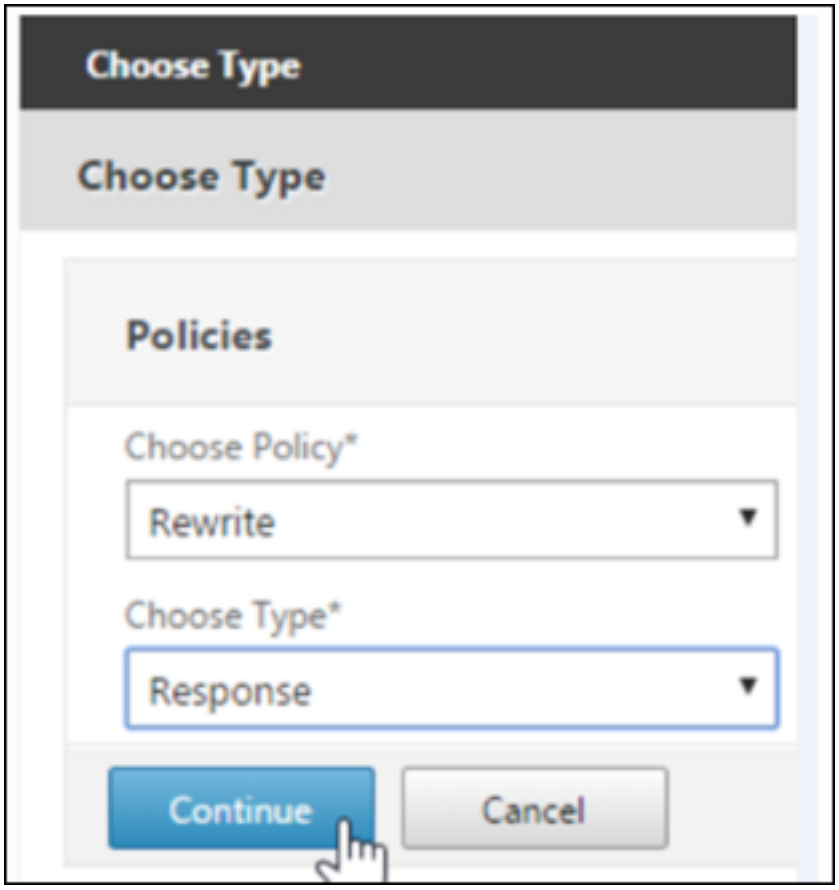
4. Binden Sie die Rewrite-Aktion an den virtuellen Server als Rewrite-Richtlinie. Gehen Sie zu **Configuration > NetScaler Gateway > Virtual Servers** und wählen Sie den virtuellen Server.



5. Klicken Sie auf **Bearbeiten**.
6. Navigieren Sie auf der Seite **Virtual Servers configuration** nach unten zu **Policies**.
7. Klicken Sie auf **+**, um eine Richtlinie hinzuzufügen.

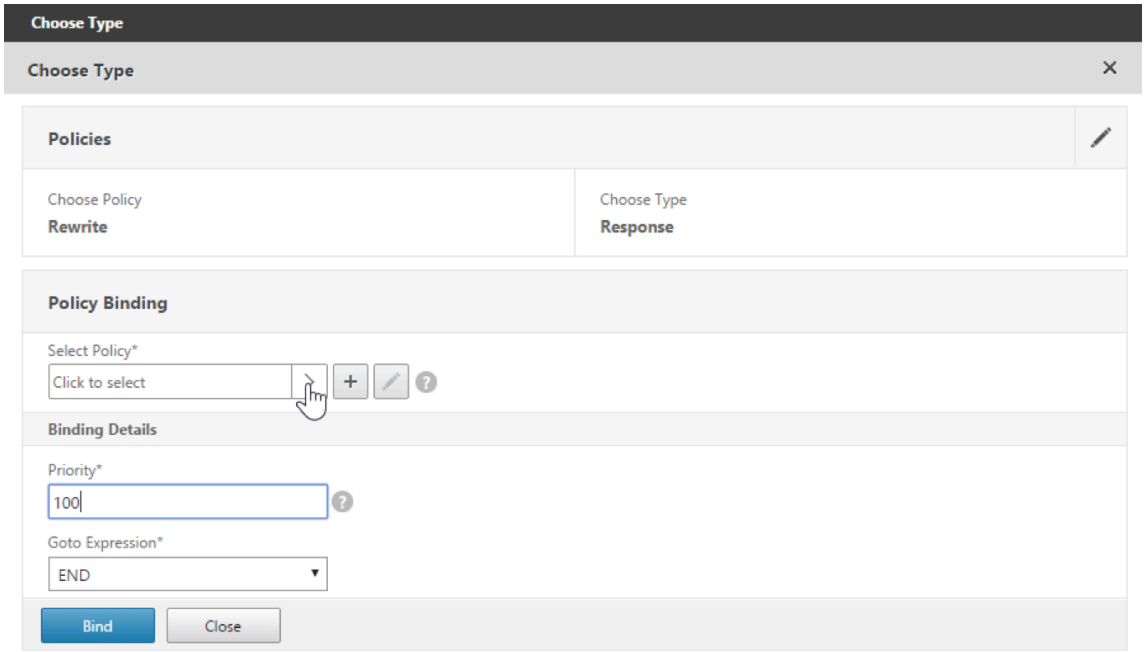


8. Geben Sie **Rewrite** im Feld **Choose Policy** ein.
9. Wählen Sie **Response** im Feld **Choose Type** aus.



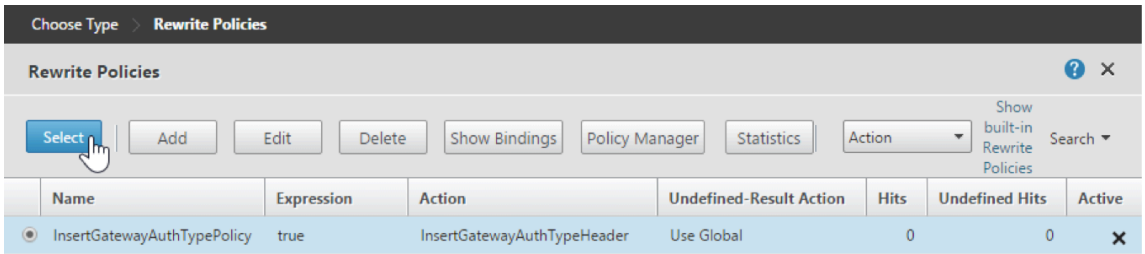
10. Klicken Sie auf **Weiter**.

    Der Abschnitt **Policy Binding** wird erweitert.

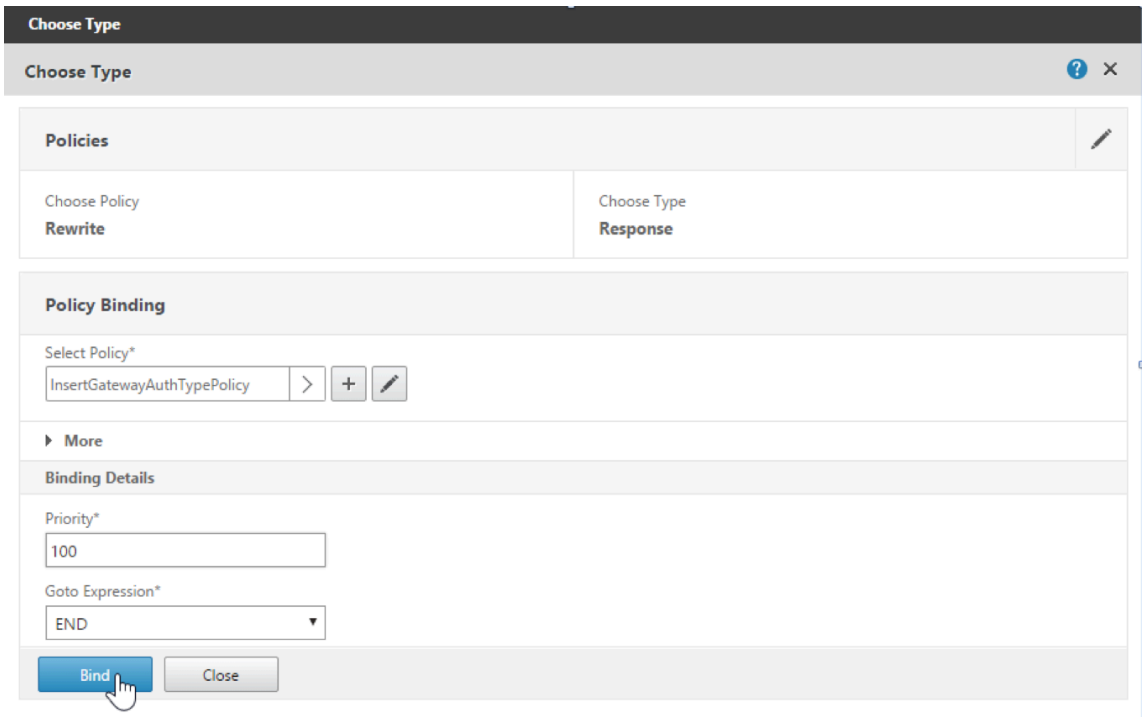


11. Klicken Sie auf **Select Policy**.

    Ein Bildschirm mit den verfügbaren Richtlinien wird angezeigt.

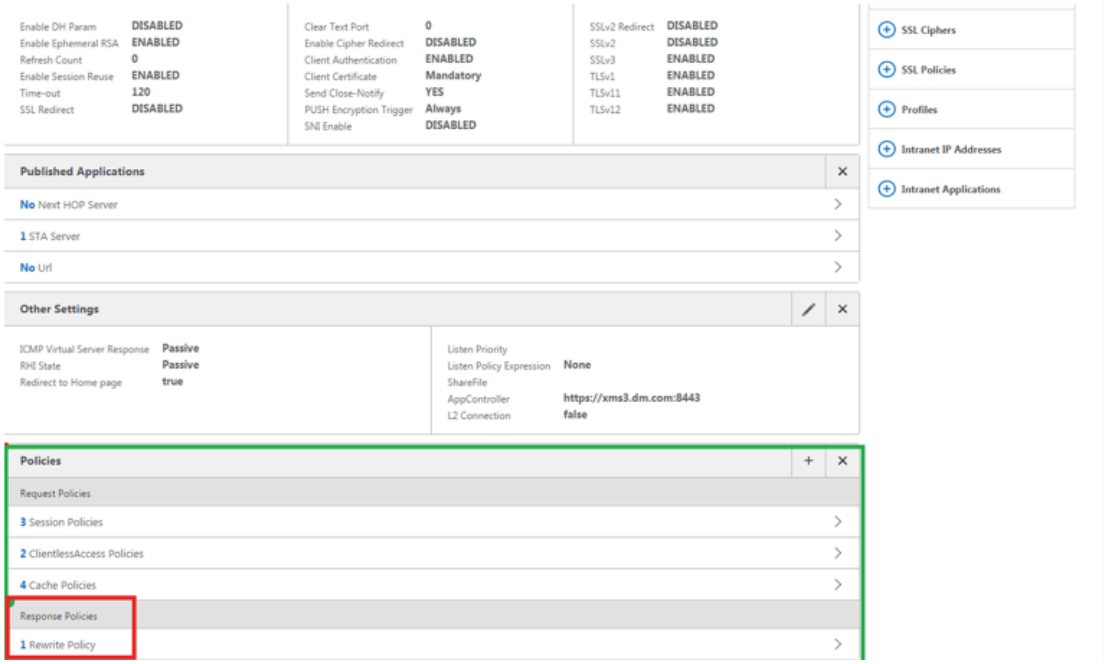


12. Klicken Sie auf die Zeile der Richtlinie, die Sie erstellt haben, und klicken Sie dann auf **Select**. Der Bildschirm **Policy Binding** wird wieder angezeigt. Er enthält die ausgewählte Richtlinie.

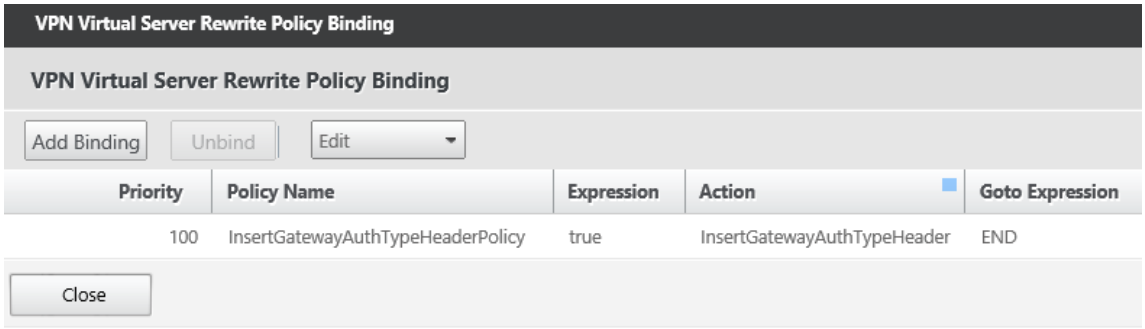


13. Klicken Sie auf **Bind**.

    Wenn die Bindung erfolgreich ist, wird der Konfigurationsbildschirm mit der vollständigen Rewrite-Richtlinie angezeigt.



14. Zum Anzeigen der Richtliniendetails klicken Sie auf **Rewrite Policy**.



Portanforderungen für die ADS-Verbindung bei Android-Geräten Die Portkonfiguration gewährleistet, dass Android-Geräte über Secure Hub innerhalb des Unternehmensnetzwerks auf den Citrix ADS zugreifen können. Der Zugriff auf ADS ist zum Herunterladen von Sicherheitsupdates wichtig, die über diesen Dienst zur Verfügung gestellt werden. ADS-Verbindungen sind eventuell nicht mit dem vorhandenen Proxyserver kompatibel. Lassen Sie in diesem Szenario zu, dass die ADS-Verbindung den Proxy-Server umgeht.

> **Wichtig:**
>
> Für Secure Hub für Android und iOS müssen Sie auf Android-Geräten den Zugriff auf ADS zulassen. Weitere Informationen finden Sie unter Portanforderungen in der Dokumentation zu Citrix Endpoint Management. Diese Verbindung erfolgt über den ausgehenden Port 443. Ihre vorhandene Umgebung lässt diesen Zugriff sehr wahrscheinlich bereits zu. Kunden, die diese Verbindung nicht gewährleisten können, wird von einem Upgrade auf Secure Hub 10.2 abgeraten. Wenn Sie Fragen haben, wenden Sie sich an den Citrix Support.

Voraussetzungen:

- Sammeln Sie die Endpoint Management- und Citrix ADC-Zertifikate. Die Zertifikate müssen im PEM-Format vorliegen und öffentlich sein, d. h. keine privaten Schlüssel sind zulässig.
- Öffnen Sie einen Supportfall beim Citrix Support, um Zertifikatpinning zu aktivieren. Bei diesem Prozess werden Ihre Zertifikate angefordert.

Die neuen Verbesserungen beim Zertifikatpinning erfordern, dass Geräte vor der Registrierung eine Verbindung mit dem ADS herstellen. Damit wird sichergestellt, dass Secure Hub über die aktuellen Sicherheitsinformationen für die Umgebung verfügt, in der das Gerät registriert wird. Kann ein Gerät den ADS nicht erreichen, lässt Secure Hub die Registrierung nicht zu. Daher ist die Aktivierung des Zugriffs auf den ADS im internen Netzwerk erforderlich, damit Geräte registriert werden können.

Damit der Zugriff auf ADS für Secure Hub für Android möglich ist, öffnen Sie Port 443 für die folgenden IP-Adressen und FQDNs:

FQDN	IP-Adresse	Port	IP- und Port-Nutzung
`discovery.mdm.zenprise.com`	52.5.138.94	443	Secure Hub - ADS-Kommunikation
`discovery.mdm.zenprise.com`	52.1.30.122	443	Secure Hub - ADS-Kommunikation
`ads.xm.cloud.com`: Secure Hub Version 10.6.15 und höher verwendet `ads.xm.cloud.com`.	34.194.83.188	443	Secure Hub - ADS-Kommunikation
`ads.xm.cloud.com`: Secure Hub Version 10.6.15 und höher verwendet `ads.xm.cloud.com`.	34.193.202.23	443	Secure Hub - ADS-Kommunikation

Wenn Zertifikatpinning aktiviert ist:

- Secure Hub pinnt das Unternehmenszertifikat während der Geräteregistrierung.
- Während des Upgrades verwirft Secure Hub alle aktuell gepinnten Zertifikate und pinnt das Serverzertifikat auf die erste Verbindung bei registrierten Benutzern.

  > **Hinweis:**
  >
  > Wenn Sie das Zertifikatpinning nach einem Upgrade aktivieren, müssen Benutzer sich erneut registrieren.

- Die Erneuerung des Zertifikats erfordert keine erneute Registrierung, sofern der öffentliche Schlüssel des Zertifikats sich nicht geändert hat.

Zertifikatpinning unterstützt untergeordnete Zertifikate, aber keine Zwischen- oder Ausstellerzertifikate. Zertifikatpinning gilt für Citrix Server, z. B. Endpoint Management und Citrix Gateway, jedoch nicht für die Server Dritter.

Deaktivieren der Option “Konto löschen”

In Umgebungen mit aktiviertem Autodiscovery-Dienst (ADS) können Sie die Option **Konto löschen** in Secure Hub deaktivieren.

Mit den folgenden Schritten deaktivieren Sie die Option **Konto löschen**:

1. Konfigurieren Sie ADS für Ihre Domäne.
2. Öffnen Sie in Citrix Endpoint Management die **Informationen zum Autodiscoverydienst** und legen Sie für `displayReenrollLink` den Wert **False** fest.
   Der Standardwert ist **True**.
3. Wenn Ihr Gerät im MDM+MAM-Modus (ENT) registriert ist, müssen Sie sich ab- und wieder anmelden, damit die Änderungen wirksam werden.
   Wenn Ihr Gerät in einem anderen Modus registriert ist, müssen Sie es erneut registrieren.

Verwenden von Secure Hub

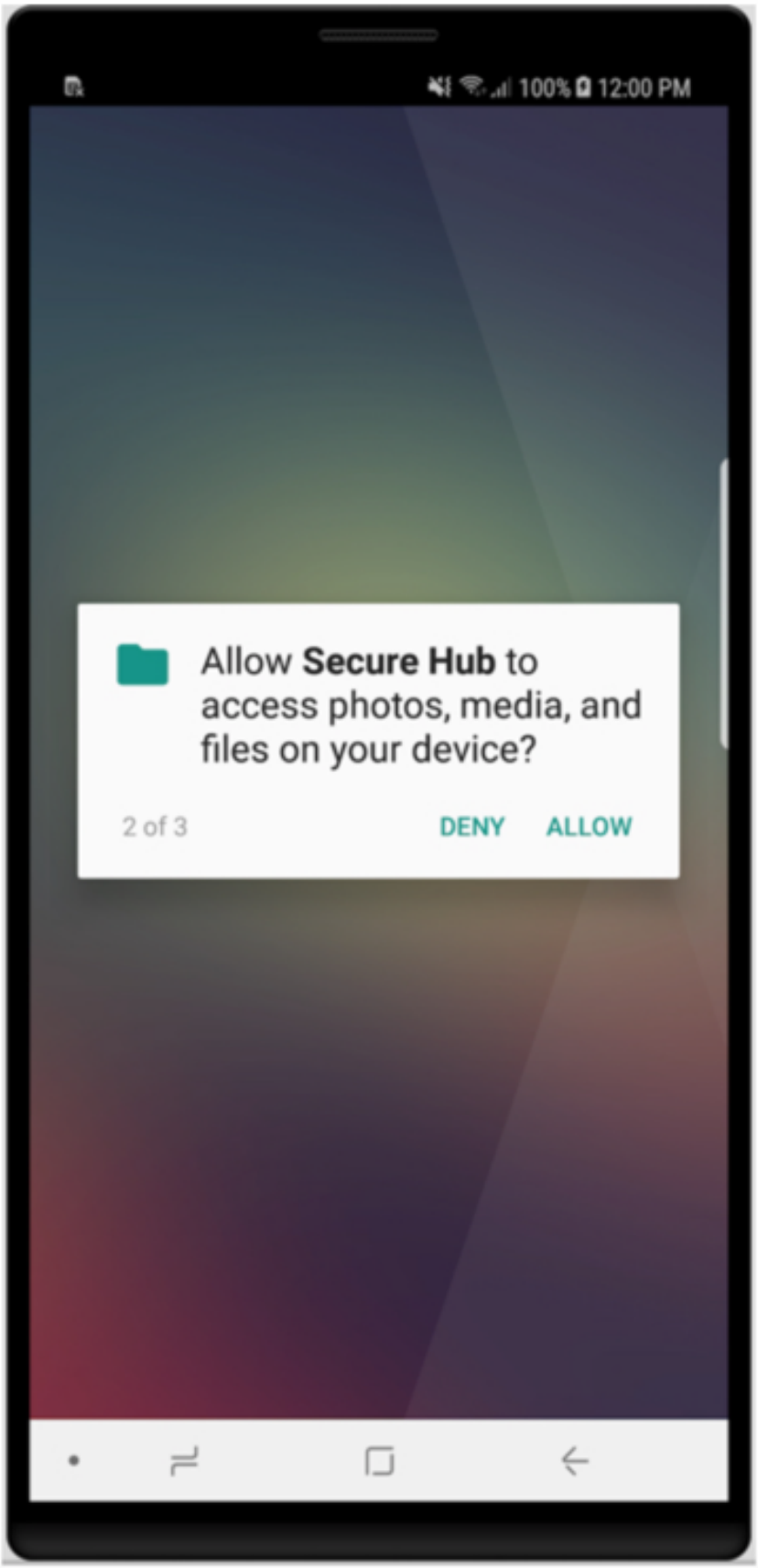
Zu Beginn laden Benutzer Secure Hub aus dem App-Store von Apple oder Android auf ihr Gerät herunter.

Wenn Secure Hub geöffnet wird, geben die Benutzer ihre von ihrem Unternehmen erhaltenen Anmeldeinformationen ein, um ihr Gerät bei Secure Hub zu registrieren. Weitere Informationen zur Geräteregistrierung finden Sie unter Benutzerkonten, Rollen und Registrierung.

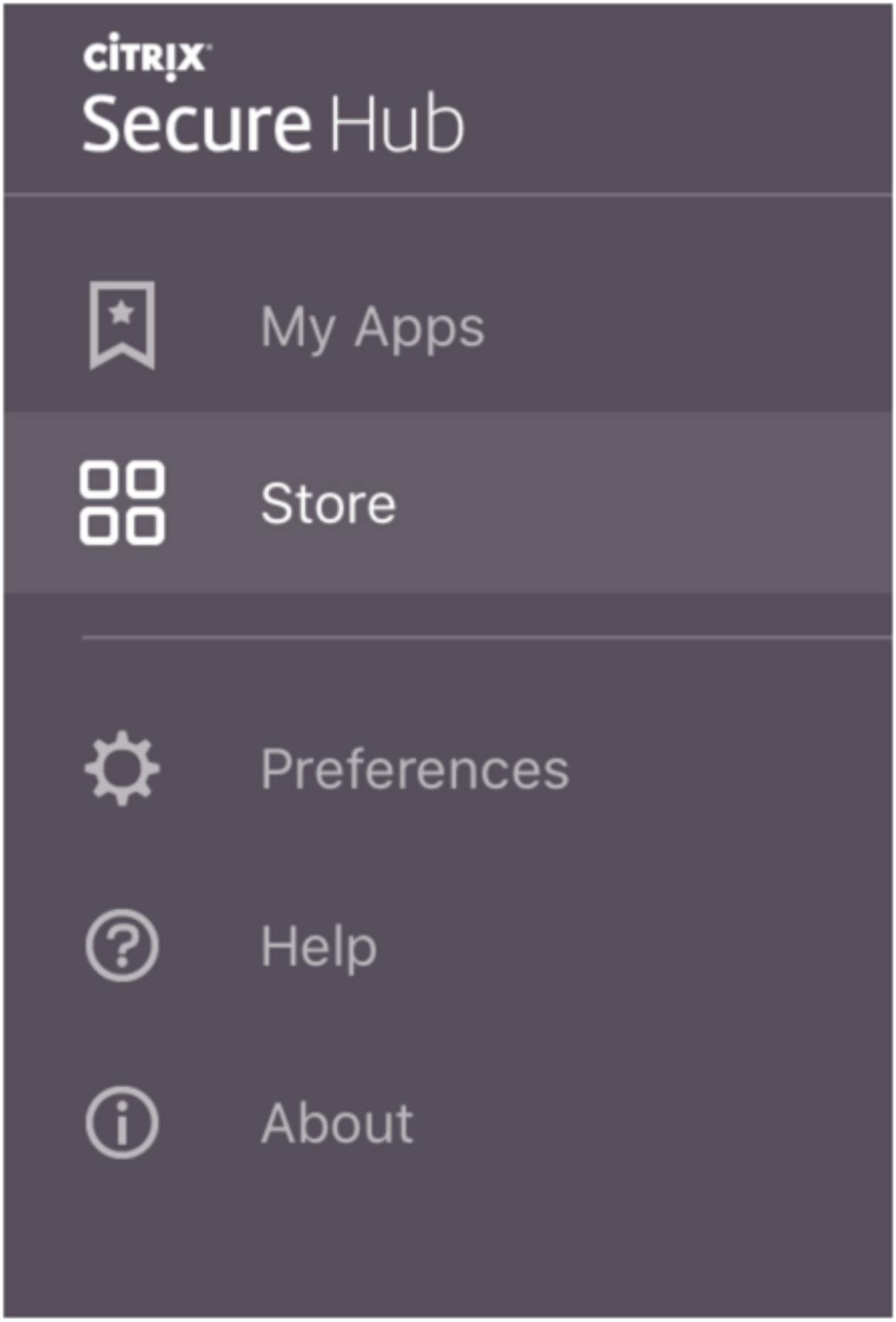
Secure Hub für Android fragt bei der Erstinstallation und Registrierung, ob Sie Secure Hub den Zugriff auf Fotos, Medien und Dateien auf Ihrem Gerät erlauben wollen.

Diese Meldung stammt vom Betriebssystem Android und nicht von Citrix. Wenn Sie auf **Zulassen** tippen, sehen Citrix und die Administratoren von Secure Hub Ihre persönlichen Daten zu keinem Zeitpunkt. Wenn Sie jedoch eine Remotesupportsitzung mit Ihrem Administrator durchführen, kann der Administrator Ihre persönlichen Dateien innerhalb der Sitzung anzeigen.

Nach der Registrierung sehen Benutzer die Apps und Desktops, die Sie ihnen auf der Registerkarte **Eigene Apps** bereitgestellt haben. Benutzer können weitere Apps aus dem Store hinzufügen. Der Store-Link findet sich auf Telefonen unter dem Symbol **Einstellungen** in der oberen linken Ecke.



Auf Tablets gibt es eine separate Registerkarte für den Store.



Wenn Benutzer mit iPhones mit iOS 9 oder höher mobile Produktivitätsapps aus dem Shop installieren, sehen sie eine Meldung. Die Meldung besagt, dass dem Unternehmensentwickler Citrix auf diesem iPhone nicht vertraut wird. Die Meldung weist darauf hin, dass die App erst dann für die Nutzung verfügbar ist, wenn dem Entwickler vertraut wird. Die Benutzer werden dann von Secure Hub aufgefordert, eine Anleitung zum Herstellen einer Vertrauensstellung für Citrix-Unternehmensapps für ihr iPhone aufzurufen.

Automatische Registrierung bei Secure Mail

Für Nur-MAM-Bereitstellungen können Sie Endpoint Management so konfigurieren, dass Benutzer, die sich mit einem iOS- oder Android-Gerät bei Secure Hub mit E-Mail-Anmeldeinformationen registrieren, automatisch bei Secure Mail registriert werden. Die Benutzer müssen für die Registrierung bei Secure Mail keine weiteren Informationen eingeben und keine zusätzlichen Schritte ausführen.

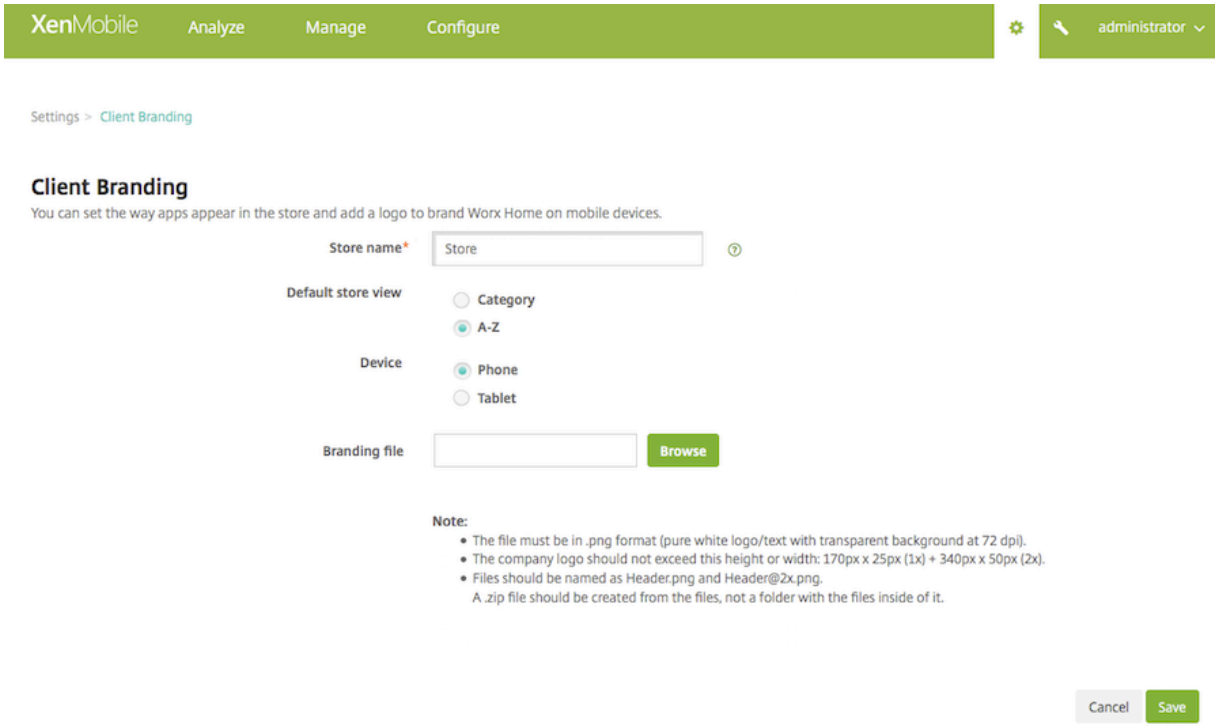
Bei der ersten Verwendung von Secure Mail werden die E-Mail-Adresse des Benutzers, die Domäne und die Benutzer-ID von Secure Hub abgerufen. Secure Mail verwendet die E-Mail-Adresse für AutoDiscovery. Der Exchange Server wird anhand von Domäne und Benutzer-ID gesucht, sodass eine automatische Authentifizierung des Benutzers in Secure Mail ermöglicht wird. Der Benutzer wird zur Eingabe des Kennworts aufgefordert, wenn die Richtlinie nicht auf Kennwort-Passthrough festgelegt ist. Der Benutzer muss jedoch keine weiteren Informationen eingeben.

Erstellen Sie zur Nutzung dieses Features drei Eigenschaften:

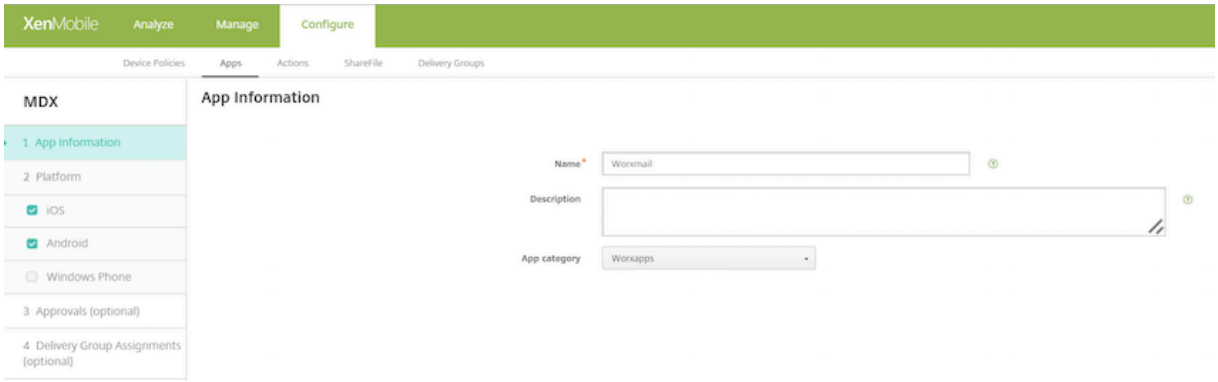
- Die Servereigenschaft MAM_MACRO_SUPPORT. Weitere Informationen finden Sie unter Servereigenschaften.
- Die Clienteigenschaften ENABLE_CREDENTIAL_STORE und SEND_LDAP_ATTRIBUTES. Weitere Informationen finden Sie unter Clienteigenschaften.

Benutzerdefinierter Store

Wenn Sie den Store anpassen möchten, gehen Sie zu **Einstellungen > Clientbranding**. Sie können dann den Namen ändern, ein Logo hinzufügen und festlegen, wie Anwendungen angezeigt werden.



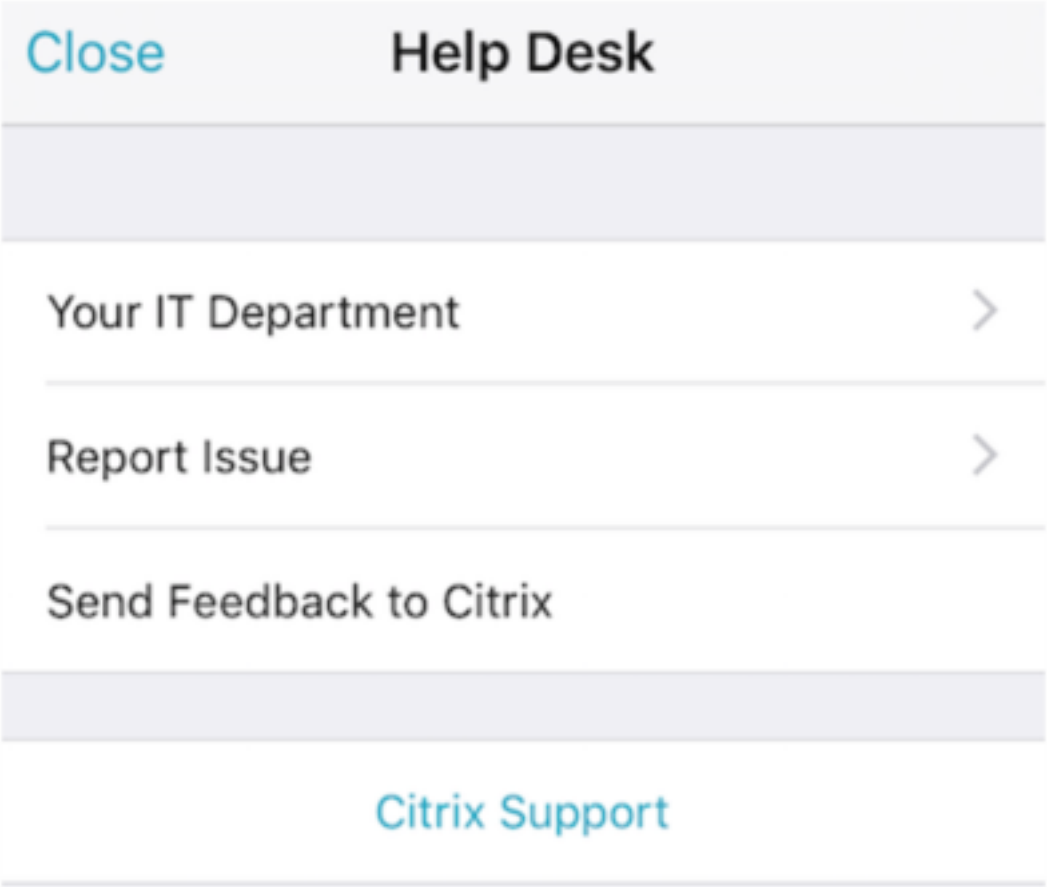
Sie können App-Beschreibungen in der Endpoint Management-Konsole bearbeiten. Klicken Sie auf **Konfigurieren** und auf **Apps**. Wählen Sie die App in der Tabelle aus und klicken Sie auf **Bearbeiten**. Wählen Sie die Plattformen aus, für die Sie die Beschreibung bearbeiten möchten, und geben Sie Text in das Feld **Beschreibung** ein.



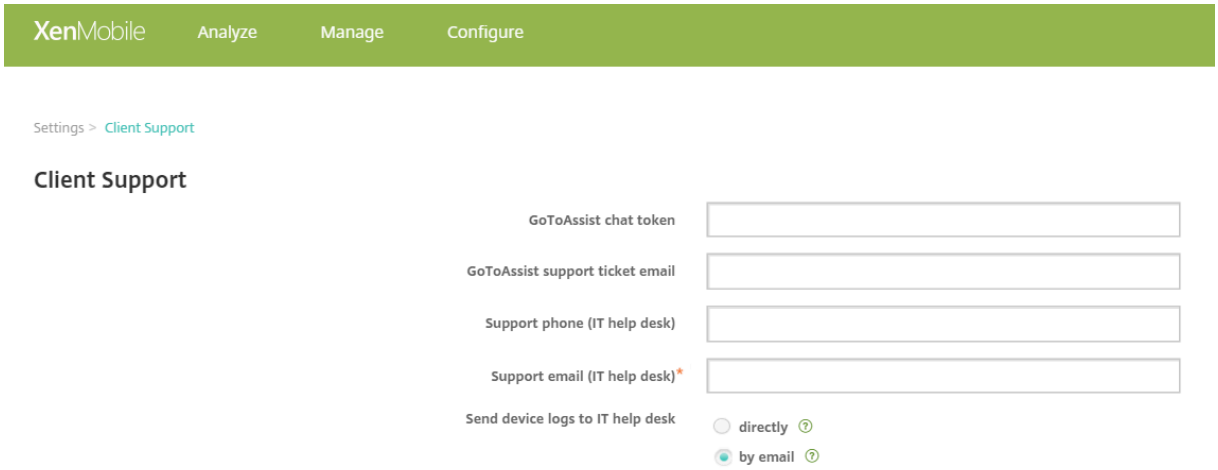
Im Store können Benutzer nur die Apps und Desktops durchsuchen, die Sie in Endpoint Management konfiguriert und gesichert haben. Zum Hinzufügen der App tippen Benutzer auf **Details** und dann auf **Hinzufügen**.

Konfigurierte Hilfeoptionen

Secure Hub bietet Benutzern ebenfalls verschiedene Wege, um Hilfe zu erhalten. Auf Tablets werden durch Antippen des Fragezeichens oben rechts die Hilfeoptionen aufgerufen. Auf Telefonen tippen Benutzer oben links auf das Symbol für Einstellungen und dann auf **Hilfe**.



Ihre IT-Abteilung: Die Telefonnummer und E-Mail-Adresse des Helpdesks Ihrer Firma. Sie geben die Telefonnummern und E-Mail-Adressen in der Endpoint Management-Konsole ein. Klicken Sie oben rechts auf das Zahnradsymbol. Die Seite **Einstellungen** wird angezeigt. Klicken Sie auf **Mehr** und dann auf **Clientsupport**. Der Bildschirm zum Eingeben der Informationen wird angezeigt.



Problem melden: Eine Liste der Apps. Benutzer wählen die App, die das Problem aufweist. Secure

Hub erstellt automatisch Protokolle und öffnet dann in Secure Mail eine Nachricht, an die die Protokolle als ZIP-Datei angefügt sind. Benutzer fügen Betreffzeilen und Problembeschreibungen hinzu. Sie können auch einen Screenshot anfügen.

Feedback an Citrix senden: In Secure Mail wird eine Nachricht an den Citrix Support geöffnet. Der Benutzer kann Verbesserungsvorschläge für Secure Mail eingeben. Wenn Secure Mail nicht auf dem Gerät installiert ist, wird das native E-Mail-Programm geöffnet.

Benutzer können auch auf **Citrix Support** tippen. Damit wird das Citrix Knowledge Center geöffnet. Dort können sie nach Supportartikeln für alle Citrix Produkte suchen.

Unter **Einstellungen** werden Benutzern Informationen über ihre Konten und Geräte angezeigt.

Standort-/Ortungsrichtlinien

Secure Hub bietet auch Geolocation- und Geotrackingrichtlinien, mit denen Sie bei Bedarf sicherstellen können, dass Geräte des Unternehmens einen bestimmten geografischen Bereich nicht verlassen. Weitere Informationen finden Sie unter Standortrichtlinie für Geräte.

Absturzerfassung und -analyse

Die von Secure Hub automatisch gesammelten und analysierten Fehlerinformationen ermöglichen Ihnen das Ermitteln der Fehlerursache. Diese Funktion wird von der Software Crashlytics unterstützt.

Weitere Features für iOS und Android finden Sie in der nach Plattform sortierten Featurematrix für Citrix Secure Hub.

Geräteseitige Protokolle für Secure Hub generieren

In diesem Abschnitt wird erklärt, wie Sie geräteseitige Secure Hub-Protokolle generieren und die richtige Debug-Stufe dafür einrichten.

Mit den folgenden Schritten rufen Sie Secure Mail-Protokolle ab:

1. Navigieren Sie zu **Secure Hub > Hilfe > Problem melden**. Wählen Sie Secure Mail aus der Liste der Apps.
   Eine an den Helpdesk Ihrer Organisation adressierte E-Mail wird geöffnet.
2. Ändern Sie die Protokolleinstellungen nur, wenn das Supportteam Sie dazu angewiesen hat. Vergewissern Sie sich immer, dass die Einstellungen richtig gewählt sind.
3. Reproduzieren Sie das Problem in Secure Mail. Notieren Sie den Zeitpunkt, zu dem die Reproduktion des Problems begann, sowie denjenigen, zu dem das Problem auftrat bzw. eine Fehlermeldung angezeigt wurde.

4. Gehen Sie zurück zu **Secure Hub > Hilfe > Problem melden**. Wählen Sie Secure Mail aus der Liste der Apps.
   Eine an den Helpdesk Ihrer Organisation adressierte E-Mail wird geöffnet.
5. Geben Sie einen Betreff an und beschreiben Sie mit einigen Wörtern das Problem. Fügen Sie die in Schritt 3 gesammelten Zeitstempel ein und klicken Sie auf **Senden**.
   Die vollständige Nachricht wird einschließlich der in einer Zip angefügten Protokolldateien geöffnet.
6. Klicken Sie erneut auf **Senden**.

   Die gesendeten ZIP-Dateien enthalten die folgenden Protokolle:

   - CtxLog_AppInfo.txt (iOS), Device_And_AppInfo.txt (Android), logx.txt und WH_logx.txt (Windows Phone)

   App-Info-Protokolle enthalten Informationen über das Gerät und die Anwendung.

Überblick über Secure Mail

November 7, 2023

Citrix Secure Mail ermöglicht Benutzern das Verwalten ihrer E-Mails, Kalender und Kontakte auf ihren Mobiltelefonen und Tablets. Damit die Kontinuität von Microsoft Outlook- oder IBM Notes-Konten gewahrt bleibt, erfolgt eine Synchronisierung zwischen Secure Mail und Microsoft Exchange Server bzw. IBM Notes Traveler.

Als Teil der Citrix App-Serie unterstützt Secure Mail das Single Sign-On (SSO) bei Citrix Secure Hub. Bei Secure Hub angemeldete Benutzer können nahtlos nach Secure Mail wechseln, ohne Benutzernamen und Kennwort erneut eingeben zu müssen. Sie können Secure Mail so konfigurieren, dass es bei Registrierung eines Geräts bei Secure Hub automatisch per Push bereitgestellt wird, oder die Benutzer können die App aus dem Store hinzufügen.

> **Hinweis:**
>
> Die Unterstützung für Exchange Server 2010 endete am 13. Oktober 2020.

Secure Mail ist mit folgender Software kompatibel:

- Exchange Server 2019 Cumulative Update 13
- Exchange Server 2019 Cumulative Update 12
- Exchange Server 2019 Cumulative Update 11
- Exchange Server 2019 Cumulative Update 10

- Exchange Server 2019 Cumulative Update 9
- Exchange Server 2019 Cumulative Update 8
- Exchange Server 2019 Cumulative Update 7
- Exchange Server 2019 Cumulative Update 6
- Exchange Server 2016 Cumulative Update 23
- Exchange Server 2016 Cumulative Update 22
- Exchange Server 2016 Cumulative Update 21
- Exchange Server 2016 Cumulative Update 20
- Exchange Server 2016 Cumulative Update 19
- Exchange Server 2016 Cumulative Update 18
- Exchange Server 2016 Cumulative Update 17
- Exchange Server 2013 Cumulative Update 23
- Exchange Server 2013 Cumulative Update 22
- Exchange Server 2013 Cumulative Update 21
- HCL Domino Version 12.0.2 FP2
- HCL Traveler Version 12.0.2.1 Build 202302010413_30
- HCL Domino 11 (früher Lotus Notes)
- HCL Domino 10.0.1 (früher Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197 (früher Lotus Notes)
- HCL Domino 10.0.1.0 Build 201811191126_20 (früher Lotus Notes)
- HCL Domino 9.0.1.21 (früher Lotus Notes)
- Microsoft Office 365 (Exchange Online)

Um den Vorgang zu starten, laden Sie Secure Mail und andere Endpoint Management-Komponenten über Citrix Endpoint Management-Downloads herunter.

Angaben zu den Systemanforderungen für Secure Mail und andere Mobility-Apps finden Sie unter Systemanforderungen.

Informationen zu Benachrichtigungen in Secure Mail für iOS und Android bei im Hintergrund ausgeführter oder geschlossener App finden Sie unter Pushbenachrichtigungen für Secure Mail.

Informationen zu den von Secure Mail unterstützten iOS-Features finden Sie unter iOS-Features für Secure Mail.

Informationen zu den von Secure Mail unterstützten Android-Features finden Sie unter Android-Features für Secure Mail.

Informationen zu den von Secure Mail unterstützten iOS- und Android-Features finden Sie unter iOS- und Android-Features für Secure Mail.

Die Hilfedokumentation finden Sie in der Citrix-Benutzerhilfe unter Citrix Secure Mail.

Citrix Secure Web

July 17, 2023

Citrix Secure Web ist ein HTML5-kompatibler mobiler Webbrowser, der sicheren Zugriff auf interne und externe Sites bietet. Sie können Secure Web so konfigurieren, dass es bei Registrierung von Benutzergeräten bei Secure Hub automatisch per Push bereitgestellt wird. Alternativ können Sie die App aus dem App-Store von Endpoint Management hinzufügen.

Angaben zu den Systemanforderungen für Secure Web und andere mobile Produktivitätsapps finden Sie unter Systemanforderungen.

Integrieren und Bereitstellen von Secure Web

> **Hinweis:**
>
> Das MDX Toolkit 10.7.10 ist das letzten Release, das Umschließen von mobilen Produktivitätsapps unterstützt. Benutzer greifen über den öffentlichen App-Store auf mobile Produktivitätsapps Version 10.7.5 und höher zu.

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”weiter unten in diesem Artikel.

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. Dies ist die Standardkonfiguration 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. Secure Web kann jedoch keine Clientzertifikate lesen, die auf einem mobilen Gerät gespeichert sind. Umschlossene Unternehmensapps von Drittanbietern sind möglicherweise installiert, die diese Funktion anbieten. 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 "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.

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 zwischen-speichern	SSO für Citrix Gateway konfiguriert	Für Secure Web sind Anmeldein-formatio-nen beim ersten Zugriff auf eine Website erforderlich	Für Secure Web sind Anmeldein-formatio-nen bei weiteren Zugriffen auf die Website erforderlich	Für Secure Web sind Anmeldein-formatio-nen nach Ken-nwortän-derung erforderlich
Tunnel – Web-SSO	HTTP	No	Ja	No	No	No
Tunnel – Web-SSO	HTTPS	No	Ja	No	No	No
Vollständiges VPN	HTTP	No	Ja	No	No	No
Vollständiges VPN	HTTPS	Ja; Wenn die Secure Web-MDX-Richtlinie “Webken-nwort-caching aktivieren” auf “Ein” festgelegt ist	No	Ja; Zum Zwischen-speichern der An-meldeinfor-mationen in Secure Web erforderlich	No	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. Unabhängig vom Protokoll können sie jedoch keine öffentlichen URLs wie Facebook, Google und Hotmail öffnen.

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

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 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. Dieses VPN 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 und löschen Sie alle Ordner in dem 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**. Die Archivierung erfolgt im Hintergrund und kann einige Minuten dauern.
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 nun 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. Dies umfasst Sites 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 Citrix Secure Mail geöffnet, ohne dass sie sich erneut authentifizieren müssen.
- In iOS können Benutzer einen Link in Secure Web von einer nativen E-Mail-App aus durch Einfügen von **ctxmobilebrowser://** vor der URL öffnen. Beispiel: Um den Link `example.com` von einer nativen E-Mail-App aus zu öffnen, verwenden Sie die URL ctxmobilebrowser://example.com.
- 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

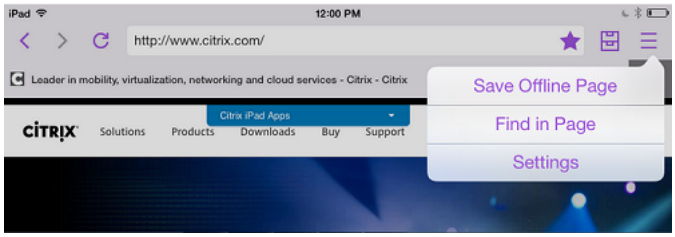
  > **Hinweis:**
  >
  > Ein Großteil des Speichers von Secure Web wird für die Wiedergabe von Popups verwendet, sodass die Leistung oft durch das Blockieren von Popups in “Einstellungen”erhöht werden kann.

- 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. Die App zeigt Schriftarten an, die die Benutzer auf ihren Geräten festlegen können.

> **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

Citrix QuickEdit für mobile Produktivitätsapps

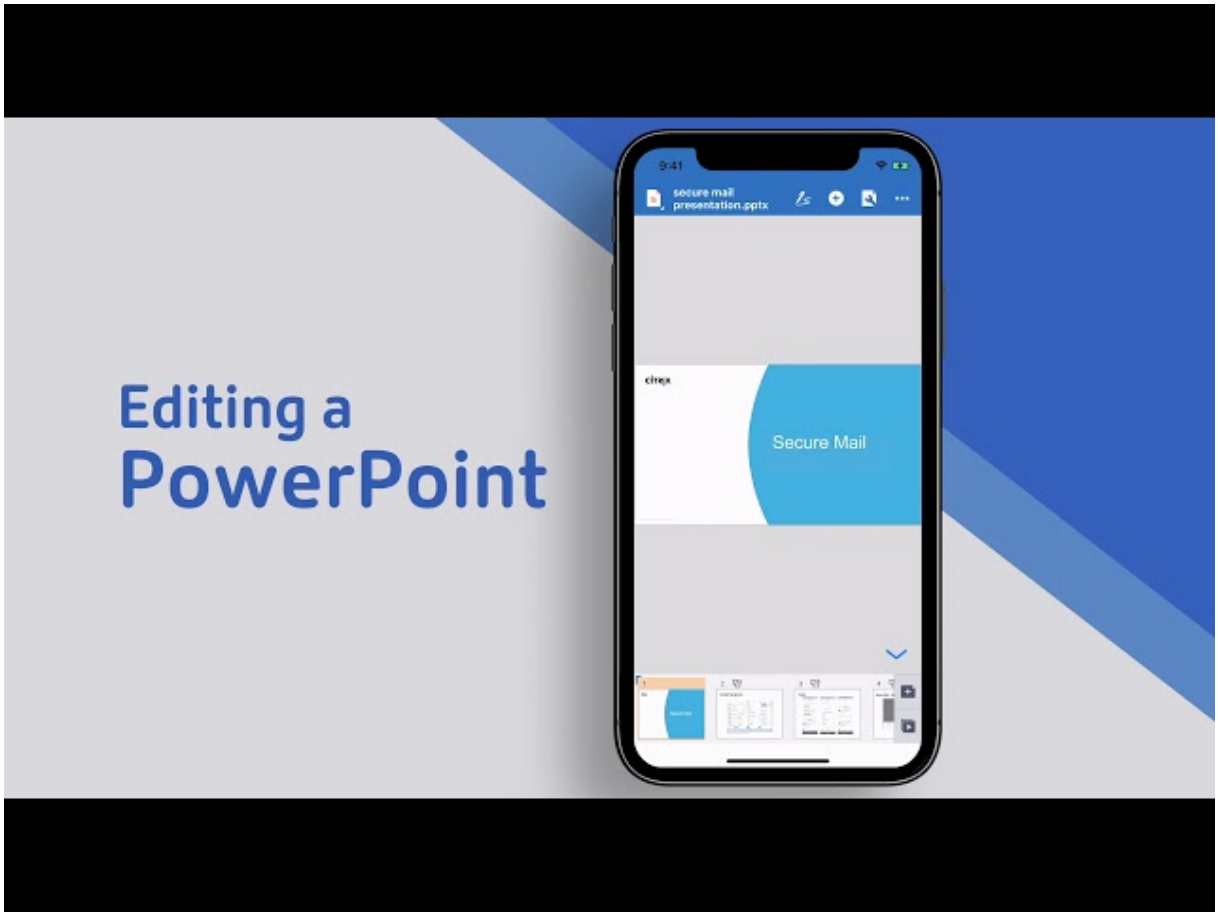
December 7, 2021

Citrix QuickEdit ist das Bearbeitungstool für mobile Produktivitätsapps. Es ist mit Citrix Secure Mail kompatibel und Citrix Content Collaboration für Endpoint Management und ermöglicht einen nahtlosen Workflow innerhalb der sicheren Endpoint Management-Umgebung.

> **Updates:**
>
> - **Update am 19. Juni 2020:** MDX-Verschlüsselung erreicht Ende des Lebenszyklus (EOL) am 1. September 2020. Sie müssen die Migration weg von der MDX-Verschlüsselung bis Juli

> 2020 testen und planen.
> - **Update am 2. Juli 2018:** QuickEdit bleibt als mobile Produktivitätsapp verfügbar. Das zuvor angekündigte Ende des Lebenszyklus (EOL) am 1. September 2018 findet nicht statt. Stattdessen sind Updates der Inhaltsverwaltungskomponente von QuickEdit geplant.

Ein Video über die Möglichkeiten der Citrix QuickEdit-Features finden Sie in diesem Video im YouTube-Kanal von Citrix:



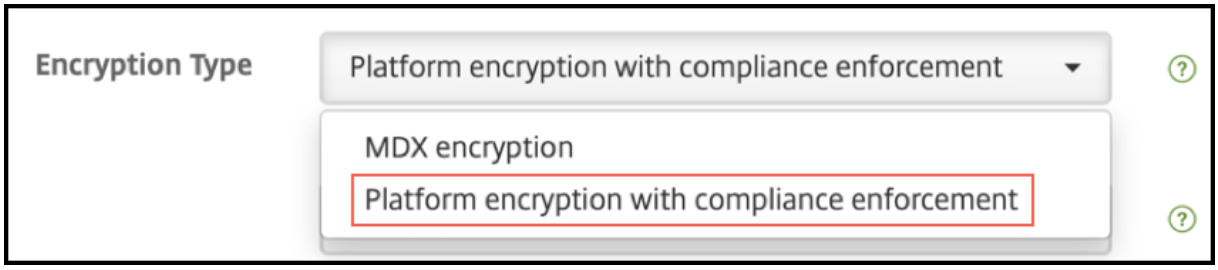
Angaben zu den Systemanforderungen für QuickEdit und andere mobile Produktivitätsapps finden Sie unter Systemanforderungen.

Sie können QuickEdit so konfigurieren, dass es bei Registrierung von Benutzergeräten bei Secure Hub automatisch per Push bereitgestellt wird. Alternativ können Benutzer die App aus dem App-Store hinzufügen.

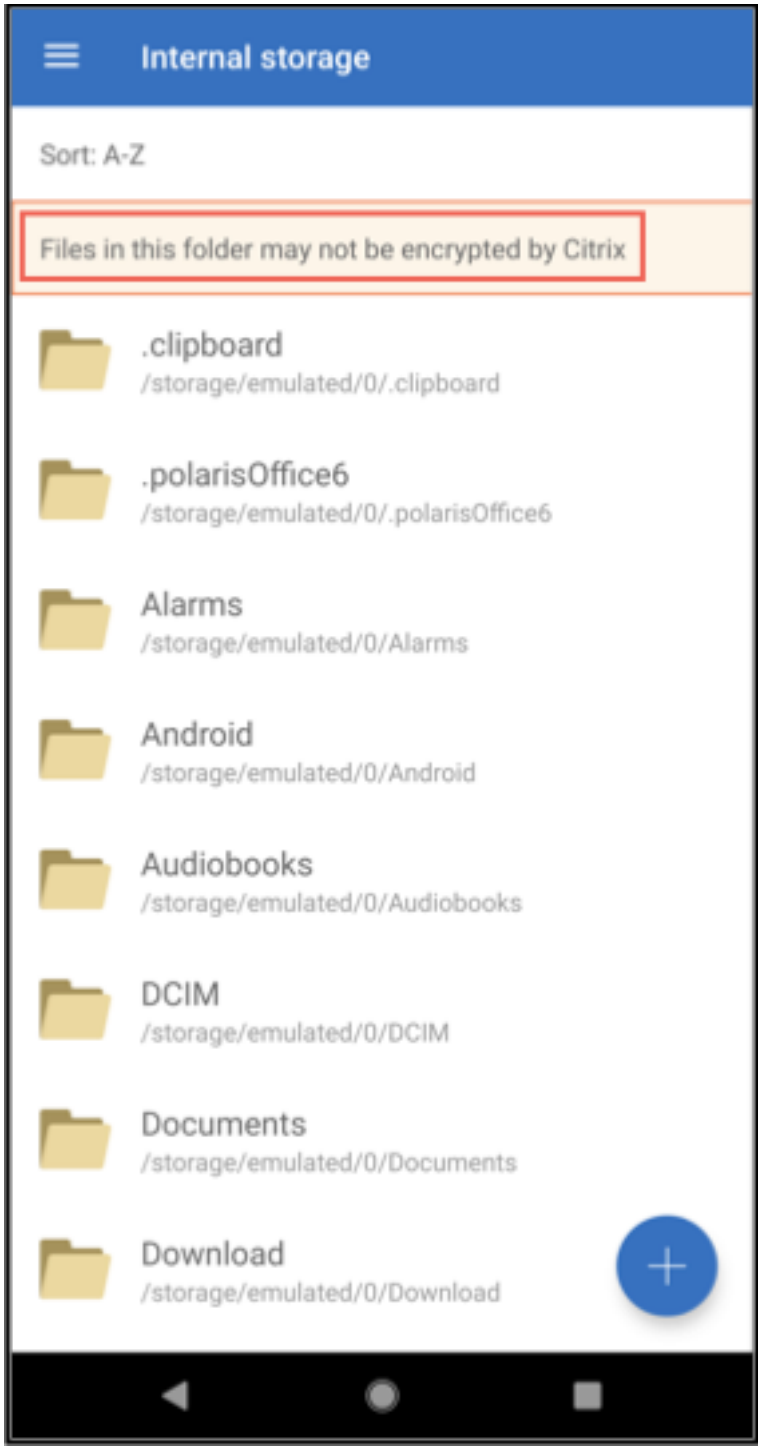
QuickEdit ist auch mit nativen E-Mail-Programmen kompatibel und ermöglicht so die einfache Freigabe oder Übertragung von Dateien als Anlage oder Citrix Files-Link.

Verschlüsselung

Mit QuickEdit Version 20.5.0 und höher können Sie den Typ der Datenverschlüsselung auswählen. Wählen Sie den Verschlüsselungstyp **Plattformverschlüsselung mit Durchsetzen der Compliance** für die Geräteplattform, um die Daten zu verschlüsseln.



Wenn Sie **Plattformverschlüsselung mit Durchsetzen der Compliance** auswählen, bleiben die Daten auf der SD-Karte des Geräts, auf der SD-Karte vorhandenen Dateien werden jedoch nicht verschlüsselt. Sie erhalten die folgende Warnung auf Ihrem Gerät:



Für Dateien, die in Cloud-Repositories gespeichert sind, ändert sich nur die Art der Datenverschlüsselung.

Unterstützte Dateitypen

- Microsoft Word: .doc und .docx
- Microsoft Excel –.xls und .xlsx
- Microsoft PowerPoint: .ppt und .pptx
- .csv, .txt
- .jpeg, .png, .png, .svg, .bmp

Die folgenden Dateitypen sind seit dem letzten Release veraltet: .docm,.xlsm,.pptm und.rft.

Integrieren und Bereitstellen von QuickEdit

Führen Sie zum Integrieren und Bereitstellen von QuickEdit mit Endpoint Management die folgenden allgemeinen Schritte aus:

1. Sie können auch Single Sign-On über Secure Hub aktivieren. Konfigurieren Sie dazu die Kontoinformationen von Citrix Files in Endpoint Management, um Endpoint Management als SAML-Identitätsanbieter für Citrix Files zu aktivieren.

   Die Konfiguration der Kontoinformationen für Citrix Files in Endpoint Management ist ein einmaliges Setup, das für alle Clients von Endpoint Management, Citrix Files und Nicht-MDX Citrix Files-Clients verwendet wird. Weitere Informationen finden Sie unter Integrieren und Bereitstellen von Citrix Files-Clients.

2. Laden Sie QuickEdit herunter.

   - Sie können QuickEdit von der Endpoint Management-Downloadseite herunterladen.
   - Für neue Benutzer ist QuickEdit auch auf der Citrix Workspace-Plattform verfügbar. Weitere Informationen finden Sie unter Citrix Workspace-Plattform.

3. Um QuickEdit zu Endpoint Management hinzuzufügen, führen Sie die gleichen Schritte aus, wie bei anderen MDX-Apps. Weitere Informationen finden Sie unter Apps hinzufügen.

Hochladen von Dateien

Sie können Dateien von Ihrem Gerät in Cloud-Repositories wie ShareFile hochladen und auf anderen Geräten darauf zugreifen. Derzeit unterstützen wir QuickEdit nur für iOS und Android. Wenn die Dateien jedoch in Cloud-Repositories migriert werden, können Sie sie mit jedem beliebigen Tool auf Ihrem Gerät bearbeiten.

Behobene und bekannte Probleme im aktuellen Release

Die folgenden Probleme sind im aktuellen Release bekannt oder wurden behoben.

Behobene Probleme

- Wenn Sie Dateien von QuickEdit für iOS oder ScanDirect an Secure Mail senden, schlägt die Dateiübertragung fehl. Um dieses Problem zu umgehen, fügen Sie in den Richtlinieneinstellungen für diese Apps die folgende Ausnahme zur Dateiverschlüsselung hinzu: "/tmp/.com.apple.Pasteboard". (Gilt für Version 6.14)

Bekannte Probleme

- Wenn eine Seitengröße 10.000 Punkte (Breite oder Höhe) überschreitet, werden Dokumente nicht geöffnet, um einen möglichen Speicherfehler zu vermeiden.
- Digitale Signaturen und Inlinebilder werden von QuickEdit nicht unterstützt.
- Wenn Benutzer auf iOS 12-Geräten unter QuickEdit eine Datei erstellen, wird eine Fehlermeldung aufgrund von unzureichendem Speicherplatz angezeigt.
- Die Benutzer können Anmerkungen zu PDF-Dateien nur dann sehen, wenn sie die Datei im Bearbeitungsmodus öffnen und dann die Option "Anmerkungen"auswählen.
- Wenn Benutzer eine PDF-Datei öffnen, die 150 MB überschreitet, wird die Fehlermeldung "Nicht unterstützte Datei"angezeigt.
- Bei QuickEdit auf iPads wird die Tastatur im **Bearbeitungsmodus** nicht wie erwartet angezeigt.
- Benutzer können keine PowerPoint-Datei (.ppt) erstellen, die mehr als ein Foto enthält.

Einschränkungen

- QuickEdit wird für gemeinsam genutzte Geräte nicht unterstützt.
- Wenn Sie eine ältere Version von QuickEdit ausführen, die gemeinsam genutzte Geräte unterstützt, und Sie ein Upgrade auf QuickEdit für iOS-Versionen 7.4.0 oder höher durchführen, gehen alle Ihre lokal verwalteten Dateien und Ordner verloren. Citrix Files-Daten bleiben jedoch unberührt und zugänglich.

ShareConnect

August 2, 2022

> **Wichtig:**
>
> ShareConnect hat das Ende des Lebenszyklus (EOL) am 30. Juni 2020 erreicht. Weitere Informationen finden Sie unter Ende des Lebenszyklus und veraltete Apps.

Mit ShareConnect können Benutzer sichere Verbindungen von iPads sowie Android-Tablets und -Telefonen mit ihren Computern herstellen und auf Dateien und Anwendungen zugreifen. Benutzer haben folgende Möglichkeiten:

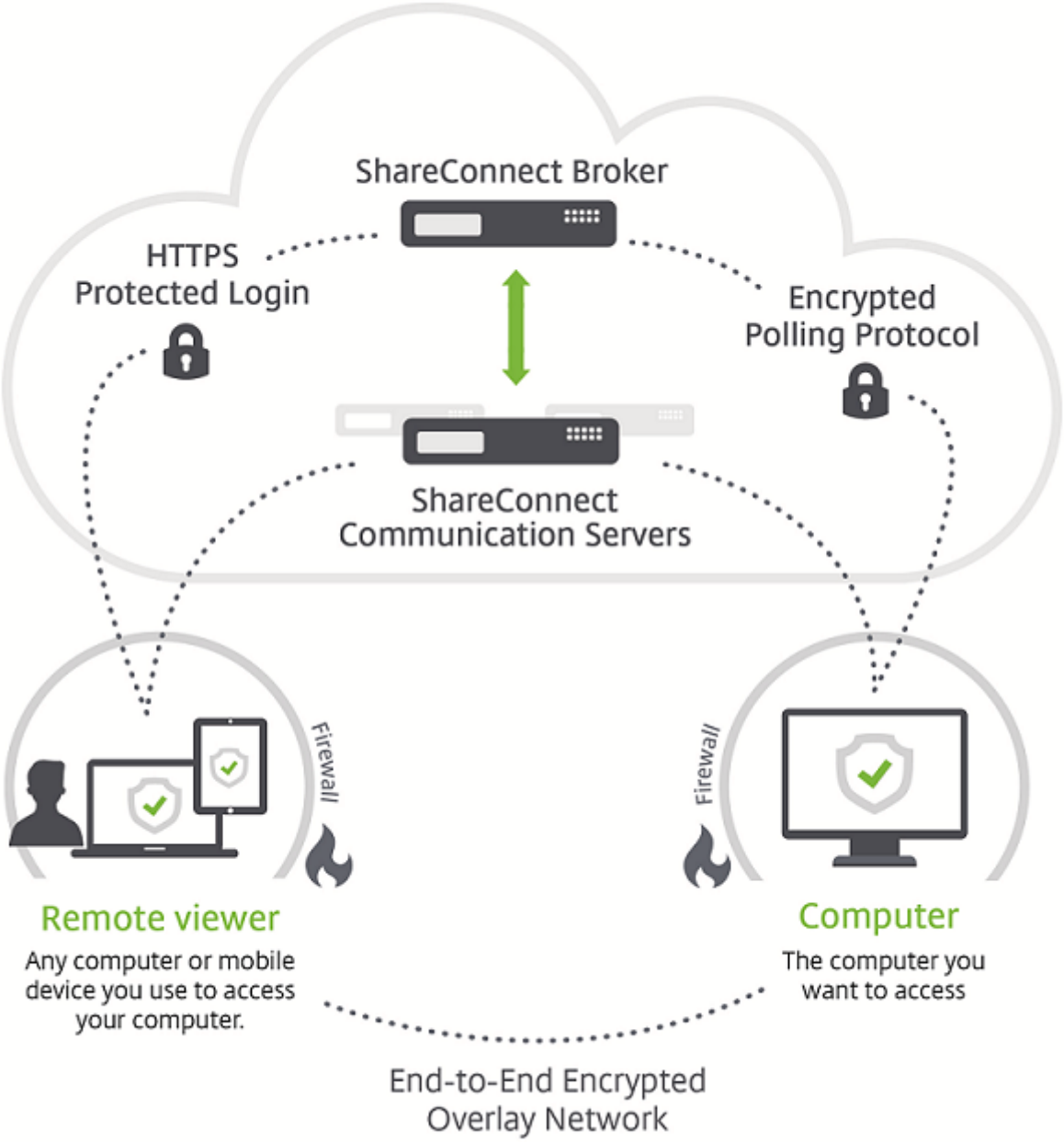
- Mit Dateien auf dem Computer und auf verbundenen Netzlaufwerken arbeiten
- Apps vom Zielcomputer in ShareConnect ausführen
- Auf mobile Apps zugreifen, ohne dass andere mobile Produktivitätsapps umschlossen werden müssen
- ShareConnect unter Citrix Virtual Desktops mit für Mobilgeräte optimiertem Zugriff ausführen

Sie können die MDX-Version von ShareConnect von der Endpoint Management-Downloadseite herunterladen.

Allgemeine Informationen zur Installation und Verwendung von ShareConnect finden Sie im Citrix Knowledge Center.

Architektur im Überblick

Zu den ShareConnect-Komponenten gehören der Citrix-eigene ShareConnect Broker und die ShareConnect-Kommunikationsserver, wie in der folgenden Abbildung dargestellt. Der ShareConnect Broker ist ein Anwendungsserver und eine Anwendungsdatenbank, mit denen Benutzer Computern zugeordnet werden. Die Anwendung informiert die Benutzer dann, ob ihr Hostcomputer online oder offline ist. ShareConnect-Kommunikationsserver werden für den Austausch von Daten zwischen Host und Clientcomputer verwendet. Basierend auf den **Endpoint Management**-Einstellungen können diese Daten über einen sicheren Micro VPN-Tunnel zwischen dem Host und den Clientcomputer geleitet werden.



Citrix Files ermöglicht zudem mit einem SAML-Identitätsanbieter wie Endpoint Management oder Active Directory-Verbunddienste (ADFS) die Benutzerauthentifizierung über Single Sign-On (SSO). Zugriff auf Ressourcen außerhalb des Netzwerks wird über Citrix Gateway in einer Bereitstellung mit Endpoint Management ermöglicht.

Funktionsweise von Verbindungen in ShareConnect

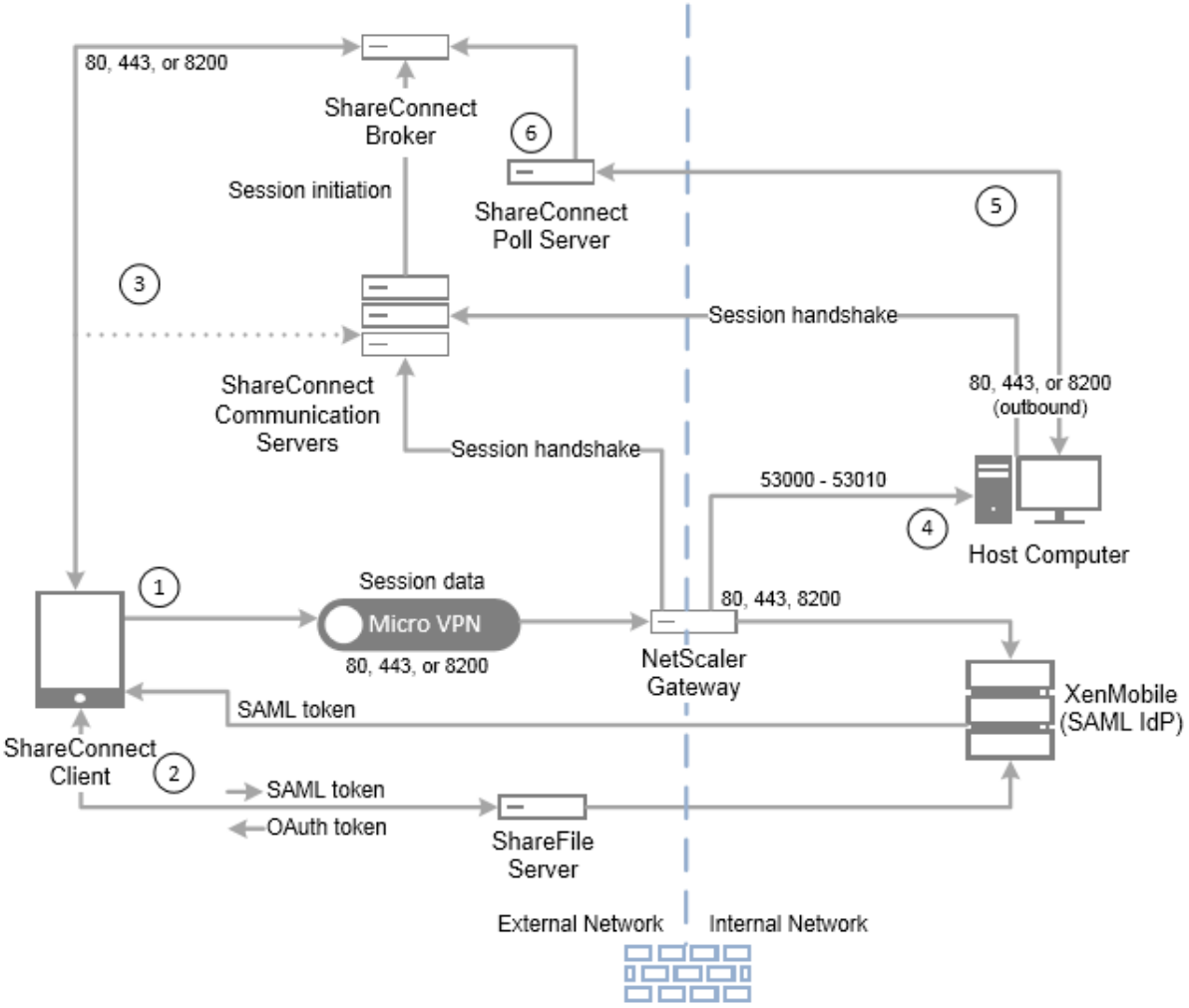
ShareConnect stellt entweder direkte oder indirekte Verbindungen her:

- **Direkte Verbindungen:** ShareConnect stellt eine direkte Verbindung zwischen Clientcomputer

und Hostcomputer her, wenn die Computer im gleichen LAN oder Wi-Fi-Netzwerk sind. In diesem Szenario fließen Daten direkt zwischen dem Hostcomputer und dem Clientcomputer oder einem mobilen Gerät, das für den Zugriff auf einen Hostcomputer verwendet wird. Die Daten werden nicht über die ShareConnect-Kommunikationsserver geleitet, was optimale Leistung ermöglicht. Bei direkten Verbindungen bietet Endpoint Management über Citrix Gateway sicheren Benutzerzugriff auf Ressourcen außerhalb des lokalen Netzwerks.

- **Indirekte Verbindungen:** ShareConnect stellt eine indirekte Verbindung zwischen einem Clientcomputer und einem Hostcomputer her, wenn die Computer nicht direkt erreichbar sind. In diesem Szenario werden Daten über die ShareConnect-Kommunikationsserver geleitet.

Die folgende Abbildung zeigt die verwendeten Verbindungen, wenn Benutzer von einem Computer oder Mobilgerät mit ShareConnect über direkte Verbindungen auf einen Hostcomputer zugreifen. Die Verbindungsschritte werden nach der Abbildungen beschrieben.



⊠ In diesem Szenario fungiert Endpoint Management als SAML-Identitätsanbieter für Citrix Files, um SSO von Secure Hub zu ermöglichen. ShareConnect fordert ein SAML-Token bei Secure Hub an, das

die Anforderung über Citrix Gateway an Endpoint Management weiterleitet. Endpoint Management sendet dann das SAML-Token an ShareConnect.

 ShareConnect sendet das SAML-Token an Citrix Files zur Validierung und um das SAML-Token gegen ein OAuth-Token einzutauschen.

 ShareConnect sendet das OAuth-Token an den ShareConnect-Broker, der dann ein Sitzungstoken an ShareConnect sendet.

 ShareConnect ruft eine Liste der Hostcomputer vom ShareConnect-Broker ab und fordert die Anmeldeinformationen des Hostcomputers an. ShareConnect stellt dann eine direkte Verbindung mit dem ShareConnect-Kommunikationsserver her. Nachdem der Hostcomputer die Anmeldeinformationen validiert hat, erhält ShareConnect eine Liste der Dateien und Apps vom Hostcomputer. Wenn der Benutzer eine Datei oder App öffnet, wird eine direkte Verbindung zwischen ShareConnect und dem Hostcomputer hergestellt.

 ShareConnect-Agent auf dem Hostcomputer sendet Statusmeldungen an den ShareConnect-Abfrageserver, um zu melden, ob er online oder offline ist.

 Der ShareConnect-Abfrageserver sendet per Load Balancing Anfragen von ShareConnect-Agent an den ShareConnect-Broker und Host-Statusaktualisierungen an den ShareConnect-Broker.

Sicherheit in ShareConnect

Mit integrierter 128-Bit-AES-Verschlüsselung gewährleistet ShareConnect die vollständige End-To-End-Verschlüsselung von Daten, die zwischen dem ShareConnect-Client und einem Hostcomputer mit ShareConnect-Agent gesendet werden. Der Verschlüsselungsschlüssel ist für jede Verbindung eindeutig. Selbst die komplexesten Geräte können die zum Dekodieren der Verschlüsselung benötigten Daten nicht abfangen.

Bei der typischen Konfiguration von ShareConnect werden Daten direkt zwischen dem ShareConnect-Client und einem Hostcomputer gesendet. Daten werden nur über die ShareConnect-Kommunikationsserver geleitet, wenn Sie für die Netzwerkzugriffsrichtlinie uneingeschränkten Zugriff festlegen. Informationen zu Richtlinien finden Sie unter “Hinzufügen von ShareConnect zu Endpoint Management”in diesem Artikel.

Für direkte und indirekte Verbindungen werden verschlüsselte Metadaten, wie die für Verbindungen erforderlichen IP-Adressen und Ports, an die ShareConnect-Server gesendet.

Darüber hinaus bietet das Umschließen von ShareConnect mit MDX Datenverschlüsselung über den MDX Vault. Der Tresor verschlüsselt mit MDX umschlossene App und zugehörige gespeicherte Daten sowohl auf iOS (vor iOS 9) als auch auf Android-Geräten. Die Verschlüsselung erfolgt mit FIPS-zertifizierten kryptografischen Modulen, die von OpenSSL bereitgestellt werden.

Informationen zu Sicherheitseinstellungen und zur Verwaltung finden Sie in den folgenden Whitepapers über Sicherheit.

ShareConnect Security Whitepaper

ShareConnect-Administratordokumentation

Portanforderungen für ShareConnect

Öffnen Sie die folgenden Ports, um die Kommunikation mit ShareConnect zuzulassen. Die Portanforderungen unterscheiden sich je nach Verbindungstyp. Die Verbindungen können direkte Verbindungen sein, wenn die Computer im gleichen LAN- oder Wi-Fi-Netzwerk sind. Oder es können indirekte Verbindungen sein, wenn die Client- und Hostcomputer einander nicht direkt erreichen können.

Für direkte Verbindungen

TCP-Port 80: für ausgehende Verbindungen von Citrix Gateway zu app.shareconnect.com

Quelle: Citrix Gateway

Ziel: app.shareconnect.com

TCP-Port 80, 443, 8200: Mindestens einer dieser Ports ist für ausgehende Verbindungen von Citrix Gateway zum ShareConnect-Kommunikationsserver erforderlich.

Quelle: Citrix Gateway

Ziel: ShareConnect-Kommunikationsserver

TCP-Port 80, 443, 8200: für ausgehende Verbindungen von ShareConnect-Hostcomputern zu Citrix Servern

Quelle: ShareConnect-Hostcomputer

Ziel: poll.shareconnect.com, ShareConnect-Kommunikationsserver

TCP-Port 443: für ausgehende Verbindungen von Citrix Gateway zu erforderlichen Sites

Quelle: Citrix Gateway

Ziel: crashlytics.com, secure.sharefile.com, ShareFile_sub-domain.sharefile.com

TCP-Port 53000–53010: für ausgehende Verbindungen von Citrix Gateway zu ShareConnect-Hostcomputern

Quelle: Citrix Gateway

Ziel: LAN-basierte ShareConnect-Hostcomputer

TCP-Port 53000–53010: für eingehende Verbindungen von Citrix Gateway zu ShareConnect-Hostcomputern

Quelle: Citrix Gateway

Ziel: LAN-basierte ShareConnect-Hostcomputer

Für indirekte Verbindungen

TCP-Port 80: für ausgehende Verbindungen vom ShareConnect-Agent zu app.ShareConnect.com

Quelle: ShareConnect-Agent

Ziel: app.shareconnect.com

TCP-Port 80, 443, 8200: Mindestens einer dieser Ports ist für ausgehende Verbindungen vom ShareConnect-Agent zum ShareConnect-Kommunikationsserver erforderlich.

Quelle: ShareConnect-Agent

Ziel: ShareConnect-Kommunikationsserver

TCP-Port 80, 443, 8200: für ausgehende Verbindungen von ShareConnect-Hostcomputern zu Citrix Servern

Quelle: ShareConnect-Hostcomputer

Ziel: poll.shareconnect.com, ShareConnect-Kommunikationsserver

TCP-Port 443: für ausgehende Verbindungen vom ShareConnect-Agent zu erforderlichen Sites

Quelle: ShareConnect-Agent

Ziel: crashlytics.com, secure.sharefile.com, ShareFile_sub-domain.sharefile.com

Integrieren und Bereitstellen von ShareConnect

Führen Sie zum Integrieren und Bereitstellen von ShareConnect mit Endpoint Management die folgenden allgemeinen Schritte aus:

1. Sie können auch Single Sign-On über Secure Hub aktivieren. Konfigurieren Sie dazu die Kontoinformationen von Citrix Files in Endpoint Management, um Endpoint Management als SAML-Identitätsanbieter für Citrix Files zu aktivieren.

   Die Citrix Files-Kontoinformationen müssen nur einmal in Endpoint Management konfiguriert werden. Dieses einmalige Setup wird für alle Clients von mobilen Produktivitätsapps, Citrix Files-Clients und Nicht-MDX Citrix Files-Clients verwendet.

2. Laden Sie ShareConnect herunter und umschließen Sie die App. Weitere Informationen finden Sie unter Informationen zum MDX Toolkit.

3. Fügen Sie ShareConnect zu Endpoint Management hinzu und konfigurieren Sie MDX-Richtlinien.
4. Installieren Sie ShareConnect-Agent auf den Hostcomputern. Der ShareConnect-Agent ist ein MSI-Paket. Daher können Sie den Agent mit den vorhandenen Bereitstellungsmethoden für Software bereitstellen und installieren. Benutzer müssen dann den Hostcomputer registrieren, indem sie sich innerhalb einer Stunde nach der Installation mit ihren Citrix Files-Anmeldeinformationen am Agent anmelden.

   Alternativ können Benutzer ShareConnect-Agent auf dem Computer installieren, mit dem sie sich über ShareConnect verbinden. Weitere Informationen finden Sie im Abschnitt “Installieren des ShareConnect-Agent auf einem Computer”in diesem Artikel.

ShareConnect zu Endpoint Management hinzufügen

Sie fügen ShareConnect zu Endpoint Management hinzu, indem Sie die gleichen Schritte wie bei anderen MDX-Apps ausführen. Weitere Informationen finden Sie unter Hinzufügen einer MDX-App. Beim Hinzufügen von ShareConnect konfigurieren Sie die entsprechenden MDX-Richtlinien wie in der folgenden Tabelle aufgeführt.

Richtlinie	Wert	Ergebnisse
Netzwerkzugriff	Tunneled to the internal network oder Unrestricted	Bei Tunneled to the internal network wird ein anwendungsspezifischer VPN-Tunnel zurück zum internen Netzwerk für den gesamten Netzwerkzugriff verwendet. Diese Konfiguration bietet eine direkte Verbindung zwischen ShareConnect und einem Hostcomputer. Bei der Einstellung Unrestricted werden verschlüsselte Daten zwischen einem Hostcomputer und ShareConnect-Agent über Citrix eigene Kommunikationsserver geleitet. Testen Sie den Setup mit unbeschränktem Zugriff, um sicherzustellen, dass alles einwandfrei funktioniert, selbst wenn Sie Tunneled to the internal network für den Netzwerkzugriff verwenden.
Bevorzugter VPN-Modus	Tunnel –Web-SSO	Legt den entsprechenden Anfangsmodus für Verbindungen fest, die Single Sign-On erfordern.
Verschlüsselung aktivieren	Ein	Verschlüsselt die Daten auf dem Tablet.
Ausschneiden und Kopieren	Uneingeschränkt	Aktiviert Ausschneide- und Kopiervorgänge für ShareConnect.
Einfügen	Uneingeschränkt	Aktiviert Einfügevorgänge für ShareConnect.

Richtlinie	Wert	Ergebnisse
Dokumentaustausch (Öffnen in)	Uneingeschränkt	Erlaubt Benutzern das Öffnen aller Dateien auf dem verbundenen Computer oder Netzlaufwerk in ShareConnect.
Kennwort speichern	Aus	Benutzer müssen bei jeder Anmeldung an ShareConnect den Benutzernamen und das Kennwort für ihren Computer eingeben.

Installieren des ShareConnect-Agent auf einem Computer

Mit den folgenden Schritten wird beschrieben, wie Benutzer ShareConnect-Agent auf physischen oder virtuellen Computern installieren, um über ein unterstütztes Mobilgerät eine Verbindung zu ihnen herzustellen.

Bevor sie diese Schritte ausführen, müssen Benutzer erst Secure Hub installieren. Dann folgen Benutzer den Aufforderungen, damit die mobilen Produktivitätsapps auf dem unterstützten Mobilgerät installiert werden.

1. Melden Sie sich auf dem Tablet bei Secure Hub an.
2. Öffnen Sie ShareConnect.
3. Tippen Sie auf “Email download link”.

   Citrix sendet Ihnen eine E-Mail von no-reply@shareconnect.com.
4. Öffnen Sie die E-Mail auf dem Hostcomputer, auf den Sie von ShareConnect aus zugreifen möchten.
5. Klicken Sie in der E-Mail auf Set up this computer.
6. Doppelklicken Sie auf **ShareConnect_Installer.exe**, um die Installation zu starten.

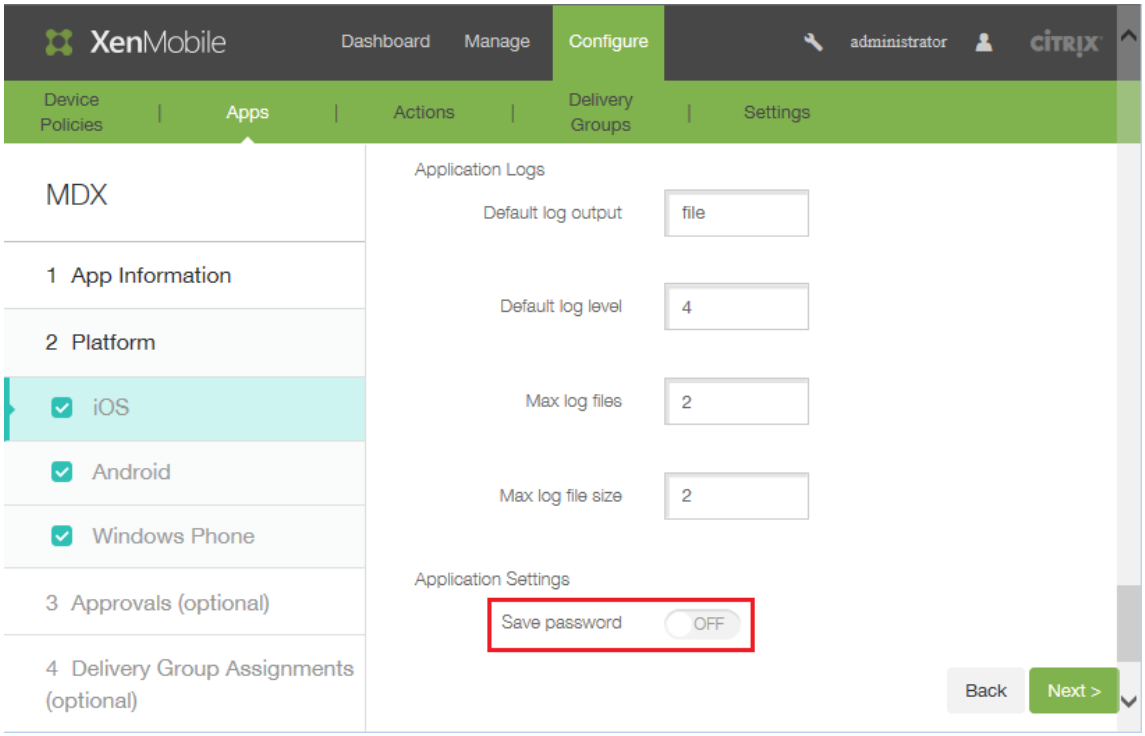
   ShareConnect-Agent wird auf Ihrem Hostcomputer installiert. Während der Installation werden Sie von ShareConnect aufgefordert, eine E-Mail-Adresse anzugeben, wenn Citrix Files-SSO konfiguriert ist. Alternativ fordert Sie ShareConnect auf, die Citrix Files-Anmeldeinformationen einzugeben, wenn Citrix Files-SSO nicht konfiguriert ist.
7. Folgen Sie den Anweisungen in den Assistenten für ShareConnect und erste Schritte.

Der ShareConnect-Agent registriert dann den Hostcomputer. Der Hostcomputer kann über einen ShareConnect-Client verbunden sein, sofern der Hostcomputer eingeschaltet ist und über wenigstens

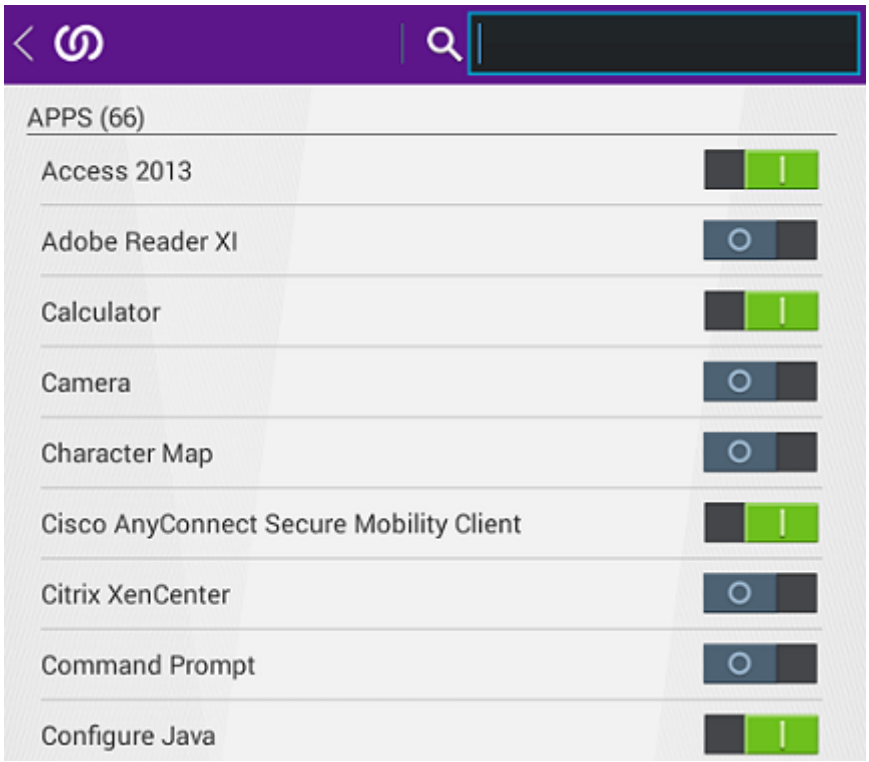
einen der veröffentlichten Ports (80, 443 oder 8200) eine Verbindung mit poll.shareconnect.com herstellen kann.

Features von ShareConnect

- **Hinzufügen von Hostcomputern**: Mit ShareConnect können Benutzer über unterstützte Mobilgeräte Remote-Hostcomputer hinzufügen und eine Verbindung mit diesen herstellen.
- **Zugreifen auf Dateien**: Benutzer können eine Liste der kürzlich verwendeten Dateien anzeigen und auf dem Hostcomputer sowie auf verbundenen Laufwerken nach Dateien suchen und sie ansteuern.
- **Bearbeiten von Dateien**: Vom Tablet aus können Benutzer auf Desktopanwendungen auf dem Hostcomputer zugreifen, um Dateien zu bearbeiten. Die Benutzer können die Anwendungen im Vollbildmodus verwenden.
- **Bildschirmfreigabe**: Anstelle der Ansicht einer einzigen Datei oder App können Benutzer mit dem Bildschirmfreigabe-Feature den Desktop ihres Hostcomputers anzeigen.
- **Citrix Files-Integration**. Benutzer können Dateien zwischen dem Hostcomputer und Citrix Files verschieben oder freigeben.
- **Tastatur und Maus**: ShareConnect unterstützt die gleichzeitige Verwendung einer Bluetooth-Tastatur und die Citrix XI Prototyp-Maus.
- **Beschränkte Ports**: ShareConnect verwendet nur die Ports 53000 bis 53010.
- **Kennworteingabe bei jeder Anmeldung erfordern**: Diese Option bietet erhöhte Sicherheit, da Benutzer bei jeder Anmeldung an ShareConnect zur Eingabe ihres Computerkennworts aufgefordert werden. Wenn die Richtlinie “Kennwort speichern”deaktiviert ist (siehe Abbildung), müssen Benutzer ihre Anmeldeinformationen für alle Verbindungen eingeben.



- **Hinzufügen oder Löschen von Apps**: Benutzer können Apps zum App-Bereich in ShareConnect hinzufügen bzw. daraus löschen, indem sie eine App mit ihrem Schalter auswählen oder die Auswahl aufheben.



- **Zwischenspeichern von in der Vorschau angezeigten Dateien**: ShareConnect speichert

Dateien zwischen, auf die bereits zugegriffen wurde, sodass die Dateien nicht erneut heruntergeladen werden müssen, wenn Benutzer nach der Vorschau von anderen Dateien zu den vorherigen zurückkehren. Mit diesem Feature wird die Ladezeit verkürzt, wenn Benutzer anschließend auf Dateien zugreifen.

Problembehandlung bei ShareConnect

ShareConnect-Agent –Installationsprobleme

Problem	Beschreibung und Lösung
Wenn ein Benutzer ShareConnect-Agent herunterlädt und dann eine Stunde oder länger mit dem Start der Installation wartet, muss der Benutzer seinen Citrix Files-Kontonamen und das Kennwort eingeben, um ShareConnect-Agent zu registrieren.	Der Installer von ShareConnect-Agent enthält ein Token, das eine Stunde nach dem Download abläuft. Wenn ein Benutzer die Installation nicht vor Ablauf des Tokens startet, muss der Benutzer sich zwei Mal an seinem Citrix Files-Konto anmelden: einmal, um ShareConnect-Agent zu registrieren und danach noch einmal, um sich nach dem Abschluss der Installation am Agent anzumelden. Wenn Benutzer ShareConnect-Agent herunterladen und innerhalb einer Stunde installieren, müssen sie sich nur einmal anmelden.
Während der Registrierung von ShareConnect-Agent stellt der Agent keine Verbindung her und eine Fehlermeldung wie “Überprüfen Sie die Verbindung, und versuchen Sie es dann erneut.”wird angezeigt.	Überprüfen Sie, dass der Port für poll.shareconnect.com nicht blockiert ist. Weitere Informationen finden Sie in diesem Artikel unter “Systemanforderungen”.

ShareConnect –Verbindungsprobleme

> **Wichtig:**
>
> Wir empfehlen, dass Sie zum Testen von ShareConnect die Netzwerkzugriffsrichtlinie auf **Uneingeschränkt** festlegen, um Probleme mit Ports und Netzwerkeinstellungen auszuschließen. Beim uneingeschränktem Zugriff ist ShareConnect gezwungen, Verbindungen über die ShareConnect-Kommunikationsserver herzustellen, sodass Sie die Verbindung testen können, wenn das ShareConnect-Mobilgerät und der Hostcomputer Internetzugriff haben.

Problem	Beschreibung und Lösung
ShareConnect wird gestartet, aber es wird keine Verbindung zum Hostcomputer hergestellt und keine Eingabeaufforderung für Anmeldeinformationen erfolgt.	Überprüfen Sie, ob Ihr Setup den unter Systemanforderungen aufgeführten Portanforderungen entspricht.
Benutzer können sich nicht mit ihren Citrix Files-Kontoanmeldeinformationen an ShareConnect anmelden.	Für SSO für ShareConnect muss Ihr Citrix Files-Konto mit einem SAML-Identitätsanbieter konfiguriert sein. Informationen zur Verwendung von Endpoint Management als SAML-Identitätsanbieter finden Sie unter Citrix Content Collaboration für Endpoint Management. Informationen zum Konfigurieren von anderen Identitätsanbietern finden Sie im Knowledge Center-Artikel. Wenn SSO nicht für Ihr Konto konfiguriert ist, fordert ShareConnect für iOS die Eingabe des Citrix Files-Benutzernamens und -Kennworts.
Wenn Benutzer sich an ShareConnect angemeldet haben, kann ShareConnect keine Verbindung mit dem Hostcomputer herstellen.	Wenn ShareConnect zum Herstellen direkter Verbindungen konfiguriert ist (d. h. die Netzwerkzugriffsrichtlinie ist auf “Tunnel zum internen Netzwerk”festgelegt), können Einschränkungen in den Netzwerkeinstellungen, wie Firewalls und konfigurierte Proxyserver, Verbindungsfehler verursachen.

Citrix ShareFile Workflows

October 31, 2018

> **Hinweis:**
>
> Secure Forms hat am 31. März 2018 das Ende des Lebenszyklus erreicht. Wir empfehlen, dass Sie ShareFile WorkFlows verwenden, das in Platinum- und Premium-Konten von Citrix Files enthalten ist.

ShareFile Workflows ist die mobile Komponente des Features für benutzerdefinierte Workflows in Citrix Files. Dieses Feature ermöglicht Benutzern das Erstellen benutzerdefinierter Workflows, die

mehrere Auslöser und Aktionen enthalten. Benutzerdefinierte Formulare können Workflowvorlagen hinzugefügt und Benutzern zugewiesen werden.

Wenn einem Benutzer ein Formular zugewiesen wird, kann der Benutzer das Formular in der mobilen ShareFile Workflows-App ausfüllen und übermitteln. Das Speichern von Formulardaten ist sicher in Citrix Files integriert. Workflowdateien werden zur Überprüfung, Referenz und zum Abrufen gespeichert.

Workflow- und Formularvorlagen werden in der Citrix Files-Webanwendung erstellt und verwaltet.

Benutzerdokumentation

Benutzerdokumentation über das Erstellen und Verwalten von Workflows und Formularvorlagen finden Sie im Citrix Knowledge Center:

- Erstellen einer Workflowvorlage
- Erstellen einer Formularvorlage
- Übermitteln von Formularen mit der mobilen Workflows-App

Citrix Content Collaboration für Endpoint Management

July 17, 2023

Citrix Content Collaboration für Endpoint Management-Clients sind MDX-fähige Versionen von mobilen Clients für Citrix Files. Diese Clients bieten sicheren, integrierten Zugriff auf Daten in anderen, mit MDX umschlossenen Apps. Citrix Content Collaboration für Endpoint Management-Clients profitieren von MDX-Features wie Micro VPN, Single Sign-On (SSO) über Secure Hub und zweistufiger Authentifizierung.

Citrix Files ist ein Dateisynchronisierungs- und Dateifreigabedienst für Unternehmen, mit dem Benutzer einfach und sicher Dateien austauschen können. In Citrix Files haben Benutzer verschiedene Zugriffsoptionen, einschließlich mobiler Citrix Files-Clients, wie Citrix Files für Android Phone und Citrix Files für iPad.

Sie können Citrix Files in Endpoint Management integrieren, um den vollen Funktionsumfang von Citrix Files bereitzustellen oder um nur Zugriff auf StorageZones-Connectors zu erhalten. Standardmäßig aktiviert die Citrix Endpoint Management-Konsole nur die Konfiguration von Citrix Files. Informationen zur Konfiguration von Endpoint Management zur Verwendung mit StorageZones-Connectors finden Sie unter Citrix Content Collaboration mit Endpoint Management in der Citrix Endpoint Management-Dokumentation.

Sie verwenden Endpoint Management, Citrix Files, StorageZones-Controller und Citrix ADC wie folgt, um Citrix Content Collaboration für Endpoint Management-Clients bereitzustellen und zu verwalten:

- Wenn Endpoint Management mit Citrix Files konfiguriert wird, fungiert Endpoint Management als SAML-Identitätsanbieter (IdP) und stellt Citrix Content Collaboration für Endpoint Management-Clients bereit. Citrix Files verwaltet Citrix Files-Daten. Es werden keine Daten von Citrix Files über Endpoint Management übertragen.
- Wenn Endpoint Managementmit Citrix Files oder mit StorageZones-Connectors konfiguriert ist, stellt der StorageZones-Controller eine Verbindung zu den Daten in Netzwerkfreigaben und SharePoint her. Benutzer greifen auf die gespeicherten Daten über die mobilen Produktivitätsapps von Citrix Files zu. Benutzer können auf Mobilgeräten Microsoft Office-Dokumente bearbeiten und Adobe PDF-Dateien in der Vorschau anzeigen und mit Anmerkungen versehen.
- Citrix ADC verwaltet Anforderungen von externen Benutzern, schützt deren Verbindungen, erledigt den Lastausgleich bei den Anforderungen und regelt das Content Switching für StorageZones-Connectors.

Informationen zum Herunterladen von Citrix Content Collaboration für Endpoint Management-Clients finden Sie unter Downloads auf citrix.com.

Angaben zu den Systemanforderungen für Citrix Content Collaboration für Endpoint Management und andere mobile Produktivitätsapps finden Sie unter Unterstützung für mobile Produktivitätsapps.

Unterschiede zwischen Citrix Content Collaboration für Endpoint Management-Clients und den mobilen Clients für Citrix Files

Im Folgenden werden die Unterschiede zwischen Citrix Content Collaboration für Endpoint Management-Clients und mobilen Clients für Citrix Files beschrieben.

Benutzerzugriff

Citrix Content Collaboration für Endpoint Management-Clients:

Benutzer erhalten und öffnen Citrix Content Collaboration für Endpoint Management-Clients über Secure Hub.

Mobile Clients für Citrix Files:

Benutzer erhalten mobile Clients für Citrix Files über App Stores.

SSO

Citrix Content Collaboration für Endpoint Management-Clients:

Für die Integration von Endpoint Management mit Citrix Files: Sie können Endpoint Management als SAML-Identitätsanbieter für Citrix Files konfigurieren. In dieser Konfiguration erhält Secure Hub ein SAML-Token für den Citrix Content Collaboration für Endpoint Management-Client, wobei Endpoint Management als SAML-Identitätsanbieter verwendet wird. Ein Benutzer, der den Citrix Content Collaboration für Endpoint Management-Client startet, aber nicht bei Secure Hub angemeldet ist, wird aufgefordert, sich bei Secure Hub anzumelden. Benutzer brauchen daher ihre Citrix Files-Domäne oder -Kontoinformationen nicht zu kennen.

Mobile Clients für Citrix Files:

Sie können Endpoint Management und Citrix Gateway als SAML-Identitätsanbieter für Citrix Files konfigurieren. In dieser Konfiguration werden Benutzer, die sich bei Citrix Files über einen Webbrowser oder über andere Citrix Files-Clients anmelden, zur Endpoint Management-Umgebung für die Benutzerauthentifizierung umgeleitet. Nach der erfolgreichen Authentifizierung durch Endpoint Management erhalten Benutzer ein SAML-Token für die Anmeldung bei ihrem Citrix Files-Konto.

Micro-VPN

Citrix Content Collaboration für Endpoint Management-Clients:

Remotebenutzer können mit einer VPN- oder Micro VPN-Verbindung über Citrix Gateway auf Anwendungen und Desktops im internen Netzwerk zugreifen. Dieses Feature ist durch die Integration von Citrix ADC in Endpoint Management verfügbar und für Benutzer transparent.

Mobile Clients für Citrix Files:

Nicht verfügbar

Zweistufige Authentifizierung

Citrix Content Collaboration für Endpoint Management-Clients:

Die Citrix ADC-Integration in Endpoint Management unterstützt außerdem die Authentifizierung mit einer Kombination aus Clientzertifikat und einem anderen Authentifizierungstyp, z. B. LDAP oder RADIUS.

Mobile Clients für Citrix Files:

Nicht verfügbar

Ordnerberechtigungen

Citrix Content Collaboration für Endpoint Management-Clients und mobile Clients für Citrix Files:

Für die Integration von Endpoint Management in Citrix Files: Von Citrix Files festgelegt.

Schutz bei Dokumentzugriff

Citrix Content Collaboration für Endpoint Management-Clients:

Benutzer können in Secure Mail erhaltene oder von einer MDX-umschlossenen App heruntergeladene Anlagen öffnen. Nur MDX-umschlossene Apps werden angezeigt, wenn der Benutzer eine "Öffnen-in"-Aktion ausführt. Daten aus einer nicht umschlossenen App sind für einen Citrix Content Collaboration für Endpoint Management-Client nicht verfügbar. Benutzer von Secure Mail können Dateien aus ihrem Citrix Files-Repository anfügen, ohne die Datei auf das Gerät herunterzuladen. Wenn ein Benutzer das umschlossene und das nicht umschlossene Citrix Files auf einem Gerät hat, hat der umschlossene Citrix Files-Client keinen Zugriff auf Dateien im persönlichen Citrix Files-Konto des Benutzers. Der umschlossene Citrix Files-Client kann nur auf die in Endpoint Management konfigurierte Citrix Files-Unterdomäne zugreifen.

Mobile Clients für Citrix Files:

Benutzer können Anlagen aus jeder App öffnen.

Citrix Files-Kontozugriff

Citrix Content Collaboration für Endpoint Management-Clients:

Für die Integration von Endpoint Management in Citrix Files: Um auf ein persönliches Citrix Files-Konto oder ein Citrix Files-Konto eines Drittanbieters zugreifen zu können, müssen Benutzer eine Nicht-MDX-Version von Citrix Files auf dem Gerät verwenden.

Mobile Clients für Citrix Files:

Für die Integration von Endpoint Management in Citrix Files: Verfügbar über Citrix Files-Clients.

Geräterichtlinien

Citrix Content Collaboration für Endpoint Management-Clients und mobile Clients für Citrix Files:

Sowohl die Geräterichtlinien für Endpoint Management als auch für Citrix Files gelten für Citrix Content Collaboration für Endpoint Management-Clients. Beispielsweise können Sie mit der Endpoint Management-Konsole ein Gerät löschen. Mit der Citrix Files-Konsole können Sie die Citrix Files-App remote löschen.

MDX-Richtlinien

Citrix Content Collaboration für Endpoint Management-Clients:

Mit den MDX-Richtlinien in Citrix Endpoint Management können Sie Einstellungen konfigurieren, die vom Endpoint Management App Store durchgesetzt werden. Richtlinien, die nur über MDX verfügbar sind, umfassen u. a. das Blockieren von Kamera, Mikrofon, E-Mail-Erstellung, Bildschirmaufnahme und von Funktionen zum Ausschneiden, Kopieren und Einfügen für die Zwischenablage.

Mobile Clients für Citrix Files:

Nicht verfügbar

Datenverschlüsselung

Citrix Content Collaboration für Endpoint Management-Clients und mobile Clients für Citrix Files:

Verschlüsselt alle gespeicherten Daten mit AES-256 und schützt Daten während der Übertragung mit SSL 3.0 und mindestens 128-Bit-Verschlüsselung.

Verfügbarkeit

Citrix Content Collaboration für Endpoint Management-Clients:

Citrix Content Collaboration für Endpoint Management-Clients sind in den Editionen Endpoint Management Advanced und Enterprise enthalten.

Mobile Clients für Citrix Files:

Alle Endpoint Management-Editionen enthalten alle Citrix Files-Features. Sie können Endpoint Management in dem vollen Funktionsumfang von Citrix Files oder nur StorageZones-Connectors integrieren.

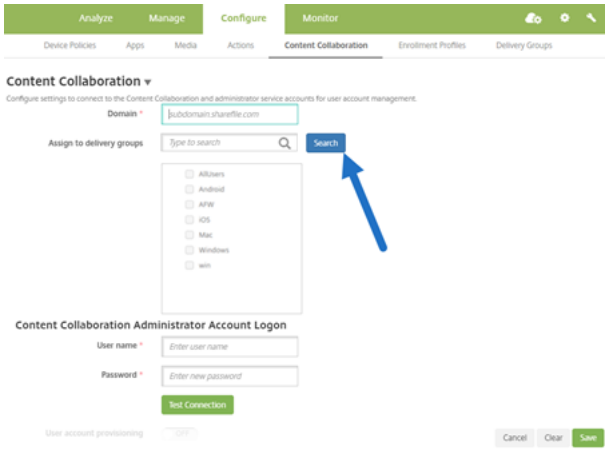
Integration und Bereitstellung von Citrix Content Collaboration für Endpoint Management-Clients

Führen Sie zum Integrieren und Bereitstellen von Citrix Content Collaboration für Endpoint Management-Clients die folgenden allgemeinen Schritte aus:

1. Aktivieren Sie Endpoint Management als SAML-Identitätsanbieter für Citrix Files, um SSO von Citrix Files-Clients für Citrix Files bereitzustellen. Hierfür müssen Sie Citrix Files-Kontoinformationen in Endpoint Management für SSO konfigurieren. Weitere Informationen finden Sie unter “Konfigurieren von Citrix Files-Kontoinformationen in Endpoint Management für SSO”.

> **Wichtig:**
>
> Um Endpoint Management als SAML-Identitätsanbieter für Nicht-MDX-Citrix Files-Clients wie die Citrix Files-Webanwendung und die Citrix Files Sync-Clients zu verwenden, ist eine zusätzliche Konfiguration erforderlich. Weitere Informationen finden Sie auf der Citrix Files-Supportsite in folgendem Artikel:
>
> Citrix Files (ShareFile) Single Sign-On SSO. Der Artikel enthält einen Downloadlink für den Endpoint Management Configuration Guide.

2. Laden Sie die Citrix Files-Clients herunter.
3. Fügen Sie die Citrix Files-Clients zu Endpoint Management hinzu. Weitere Informationen zum "Hinzufügen von Citrix Files zu Endpoint Management"finden Sie weiter unten in diesem Artikel.
4. Überprüfen Sie die Konfiguration. Weitere Informationen finden Sie unter "Validieren von Citrix Files-Clients"weiter unten in diesem Artikel.



Info zu den Einstellungen:

- Domain ist die Citrix Files-Unterdomäne, die für die Clients verwendet wird.
- Nur die Benutzer in den ausgewählten Bereitstellungsgruppen haben über die Clients SSO-Zugriff auf Citrix Files.

  Wenn ein Benutzer in einer Bereitstellungsgruppe kein Citrix Files-Konto hat, stellt das Endpoint Management dem Benutzer Citrix Files zur Verfügung, wenn Sie den Citrix Files-Client zum Endpoint Management hinzufügen.
- Mit den Anmeldeinformationen für das Citrix Files-Administratorkonto speichert Endpoint Management die SAML-Einstellungen in der Citrix Files-Steuerungsebene.

> **Wichtig:**
>
> Die Konfiguration, die Single Sign-On von Citrix Files-Clients an Citrix Files ermöglicht, authentifiziert die Benutzer nicht an Netzwerkfreigaben oder SharePoint-Dokumentbibliotheken. Für den Zugriff auf diese Connector-Datenquellen ist die Authentifizierung bei der Active Directory-Domäne erforderlich, in der sich die Netzwerkfreigaben oder SharePoint-Server befinden.

Konfigurieren von Citrix Files-Kontoinformationen in Endpoint Management für SSO

Um SSO vom Secure Hub für mobile Produktivitätsapps zu aktivieren, geben Sie in der Endpoint Management-Konsole Informationen zum Citrix Files-Konto und zum Citrix Files-Administratordienstkonto an. Mit dieser Konfiguration fungiert Endpoint Management als SAML-Identitätsanbieter für Citrix Files, für mobile Produktivitätsappclients, Citrix Files-Clients und Nicht-MDX-Citrix Files-Clients. Wenn ein Benutzer einen mobilen Produktivitätsappclient startet, bezieht Secure Hub einen SAML-Token für den Benutzer aus Endpoint Management und sendet ihn an den Citrix Files-Client.

Klicken Sie in der Endpoint Management-Konsole auf **Konfigurieren** > **Content Collaboration**. Dies ist der frühere Name von Citrix Files.

Hinzufügen von Citrix Content Collaboration für Endpoint Management-Clients zu Endpoint Management

Wenn Sie Citrix Content Collaboration für Endpoint Management-Clients zu Endpoint Management hinzufügen, können Sie den SSO-Zugriff auf Connector-Datenquellen aus Citrix Content Collaboration für Endpoint Management-Clients aktivieren. Dazu müssen Sie die Netzwerkzugriffsrichtlinie und die Richtlinie “Bevorzugter VPN-Modus”konfigurieren (Anweisungen in diesem Abschnitt).

Voraussetzungen

- Endpoint Management muss in der Lage sein, Ihre Citrix Files-Unterdomäne zu erreichen. Um die Verbindung zu testen, pingen Sie Ihre Citrix Files-Unterdomäne über den Endpoint Management-Server an.
- Für Ihr Citrix Files-Konto und für das Hypervisor, auf dem Endpoint Management ausgeführt wird, müssen identische Zeitzonen konfiguriert sein. Wenn die Zeitzonen unterschiedlich sind, schlagen SSO-Anfragen u. U. fehl, weil das SAML-Token Citrix Files möglicherweise nicht im erwarteten Zeitrahmen erreicht. Um den NTP-Server für Endpoint Management zu konfigurieren, verwenden Sie die Befehlszeilenschnittstelle von Endpoint Management.

> **Hinweis:**
>
> Der Hyper-V-Host legt die Zeit einer Linux-VM auf die lokale Zeitzone und nicht auf UTC fest.

- Melden Sie sich als Administrator beim ShareFile-Konto an und überprüfen Sie die SAML-SSO-Einstellungen in **Einstellungen** > **Administratoreinstellungen** > **Sicherheit** > **Anmelde- und Sicherheitsrichtlinie** > **Single Sign-On / SAML 2.0-Konfiguration**.
- Laden Sie die Citrix Content Collaboration für Endpoint Management-Clients herunter.

Schritte:

1. Klicken Sie in der Endpoint Management-Konsole auf **Konfigurieren > Apps** und dann auf **Hinzufügen**.
2. Klicken Sie auf **MDX**.
3. Geben Sie für die App Informationen in die Felder **Name** und optional **Beschreibung** und **App-Kategorie** ein.
4. Klicken Sie auf **Weiter** und laden Sie dann die MDX-Datei für den Citrix Content Collaboration für Endpoint Management-Client hoch.
5. Klicken Sie auf **Weiter**, um die App-Informationen und -Richtlinien zu konfigurieren.

   Die Konfiguration, die Single Sign-On von Citrix Content Collaboration für Endpoint Management-Clients an Citrix Files ermöglicht, authentifiziert die Benutzer nicht bei Netzwerkfreigaben oder SharePoint-Dokumentbibliotheken.
6. Zum Aktivieren von SSO zwischen dem Secure Hub-Micro-VPN und StorageZones-Controllern führen Sie die folgenden Richtlinienkonfigurationen durch:

   - Legen Sie die Netzwerkzugriffsrichtlinie auf **Tunnel zum internen Netzwerk** fest.

     In diesem Modus wird der gesamte Netzwerkverkehr, der vom Citrix Content Collaboration für Endpoint Management-Client ausgeht, durch das MDX Framework abgefangen. Mit einem app-spezifischen Micro-VPN wird der Netzwerkverkehr dann über Citrix Gateway umgeleitet.
   - Legen Sie die Richtlinie “Bevorzugter VPN-Modus”auf **Tunnel - Web-SSO** fest.

     In diesem Tunnelmodus beendet das MDX Framework den SSL/HTTP-Datenverkehr von einer MDX-App und initiiert für den Benutzer neue Verbindungen zu internen Verbindungen. Mit dieser Einstellung kann das MDX Framework Authentifizierungsaufforderungen von Webservern erkennen und darauf reagieren.
7. Erteilen Sie die Genehmigungen und führen Sie Bereitstellungsgruppenzuweisungen nach Bedarf aus.

Nur die Benutzer in den ausgewählten Bereitstellungsgruppen haben über die Citrix Content Collaboration für Endpoint Management-Clients SSO-Zugriff auf Citrix Files. Wenn ein Benutzer in einer Bereitstellungsgruppe kein Citrix Files-Konto hat, stellt das Endpoint Management dem Benutzer Citrix Files zur Verfügung, wenn Sie den Citrix Content Collaboration für Endpoint Management-Client zum Endpoint Management hinzufügen.

So überprüfen Sie Citrix Content Collaboration für Endpoint Management-Clients

1. Nachdem Sie die hier beschriebene Konfiguration durchgeführt haben, starten Sie den Citrix Content Collaboration für Endpoint Management-Client. Sie werden nicht von Citrix Files aufgefordert, sich anzumelden.
2. Verfassen Sie in Secure Mail eine E-Mail und fügen Sie eine Anlage aus Citrix Files hinzu. Die Citrix Files-Homepage wird geöffnet, ohne dass Sie zur Anmeldung aufgefordert werden.

> **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

Ende des Lebenszyklus und veraltete Apps

July 17, 2023

Die folgenden Apps haben das Ende des Lebenszyklus (EOL) erreicht oder stehen kurz davor, den EOL-Status zu erreichen. Wenn ein Produktrelease EOL erreicht, können Sie das Produkt entsprechend den Bedingungen der Lizenzvereinbarung weiterhin verwenden, jedoch sind die verfügbaren Supportoptionen beschränkt. Historische Informationen wird im Knowledge Center oder in anderen Online-Ressourcen angezeigt. Die Dokumentation wird nicht mehr aktualisiert und bleibt im derzeitigen Status verfügbar. Weitere Informationen über den Produktlebenszyklus finden Sie in der Produktmatrix.

> **Hinweis:**
>
> Vorankündigungen zu Features von Citrix Endpoint Management, die schrittweise ausgemustert werden, finden Sie unter Einstellung von Features und Plattformen.

Citrix Files für XenMobile (MDX): Citrix Files für XenMobile erreichte EOL am 1. Juli 2023.

Wir empfehlen Kunden, Citrix Files zu verwenden, das im Apple App Store und in Google Play verfügbar ist. Es ist MAM-SDK-fähig.

Secure Mail für Intune SDK (iOS und Android): Secure Mail erreichte EOL am 30. April 2023.

Citrix Files für Intune: Veraltet ab 31. Dezember 2020.

Wir empfehlen, die Plattformfunktionen zu nutzen, um die normale Citrix Files-App (die in den App-Stores verfügbar ist) über Android Enterprise (mit Arbeitsprofil) und iOS-Benutzerregistrierung in einem Container zu verpacken.

ShareConnect: ShareConnect hat EOL am 30. Juni 2020 erreicht.

Secure Notes: Das End-of-Life-Datum (EOL) war der 31. Dezember 2018.

Wenn Sie die Funktionen von Secure Notes und Secure Tasks benötigen, empfehlen wir Notate for Citrix, eine Drittanbieteranwendung, die Sie mit MDX-Richtlinien sichern können.

Wenn Benutzer von Secure Notes und Secure Tasks Daten in Outlook gespeichert haben, können sie auf die Daten in Notate zugreifen. Wenn Benutzer Daten in ShareFile, jetzt Citrix Files, gespeichert haben, werden die Daten nicht migriert.

Die Benutzer können Secure Notes über das EOL-Datum hinaus weiterverwenden, bis ihr Plattformbetriebssystem die Benutzeroberfläche nicht mehr unterstützt. Citrix rät jedoch von der Verwendung nicht unterstützter Produkte ab.

Secure Tasks: Das End-of-Life-Datum (EOL) war der 31. Dezember 2018.

Secure Forms: Das End-of-Life-Datum (EOL) war der 31. März 2018. Citrix empfiehlt den Wechsel zu Citrix ShareFile Workflows, die im Angebot für Citrix Files Platinum- und Premium-Konten enthalten sind. Weitere Informationen finden Sie unter Citrix ShareFile Workflows.

ScanDirect: ScanDirect hat EOL am 1. September 2018 erreicht.

Zulassen der sicheren Interaktion mit Office 365-Apps

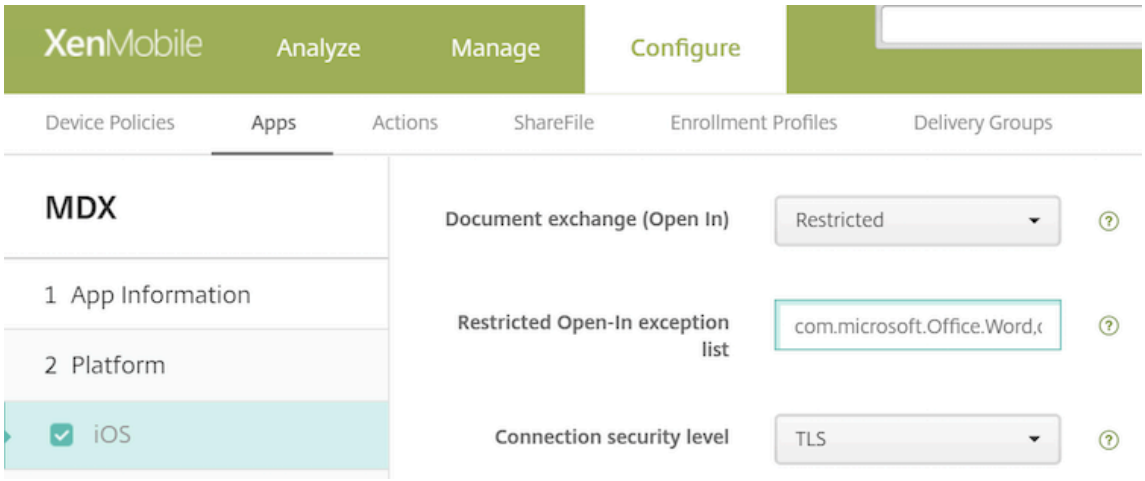
December 7, 2021

Citrix Secure Mail, Secure Web und Citrix Files bieten die Option, den MDX-Container zu öffnen und Benutzern die Übertragung von Dokumenten und Daten zu Microsoft Office 365-Apps zu erlauben. Diese Funktionalität wird für iOS- und Android-Plattformen mit den Öffnen-in-Richtlinien in der Endpoint Management-Konsole verwaltet.

Daten, die in einer Microsoft-App geöffnet werden, sind nicht länger im MDX-Container gesichert oder verschlüsselt. Überlegen Sie sich die Auswirkungen auf die Sicherheit, bevor Sie dieses Feature aktivieren. Besonders Kunden, die großen Wert auf den Schutz vor Datenverlust legen oder die dem HIPAA oder anderen strengen rechtlichen Bestimmungen unterliegen, sollten sich die möglichen Auswirkungen durch das Öffnen des Containers gut überlegen.

Aktivieren von Office 365 in iOS

1. Laden Sie die aktuelle Version von Secure Mail, Secure Web oder Citrix Files-Apps von der Endpoint Management-Downloadseite herunter.
2. Laden Sie die Dateien auf die Endpoint Management-Konsole hoch.
3. Navigieren Sie zur Richtlinie **Dokumentaustausch (Öffnen in)** und legen Sie sie auf **Eingeschränkt** fest. Microsoft Word, Excel, PowerPoint, OneNote und Outlook werden automatisch in der **Ausnahmeliste für eingeschränktes Öffnen** aufgeführt. Zum Beispiel: com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook



Bei MDM-Registrierungen sind weitere Steuerelemente für iOS-Geräte verfügbar.

Sie können iTunes-Apps in die Endpoint Management-Konsole hochladen und die Apps per Push auf Geräten bereitstellen. Wenn Sie diese Option wählen, legen Sie die folgenden Richtlinien auf **EIN** fest:

- App entfernen, wenn MDM-Profil entfernt wird:
- App-Datenbackup verhindern
- Verwaltung der App erzwingen (Beim selektiven Löschen werden die App und alle Daten gelöscht.)

Damit keine Dokumente und Daten von Microsoft-Apps zu nicht verwalteten Apps auf dem Gerät übermittelt werden können, navigieren Sie in der Endpoint Management-Konsole zu **Konfigurieren > Geräte > Einschränkungen > iOS** und legen Sie für die Richtlinien **Dokumente von verwalteten Apps in nicht verwalteten Apps** und **Dokumente von nicht verwalteten Apps in verwalteten Apps** die Einstellung **AUS** fest.

Aktivieren von Office 365 in Android

1. Laden Sie die aktuelle Version von Secure Mail, Secure Web oder Citrix Files-Apps von der Endpoint Management-Downloadseite herunter.
2. Laden Sie die Dateien auf die Endpoint Management-Konsole hoch.
3. Navigieren Sie in der Richtlinie **Dokumentaustausch (Öffnen in)** nach unten und legen Sie **Eingeschränkt** fest.
4. Fügen Sie in der **Ausnahmeliste für eingeschränktes Öffnen** die folgenden Paket-IDs hinzu:

   `{ package=com.microsoft.office.word } { package=com.microsoft.office.powerpoint } { package=com.microsoft.office.excel }`
5. Konfigurieren Sie wie gewohnt die weiteren App-Richtlinien und speichern Sie die Apps.

Die Benutzer müssen Dateien aus Secure Mail, Secure Web oder Citrix Files auf ihren Geräten speichern und mit einer Office 365-App öffnen.

Die Benutzer können sowohl unter iOS als auch unter Android die folgenden Dateitypen auf ihren Geräten öffnen und bearbeiten:

Unterstützte Dateiformate

Die unterstützten Dateiformate finden Sie in der Microsoft Office-Dokumentation.