Secure Hub

Contents

Citrix Secure Hub

June 11, 2019

Citrix Secure Hub ist das Launchpad 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 Downloadseite für Citrix Endpoint Management herunterladen.

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

Neue Funktionen in diesem Release

Secure Hub für Android 19.5.5

Dieses Release enthält Leistungsverbesserungen und Fehlerbehebungen.

Was ist neu in früheren Releases

Secure Hub 19.5.0, 19.4.5 und 19.3.5

Diese Releases enthalten Leistungsverbesserungen und Fehlerbehebungen.

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 Fehlerbehebungen.

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 WiFi-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

Verbesserte Secure Hub-Benutzeroberfläche einschließlich Schriftarten und Farben. 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 Fehlerbehebungen.

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 Geräteeinschränkungsrichtlinie.

Secure Hub 18.10.5 bis 18.11.0 beinhaltet Fehlerbehebungen und Leistungsverbesserungen.

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 Geräteeinschränkungsrichtlinie.

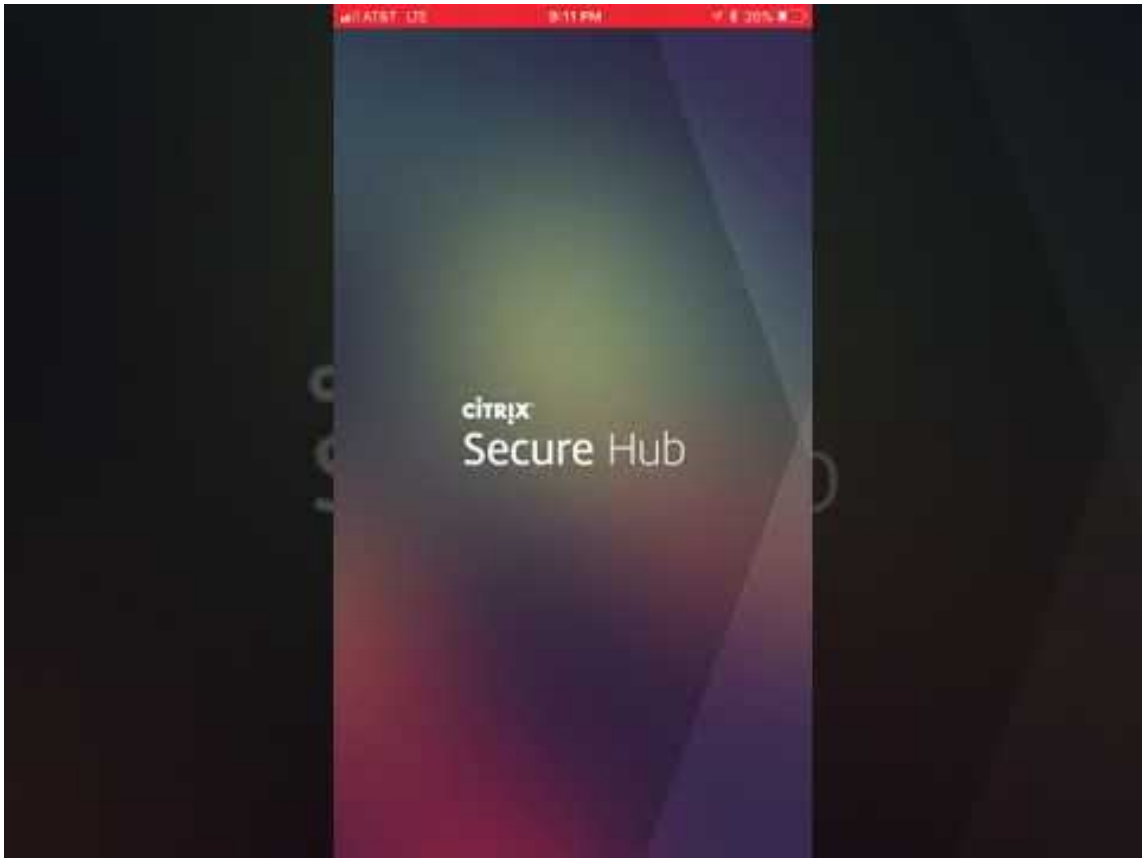
- **Unterstützung für Android SafetyNet:** Sie können Endpoint Management zur Verwendung des **Android SafetyNet**-Features konfigurieren, um die Kompatibilität und Sicherheit von Android-Geräten mit installiertem Secure Hub zu bewerten. Die Ergebnisse können genutzt werden, um automatisierte Aktionen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

Secure Hub 10.8.60 bis 18.9.0

Fehlerbehebungen und Leistungsverbesserungen.

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 bzw. mit Domäne und Sicherheitstoken.
- Workspace-Integration für Endpoint Management aktivieren. Weitere Informationen zur Workspaceintegration finden Sie unterWorkspacekonfiguration.

> 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 im Artikel zu Verhaltensänderungen unter Android P auf der Android Developer Website.

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). Einzelheiten finden Sie auf 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 instal-

> lieren, 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. Einzelheiten finden Sie unter Endpoint Management AutoDiscovery Service.
- Private oder selbstsignierte ZS und der Autodiscovery-Service (ADS) von Endpoint Management 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. 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.
- 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 bi-

etet hohe Sicherheit, die keine Active Directory-Spur auf Benutzergeräten hinterlässt.

Damit Secure Hub diesen Authentifizierungstyp 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. Einzelheiten 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 **Edit**.
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 FQDNs:

FQDN	IP-Adresse	Port	IP- und Port-Nutzung
`discovery.mdm.zenprise.com`	52.5.138.94	443	Secure Hub - ADS-Kommunikation

FQDN	IP-Adresse	Port	IP- und Port-Nutzung
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.

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 Registrierungseinstellungen.

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. Anweisungen finden Sie unter Servereigenschaften.
- Die Clienteigenschaften ENABLE_CREDENTIAL_STORE und SEND_LDAP_ATTRIBUTES. Anweisungen 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. Einzelheiten 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 Featurematrix nach Plattform für Citrix Secure Hub.

Bekannte und behobene Probleme

June 11, 2019

Bekannte Probleme in Secure Hub für Android 19.5.5

- In Secure Hub für Android verlieren Geräte im COSU-Modus (Corporate Owned Single Use) nach wenigen Minuten der Registrierung die Konnektivität und erhalten keine Benachrichtigungen, selbst wenn GCM aktiviert ist. [CXM-62977]
- Wenn Sie die Standortrichtlinie auf Geräten gleichzeitig für den Modus “Profilbesitzer” und “Gerätebesitzer” bereitstellen, wird das Benutzerkonto im Modus “Gerätebesitzer” gelöscht. Dieses Problem tritt während der NFC-Bump-Registrierung auf und wenn Endpoint Management im MDM-Modus konfiguriert ist. [CXM-63429]

Behobene Probleme in Secure Hub für Android 19.5.5

- Ab diesem Release unterstützt Secure Hub nur Geräte mit Android 5.0 und höher. [CXM-35542]
- Registrieren Sie in Secure Hub für Android ein Gerät im Gerätebesitzermodus und legen Sie ein neues Kennwort fest. Das Gerät ist beim ersten Versuch nicht gesperrt. [CXM-66509]

Bekannte und behobene Probleme in früheren Versionen

Bekannte Probleme in Secure Hub für Android 19.5.0

- Nach der Registrierung ist auf Geräten mit OnePlus Android Version 7.1.1 und OnePlus 5T Android Version 9.0.3 für die Eingabe der Citrix PIN ein manueller Neustart von Secure Hub erforderlich. [CXM-64120]
- In Secure Hub für Android werden erforderliche Apps nur dann auf Android-Geräten bereitgestellt, wenn Sie die Richtlinie oder den Store aktualisieren. [CXM-65635]

Behobene Probleme in Secure Hub für Android 19.5.0

- Ab diesem Release unterstützt Secure Hub nur Geräte mit Android 5.0 und höher. [CXM-35542]
- In Secure Hub für Android können Android 6.0-Geräte nicht registriert werden, wenn im Serverzertifikat mehrere alternative Antragstellernamen angegeben sind. [CXM-65030]
- In Secure Hub für Android werden verwaltete Apps nach der Aufhebung der Registrierung von Geräten nicht deinstalliert. [CXM-65369]
- Auf Samsung S9-Geräten tritt nach dem Update auf Android P das folgende Problem auf: Wenn Sie das Gerätekennwort über Endpoint Management ändern, wird das Kennwort auf dem Gerät nicht geändert. Stattdessen wird der Bildschirm schwarz und die Endpoint Management-Konsole zeigt für das Geräte den Status “Gesperrt” an. [CXM-66391]

Bekannte Probleme in Secure Hub Version 19.4.5

Es gibt keine bekannten Probleme in diesem Release.

Behobene Probleme in Version 19.4.5

Secure Hub für iOS

Wenn Sie auf iOS-Geräten auf den Link zur Geräteregistrierung klicken, wird der Name der Endpoint Management-FQDN-Instanz nicht automatisch in Secure Hub ausgefüllt. Die Geräteregistrierungsanforderung schlägt fehl. [CXM-65423]

Secure Hub für Android

In diesem Release wurden keine Probleme behoben.

Bekannte Probleme in Version 19.3.5

Secure Hub für iOS

Beim Empfang neuer Benachrichtigungen von Secure Hub für iOS wird der Benachrichtigungszähler für Secure Hub nicht aktualisiert. [CXM-53500]

Secure Hub für Android

Es gibt keine bekannten Probleme in diesem Release.

Behobene Probleme in Version 19.3.5

Secure Hub für iOS

In diesem Release wurden keine Probleme behoben.

Secure Hub für Android

- Wenn Sie in Secure Hub für Android gemeinsam genutzte Geräte registrieren, die **Webclip**-Richtlinie bereitstellen und Web- und SaaS-Apps hinzufügen, können Sie die Bereitstellung erfolgreich abschließen. Im **App-Bestandsfenster** der Citrix Endpoint Management-Konsole wird die Bereitstellung jedoch als fehlgeschlagen angezeigt. [CXM-57500]
- Wenn sich Benutzer in Secure Hub für Android mit Secure PIN anmelden, wird zwar ein VPN-Tunnel eingerichtet, aber keine Website in Secure Web geladen. Die Website wird jedoch normal geladen, wenn Secure Web geschlossen und erneut geöffnet wird. [CXM-60751]
- In Secure Mail für Android wird bei Konfiguration mit Microsoft Intune-Richtlinien nach der Authentifizierung ein leerer Bildschirm angezeigt. [CXM-61457]
- In Secure Hub für Android versuchen Apps mit deaktivierter Verschlüsselung, einen Verschlüsselungsschlüssel von Secure Hub abzurufen. [CXM-61459]
- Secure Mail für Android stürzt beim Start ab, wenn Intune-Unternehmensportal 5.0.4324.0 installiert ist. Weitere Informationen finden Sie in diesem Support Knowledge Center-Artikel. [CXM-62516]
- In Secure Hub für Android können Sie auf unternehmenseigenen Android Enterprise-Einzweckgeräten mit Android 7.1.1 keine Systemanwendungen verwenden. [CXM-63653]
- Wenn Sie in Secure Hub für Android mehrere Apps von Google Play als erforderliche Apps konfigurieren und sich dann registrieren, erhalten Sie nacheinander für jede App eine sofortige Aufforderung, sie zu installieren. [CXM-63654]

Bekannte Probleme in Version 19.3.0

Secure Hub für iOS

Es gibt keine bekannten Probleme in diesem Release.

Secure Hub für Android

- Wenn Sie in Secure Hub für Android gemeinsam genutzte Geräte registrieren, die Webclip-Richtlinie bereitstellen und Web- und SaaS-Apps hinzufügen, können Sie die Bereitstellung erfolgreich abschließen. Im App-Bestandsfenster der Citrix Endpoint Management-Konsole wird die Bereitstellung jedoch als fehlgeschlagen angezeigt. [CXM-57500]

- Wenn auf Android Enterprise-Geräten in der Standortrichtlinie eine Sperraktion für Geofence-Verletzungen festgelegt ist, fordert das Gerät Sie auf, einen neuen Code festzulegen, anstatt den vom System generierten Passcode zu verwenden. [CXM-60425]

Behobene Probleme in Version 19.3.0

Secure Hub für iOS

In diesem Release wurden keine Probleme behoben.

Secure Hub für Android

Das Sperren vollständig verwalteter Android Enterprise-Geräte mit der Sicherheitsaktion Mit Passcode sperren kann fehlschlagen, ohne dass eine entsprechende Fehlermeldung angezeigt wird. Um sicherzustellen, dass ein Gerät gesperrt wird, legen Sie Mit Passcode sperren zwei Mal fest. Das Gerät wird mit dem zweiten von Ihnen festgelegten Passcode gesperrt. [CXM-61095]

Bekannte Probleme in Version 19.3.0

Secure Hub für iOS

Es gibt keine bekannten Probleme in diesem Release.

Secure Hub für Android

- Wenn Sie in Secure Hub für Android gemeinsam genutzte Geräte registrieren, die Webclip-Richtlinie bereitstellen und Web- und SaaS-Apps hinzufügen, können Sie die Bereitstellung erfolgreich abschließen. Im App-Bestandsfenster der Citrix Endpoint Management-Konsole wird die Bereitstellung jedoch als fehlgeschlagen angezeigt. [CXM-57500]
- Wenn auf Android Enterprise-Geräten in der Standortrichtlinie eine Sperraktion für Geofence-Verletzungen festgelegt ist, fordert das Gerät Sie auf, einen neuen Code festzulegen, anstatt den vom System generierten Passcode zu verwenden. [CXM-60425]

Behobene Probleme in Version 19.3.0

Secure Hub für iOS

In diesem Release wurden keine Probleme behoben.

Secure Hub für Android

Das Sperren vollständig verwalteter Android Enterprise-Geräte mit der Sicherheitsaktion Mit Passcode sperren kann fehlschlagen, ohne dass eine entsprechende Fehlermeldung angezeigt wird. Um sicherzustellen, dass ein Gerät gesperrt wird, legen Sie Mit Passcode sperren zwei Mal fest. Das Gerät wird mit dem zweiten von Ihnen festgelegten Passcode gesperrt. [CXM-61095]

Bekannte Probleme in Version 19.2.0

In Version 19.2.0 gibt es keine bekannten Probleme.

Behobene Probleme in Version 19.2.0

Secure Hub für iOS

In Secure Hub für iOS wird bei der Abmeldung der Benutzer vom Secure Hub-Store wiederholt folgende SSL-Handshake-Fehlermeldung angezeigt: Timeout des Servers bei Netzwerkanfrage zum Abrufen von Apps. [CXM-61339]

Secure Hub für Android

- Die Dateirichtlinie für Android Enterprise nicht auf Android-Geräten im Arbeitsprofilmodus bereitgestellt. [CXM-61196]
- In Secure Hub für Android dauert die Anmeldeautorisierung für neue Benutzer auf freigegebenen Geräten lange. Wenn Sie sich als registrierter Benutzer abmelden und als neuer Benutzer anmelden, bleibt Secure Hub beim Ladevorgang hängen, bis Sie das Gerät neu starten. [CXM-61338]
- In Secure Hub für Android können Cloud-Kunden keine Android Enterprise-Geräte mit einem externen Identitätsanbieter registrieren. [CXM-61738]
- In Secure Hub für Android werden im COSU-Modus die App-Symbole überlappend angezeigt. [CXM-61740]
- In Secure Hub für Android mit aktiviertem Zertifikatpinning schlägt die Authentifizierung fehl und es wird der Bildschirm für erstmalige Benutzer angezeigt, wenn das Zertifikat mehrere alternative Antragstellernamen hat. [CXM-61933]

Bekannte Probleme in Version 19.1.5

- Wenn Sie in Secure Hub für Android das Kennwort aufgrund einer Änderung der Kennwortrichtlinie aktualisieren, werden die Apps mit Badges nicht auf Samsung Galaxy S8-Geräten angezeigt. [CXM-61177]

- In Secure Hub für Android wird die Dateirichtlinie für Android Enterprise nicht auf Geräten im Arbeitsprofilmodus bereitgestellt. [CXM-61196]

Behobene Probleme in Version 19.1.5

- Wenn sich Benutzer in Secure Hub für Android mit Secure PIN anmelden, wird ein VPN-Tunnel eingerichtet, in Secure Web jedoch keine Website geladen. Die Website wird jedoch normal geladen, wenn Secure Web geschlossen und erneut geöffnet wird. [CXM-58576]
- Wenn sich Benutzer in Secure Hub für Android mit Secure PIN anmelden, wird ein VPN-Tunnel eingerichtet, in Secure Web jedoch keine Website geladen. Die Website wird jedoch normal geladen, wenn Secure Web geschlossen und erneut geöffnet wird. [CXM-60751]
- Wenn Sie in Secure Hub für Android eine Protokollierung für die interne App TechXpert versuchen, startet Secure Hub neu und fordert eine erneute Authentifizierung an. [CXM-61310]

Bekannte Probleme in Version 19.1.0

Secure Hub für iOS

In Secure Hub für iOS werden bereitgestellte MDX-, Web- und SaaS-Apps im Bildschirm **Eigene Apps** angezeigt. Wenn Sie auf **Mehr** tippen, wird ein Dialogfeld mit den Optionen **Löschen** und **Abbrechen** im alten Format angezeigt. [CXM-60683]

Behobene Probleme in Version 18.12.0

- Auf für Android For Work registrierten Samsung Knox-Geräten, wird “Kennwort abgelaufen” wiederholt angezeigt, wenn die Kennwortrichtlinie auf einen Ablauf in einem oder zwei Tagen festgelegt ist. [CXM-59250]
- OnePlus 5T- Geräte können nicht per QR-Code für Android Enterprise registriert werden. [CXM-59288]

Behobene Probleme in Version 18.11.0

Secure Hub für iOS

- Auf Android-Geräten, die als gemeinsam genutztes Gerät registriert wurden, ist kein Single Sign-On möglich. Es wird folgende Fehlermeldung angezeigt: Ihre Unternehmensanmeldeinformationen können zurzeit nicht abgerufen werden. Die manuelle Anmeldung an ShareFile wird von der Verwaltungsrichtlinie blockiert. [CXM-58238]
- Auf unternehmenseigenen Einzweckgeräten können die Android-Lautstärkestufen nicht bearbeitet werden [CXM-58323]

Behobene Probleme in Version 18.10.5

- Wenn Sie den FIPS-Modus in XenMobile Server aktiviert haben, wird nach dem Update von Secure Hub für iOS auf Version 18.10.5 eine Fehlermeldung bezüglich der Verschlüsselung angezeigt, wenn Benutzer Apps öffnen. Informationen zur Entwicklung einer Lösung finden Sie in diesem Citrix Knowledge Center-Artikel. [CXM-56454]

Behobene Probleme in den Versionen 10.8.25 bis 18.10.6

- Die Secure Hub-Versionen 10.8.25 bis 18.10.6 (Android) enthalten keine bekannten Probleme. Die folgenden Probleme sind in Secure Hub behoben. Die Liste enthält Probleme mit MDX, die sich auf Secure Hub auswirken.

Behobene Probleme in Version 18.10.0

- Wenn die MVPN-Richtlinie in der EMS-Konsole deaktiviert ist, zeigt Secure Hub einen leeren Bildschirm an, wenn versucht wird, von Intune verwaltete Anwendungen zu öffnen. [CXM-56033, CXM-56086, CXM-54393, CXM-54823]

Behobene Probleme in Version 10.8.60

- Auf Samsung Galaxy Tab Active 2 SM-T395-Geräten schlägt die Sicherheitsaktion Full Wipe für Secure Hub für Android fehl, wenn Administratoren in XenMobile die Einschränkung zur Deaktivierung der Zurücksetzung auf Werkseinstellungen festlegen. [CXM-54452]
- Secure Hub für Android reagiert nicht mehr bei der Registrierung von Geräten, wenn die VPN-Richtlinie konfiguriert ist und die Citrix SSO-Anwendung nicht auf dem Gerät installiert ist. Die App reagiert wieder, wenn Sie auf **Zurück** tippen oder die App neu starten. [CXM-54627]
- Secure Hub für Android stürzt bei der Registrierung im Gerätebesitzer-Modus in einer Android Enterprise-Umgebung ab. [CXM-55008]
- Nachdem Benutzer eine gültige PIN für Secure Hub für iOS eingegeben haben, fordert Secure Hub die Benutzer wiederholt zur Eingabe der PIN auf. [CXM-55047]
- Secure Hub für Android stürzt bei der Registrierung im Profilbesitzer-Modus in einer Android Enterprise-Umgebung ab. [CXM-55076]
- Bei Verwendung von Android Enterprise in Secure Hub für Android wird Google Chrome standardmäßig installiert. [CXM-55232]
- Beim Upgrade von Secure Hub für iOS auf Version 10.8.55 werden keine bestehenden oder neuen Anmeldungen von iOS-Geräten zugelassen. [CXM-55267]

Behobene Probleme in Version 10.8.55

- Benutzer können sich nicht bei Secure Hub anmelden, um sich bei Android for Work-Konten zu registrieren, wenn sich die G Suite-Anmeldeinformationen von den Anmeldeinformationen in Endpoint Management unterscheiden. [CXM-53956]

Behobene MDX-Probleme in Version 10.8.55

- Bei Enterprise-Apps können Verbindungsprobleme mit internen Ressourcen auftreten, wenn der bevorzugte VPN-Modus auf SecureBrowse festgelegt ist. [CXM-52309]
- Apps, die android.support.multidex.MultiDexApplication oder android.app.Application als ihre Anwendungsklasse angeben, können im Secure Browse-Modus keine Verbindung zu internen Netzwerken herstellen. [CXM-53126]
- Auf Android-Geräten werden mehrere Zertifikate generiert und Zertifikate werden vor ihrem Ablaufdatum widerrufen. [CXM-53428]

Bekanntes Problem in Version 10.8.55

- Nach dem Entfernen Ihres Secure Hub-Kontos vom Gerät schlägt die MDM-Neuregistrierung fehl. [CXM-54142]

Bekanntes Problem in Version 10.8.50

- In Secure Hub für Android können Benutzer keine Weblink-Verknüpfungen hinzufügen. [XMHELP-952]

Behobene Probleme in Version 10.8.35

- Unter Android O werden durch Richtlinien erstellte Verknüpfungen nicht auf dem Homebildschirm von Geräten angezeigt. Dies ist in Android O beabsichtigt. [CXM-35460]
- Unter Android wird Secure Hub nach einer gewissen Inaktivitätsphase nicht auf Samsung-Tablets geöffnet. [CXM-50797]
- In Secure Hub für Android können Sie die Push-Richtlinie nicht auf Samsung Knox-Geräten bereitstellen. [CXM-50869]
- In Secure Hub für iOS tritt gelegentlich das folgende Problem auf: Nachdem Benutzer ihr Active Directory-Kennwort geändert haben, müssen sie ihre PIN weiterhin in einer Schleife eingeben. [CXM-50224]

Behobene Probleme in Version 10.8.25

- Bei iOS-Cordova-Apps von Drittanbietern, die mit dem MDX Toolkit Version 10.7.20 umschlossen wurden, wird auf iOS-Geräten nach Aktivieren der Richtlinie **Bildschirminhalt verbergen** anstelle eines PIN-Bildschirms ein schwarzer Bildschirm angezeigt. [CXM-48471]
- Auf Zebra T51-Geräten mit Android 7 können Benutzer die Citrix Launcher-App nicht installieren. [CXM-50621]

Behobene Probleme in Version 10.8.20

- Wenn Benutzer ihre Android-Geräte auf Version 8 (Oreo) aktualisieren, können sie keine Enterprise- oder APK-Apps aus dem über Endpoint Management bereitgestellten App-Store installieren. Das Problem besteht selbst dann, wenn Benutzer die Installation von Apps von Drittanbietern aktivieren. Das Problem ist nicht auf Samsung-Geräte beschränkt. [CXM-50401]

Behobene Probleme in Version 10.8.15

- Secure Hub für Android stürzt beim Abrufen der Standortdaten auf Geräten mit Android O ab. [CXM-47893]

Behobene Probleme in Version 10.8.10

- Auf Android-Geräten: Wenn mehrere Apps nicht automatisch installiert werden oder Benutzer nicht auf **Installieren** klicken, werden die Apps trotzdem weiter heruntergeladen. Das Resultat ist eine hohe Datennutzung. [CXM-46404]
- Auf Geräten mit Android 7 oder höher: Wenn Sie als Sicherheitsaktion eine Sperre mit Kennwort von XenMobile Server an das Gerät senden, wird das Gerät gesperrt. Das Gerätekennwort ändert sich jedoch nicht, wenn Benutzer bereits ein Kennwort für den Sperrbildschirm haben. Benutzer können dann den ursprünglichen Passcode zum Entsperren des Geräts verwenden. [CXM-47908]

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.

Szenarios für Authentifizierungsaufforderungen

April 26, 2019

In verschiedenen Szenarios werden Benutzer zur Authentifizierung bei Secure Hub durch Eingabe ihrer Anmeldeinformationen auf ihrem Gerät aufgefordert.

Die Szenarios hängen von den folgenden Faktoren ab:

- MDX-App-Richtlinie und Konfiguration der Clienteigenschaft in den Einstellungen der Endpoint Management-Konsole.
- Ob die Authentifizierung offline oder online erfolgen muss (Netzwerkverbindung mit Endpoint Management erforderlich).

Auch die Art der Anmeldeinformationen die Benutzer eingeben – Active Directory-Kennwort, Citrix PIN oder Passcode, Einmalkennwort, Authentifizierung per Fingerabdruck (in iOS Touch ID genannt) –, hängen von Typ und Häufigkeit der benötigten Authentifizierung ab.

Nachfolgend werden zunächst die Szenarios vorgestellt, die zu einer Authentifizierungsaufforderung führen.

- **Neustart des Geräts:** Wenn Benutzer ihr Gerät neu starten, müssen sie sich neu bei Secure Hub authentifizieren.
- **Offline/Inaktivität (Timeout):** Wenn die MDX-Richtlinie “App-Passcode” aktiviert ist (was standardmäßig der Fall ist), wird die Endpoint Management-Clienteigenschaft “Inaktivitätstimer” relevant. Der Inaktivitätstimer legt die Zeitdauer fest, die ohne Benutzeraktivität an einer der Apps, die den sicheren Container verwenden, verstreichen darf.

Wenn der Inaktivitätstimer abläuft, muss sich der Benutzer bei dem sicheren Container auf dem Gerät neu authentifizieren. Wenn ein Benutzer beispielsweise sein Gerät unbeaufsichtigt lässt, kann mit dem Gerät nach Ablauf des Inaktivitätstimer nicht von anderen Personen auf vertrauliche Daten im Container zugegriffen werden. Die Clienteigenschaft “Inaktivitätstimer” wird in der Endpoint Management-Konsole festgelegt. Der Standardwert ist 15 Minuten. Die Kombination aus App-Passcode = **Ein** und der Clienteigenschaft “Inactivity Timer” ist wahrscheinlich das häufigste Szenario für Authentifizierungsaufforderungen.

- **Abmelden von Secure Hub:** Wenn Benutzer sich von Secure Hub abmelden, müssen sie sich beim nächsten Zugriff auf Secure Hub oder eine MDX-App neu authentifizieren, wenn gemäß MDX-Passcode-Richtlinie und Status des Inaktivitätstimers ein Passcode erforderlich ist.
- **Maximale Offlinezeit:** Dieses Szenario ist App-spezifisch, da es über MDX-Richtlinien für jede App gesteuert wird. Die MDX-Richtlinie “Maximale Offlinezeit” hat eine Standardeinstellung von 3 Tagen. Wenn der zulässige Zeitraum abläuft, den eine App ohne Onlineauthentifizierung bei Secure Hub ausgeführt werden darf, wird ein Check-in bei Endpoint Management erforderlich, um App-Anspruch zu bestätigen und die Richtlinien zu aktualisieren. Bei diesem Check-in löst die App bei Secure Hub die Aufforderung zur Onlineauthentifizierung aus. Der Benutzer muss sich neu authentifizieren, bevor er Zugriff auf die MDX-App erhält.

Zwischen den MDX-Richtlinien “Maximale Offlinezeit” und “Aktives Abfrageintervall” besteht folgende Beziehung:

- Das aktive Abfrageintervall ist der Zeitraum, in dem eine App bei Endpoint Management eincheckt, um Sicherheitsaktionen auszuführen, wie z. B. App sperren und löschen. Außerdem prüft die App zu diesem Zeitpunkt auf aktualisierte App-Richtlinien.
- Nach einer erfolgreichen Prüfung auf Richtlinien gemäß dem aktiven Abfrageintervall wird der Timer “Maximale Offlinezeit” zurückgesetzt.

Beide Check-in-Vorgänge bei Endpoint Management (für “Aktives Abfrageintervall” und “Maximale Offlinezeit”) erfordern einen gültigen Citrix Gateway-Token auf dem Gerät. Wenn das Gerät einen gültigen Citrix Gateway-Token hat, ruft die App ohne Unterbrechung für den Benutzer neue Richtlinien von Endpoint Management ab. Wenn die App kein Citrix Gateway-Token hat, erfolgt ein Wechsel zu Secure Hub, wo eine Aufforderung zur Authentifizierung bei Secure Hub angezeigt wird.

Auf Android-Geräten werden Secure Hub-Aktivitätsseiten direkt über der aktuellen App geöffnet. Auf iOS-Geräten muss Secure Hub stattdessen in den Vordergrund treten, wodurch die aktuelle App vorübergehend verdeckt wird.

Nach der Eingabe von Anmeldeinformationen durch die Benutzer wechselt Secure Hub zurück zur ursprünglichen App. In diesem Fall, wenn Sie zwischengespeicherte Active Directory-Anmeldeinformationen zulassen oder ein Clientzertifikat konfiguriert haben, können Benutzer eine PIN, ein Kennwort oder die Authentifizierung per Fingerabdruck verwenden. Ist dies nicht der Fall, müssen die Benutzer ihre vollständigen Active Directory-Anmeldeinformationen eingeben.

Der Citrix ADC-Token kann aufgrund einer Inaktivität der Citrix Gateway-Sitzung oder einer erzwungenen Sitzungstimeoutrichtlinie (siehe nachfolgende Liste der Citrix Gateway-Richtlinien) ungültig werden. Benutzer können die App jedoch weiter verwenden, wenn sie sich wieder bei Secure Hub anmelden.

- **Citrix Gateway-Sitzungsrichtlinien:** Zwei Citrix Gateway-Richtlinien beeinflussen, wann Benutzer zur Authentifizierung aufgefordert werden. In diesen Fällen erfolgt die Authentifizierung zum Erstellen einer Onlinesitzung mit Citrix ADC zur Herstellung einer Verbindung mit Endpoint Management.
  - **Session time-out:** Die Citrix ADC-Sitzung für Endpoint Management wird getrennt, wenn während eines vorgegebenen Zeitraums keine Netzwerkaktivität stattfindet. Der Standardwert ist 30 Minuten. Wenn Sie den Citrix Gateway-Assistenten verwenden, um die Richtlinie zu konfigurieren, ist der Standardwert jedoch 1440 Minuten. Die Benutzer werden zur Authentifizierung für die Verbindung mit dem Unternehmensnetzwerk aufgefordert.
  - **Forced time-out:** Wird diese Richtlinie **aktiviert**, dann werden Citrix ADC-Sitzungen mit Endpoint Management getrennt, wenn der festgelegte Zeitraum abläuft. Durch das erzwungene Timeout wird eine erneute Authentifizierung nach dem festgelegten

Zeitraum obligatorisch. Die Benutzer werden bei der nächsten Verwendung zur Authentifizierung für die Verbindung mit dem Unternehmensnetzwerk aufgefordert. Die Standardeinstellung ist **Aus**. Wenn Sie den Citrix Gateway-Assistenten verwenden, um die Richtlinie zu konfigurieren, ist der Standardwert jedoch 1440 Minuten.

Arten von Anmeldeinformationen

In den Abschnitten oben wurde beschrieben, wann die Benutzer zur Authentifizierung aufgefordert werden. In diesem Abschnitt wird erläutert, welche Art von Anmeldeinformationen sie eingeben müssen. Es sind verschiedene Authentifizierungen erforderlich, um Zugriff auf verschlüsselte Daten auf einem Gerät zu erhalten. Beim ersten Entsperren eines Geräts wird dessen *primärer Container* entsperrt. Wird dieser anschließend wieder gesperrt, muss für den erneuten Zugriff ein *sekundärer Container* entsperrt werden.

> Hinweis:
>
> Der Ausdruck *verwaltete App* bezieht sich in diesem Artikel auf Apps, die mit dem MDX Toolkit umschlossen wurden und für die die MDX-Richtlinie "App-Passcode" standardmäßig aktiviert ist und die Clienteigenschaft des Inaktivitätstimers richtig genutzt wird.

Die Art der Anmeldeinformationen hängen von folgenden Bedingungen ab:

- **Entsperren des primären Containers:** Active Directory-Kennwort, Citrix PIN oder -Passcode, Einmalkennwort, Touch-ID oder Fingerabdruck-ID sind erforderlich, um den primären Container zu entsperren.
  - Unter iOS, wenn Benutzer Secure Hub oder eine verwaltete App zum ersten Mal nach der Installation auf dem Gerät öffnen
  - Unter iOS, wenn Benutzer das Gerät neu starten und dann Secure Hub öffnen
  - Unter Android, wenn Benutzer eine verwaltete App öffnen und Secure Hub nicht ausgeführt wird
  - Unter Android, wenn Benutzer Secure Hub neu starten (egal aus welchem Grund, einschließlich Geräteneustarts)
- **Entsperren des sekundären Containers:** Authentifizierung per Fingerabdruck (sofern konfiguriert), Citrix PIN oder Passcode oder Active Directory-Anmeldeinformationen sind zum Entsperren des sekundären Containers erforderlich.
  - Wenn Benutzer eine verwaltete App nach Ablaufen des Inaktivitätstimers öffnen
  - Wenn Benutzer sich von Secure Hub abmelden und anschließend eine verwaltete App öffnen

Unter folgenden Bedingungen sind Active Directory-Anmeldeinformationen zum Entsperren beider Container erforderlich:

- Wenn Benutzer den Passcode ändern, der ihrem Unternehmenskonto zugeordnet ist.

- Wenn Sie in den Clienteigenschaften in der Endpoint Management-Konsole die Citrix PIN nicht aktiviert haben: ENABLE_PASSCODE_AUTH und ENABLE_PASSWORD_CACHING.
- Wenn die NetScaler Gateway-Sitzung endet. Dies kann in folgenden Situationen geschehen: Ablauf des Timers der Richtlinie "Session time-out" oder "Forced time-out", wenn auf dem Gerät keine Anmeldeinformationen zwischengespeichert werden oder das Gerät kein Clientzertifikat hat.

Ist die Authentifizierung per Fingerabdruck aktiviert, können Benutzer können sich per Fingerabdruck anmelden, wenn Offlineauthentifizierung aufgrund von Inaktivität in der App erforderlich ist. Benutzer müssen immer noch eine PIN eingeben, wenn sie sich zum ersten Mal bei Secure Hub anmelden und wenn sie das Gerät neu starten. Informationen zum Aktivieren der Authentifizierung per Fingerabdruck finden Sie unter Authentifizierung per Touch ID bzw. Fingerabdruck.

Im folgenden Flussdiagramm ist der Entscheidungsfluss dargestellt, durch den bestimmt wird, welche Anmeldeinformationen ein Benutzer für die Authentifizierung eingeben muss.

Secure Hub-Bildschirmwechsel

Im Zusammenhang mit der Authentifizierung ist auch der Wechsel der Anzeige von einer App zu Secure Hub und zurück zu bedenken. Bei dem Wechsel wird eine Meldung angezeigt, die der Benutzer bestätigen muss. Eine Authentifizierung ist nicht erforderlich. Die Situation tritt nach dem Check-in bei Endpoint Management auf, wie in den MDX-Richtlinien "Aktives Abfrageintervall" und "Maximale Offlinezeit" angegeben, wenn Endpoint Management aktualisierte Richtlinien erkennt, die dem Gerät per Push über Secure Hub bereitgestellt werden müssen.

VPN-Installation unter iOS

March 9, 2019

Auf Geräten mit iOS 10 und höher wird das Secure Hub-VPN zum sicheren Austausch lokaler Daten zwischen Secure Hub und MDX-Apps verwendet. Das Secure Hub-VPN wird auf Geräten mit iOS 10 und höher ausgeführt. Das Secure Hub-VPN bietet die optimale Benutzererfahrung, da Secure Hub und MDX-Apps problemlos über das VPN kommunizieren können.

Das Secure Hub-VPN funktioniert für Apps, die von einem Apple Enterprise Developer-Konto ("team id"), von Citrix Zertifikaten, Unternehmenszertifikaten oder Zertifikaten unabhängiger Softwarehersteller signiert sind.

Das Secure Hub-VPN wird standardmäßig auf iOS 10-Geräten verwendet. Wenn das Secure Hub-VPN nicht auf iOS 10-Geräten ausgeführt wird, verwendet MDX den freigegebenen iOS-Schlüsselbund für die sichere Datenfreigabe. Für die Methode mit dem freigegebenen iOS-Schlüsselbund müssen alle

Apps mit demselben Zertifikat signiert sein, damit der Zugriff auf den angegebenen freigegebenen Schlüsselbund für die iOS “team id” möglich ist. Wenn eine App nicht mit dem gleichen Zertifikat signiert ist wie die von Citrix signierte Secure Hub-App, wechselt die App u. U. zu Secure Hub, um die die erforderlichen Informationen abzurufen.

Das Secure Hub-VPN ist nur für Citrix Endpoint Management Enterprise und Nur-MAM-Bereitstellungen verfügbar. Das Secure Hub-VPN kann nicht in Nur-Endpoint Management-MDM-Umgebungen verwendet werden und bei Nur-MDM-Registrierungen wird es nicht installiert.

Das Secure Hub-VPN wird für die Kommunikation zwischen Secure Hub und mobile Produktivitätsapps verwendet. Es filtert oder überwacht nicht den Datenverkehr auf dem Gerät und ist vom MDX Micro VPN unabhängig.

> Hinweis:
>
> Citrix empfiehlt, das Secure Hub-VPN in Umgebungen, in denen es standardmäßig aktiviert ist, aktiviert zu lassen.
>
> Da iOS nicht zulässt, dass mehr als ein VPN-Client gleichzeitig auf einem iOS-Gerät ausgeführt wird, müssen Sie aber auf folgenden Fall achten. Das Secure Hub-VPN kann nicht verwendet werden, wenn eine andere VPN-App (z. B. Cisco AnyConnect oder Citrix VPN) auf dem iOS-Gerät verwendet werden muss, um ein VPN auf Geräteebene einzurichten. Sie können für iOS ein Pro-App-VPN einrichten, auch wenn Secure Hub VPN nicht deaktiviert ist. Die App, die das iOS-Pro-App-VPN verwendet, stellt eine Pro-App-VPN-Verbindung her, wenn die App im Vordergrund ist.
>
> Informationen zum Deaktivieren der Secure Hub-VPNs finden Sie im folgenden Abschnitt in diesem Artikel. Wenn das Secure Hub-VPN deaktiviert ist, wechseln verwaltete Apps u. U. häufiger zu Secure Hub.

Deaktivieren und Reaktivieren des Secure Hub-VPN in Endpoint Management

Das Secure Hub-VPN wird standardmäßig aktiviert, wenn Secure Hub 10.3.10 und höher auf einem iOS 10-Gerät erstmals verwendet wird.

Zum Deaktivieren des Secure Hub-VPNs und Konfigurieren der iOS-Geräte in der Bereitstellung zur Verwendung eines freigegebenen Schlüsselbunds führen Sie die folgenden Schritte aus:

1. Navigieren Sie in der Endpoint Management-Konsole zu **Einstellungen > Client > Clienteigenschaften**.
2. Erstellen Sie auf der Seite **Clienteigenschaften** eine benutzerdefinierte Eigenschaft namens **ENABLE_NETWORK_EXTENSION** und legen Sie den Wert auf 0 fest.

   Zum Reaktivieren des Secure Hub-VPNs legen Sie den Wert für **ENABLE_NETWORK_EXTENSION** auf 1 fest.

Installieren des Secure Hub-VPNs auf einem Clientgerät

In zwei Fällen wird das Secure Hub-VPN installiert: nach der Installation von Secure Hub 10.3.10 auf einem iOS 10-Gerät oder wenn ein Gerät mit Secure Hub 10.3.10 auf iOS 10 aktualisiert wird.

Benutzern wird diese Informationsmeldung angezeigt.

Danach werden Benutzer in einer iOS-Meldung um die Erlaubnis zum Hinzufügen von VPN-Konfigurationen gebeten. Diese Meldung wird nur einmal, bei der ersten Installation des VPNs angezeigt. Wenn Benutzer Secure Hub erneut öffnen, wird sie nicht angezeigt.

Die Meldung auf diesem Bildschirm kann nicht angepasst werden. Sie ist ein iOS-Standarddialogfeld, das für alle VPN-Installationen verwendet wird.

Auf dem Bestätigungsbildschirm für das Hinzufügen der VPN-Konfiguration: Wenn Benutzer **Nicht zulassen** wählen, werden sie in einer weiteren Meldung davon unterrichtet, dass sie für den Zugriff auf Secure Hub das VPN installieren müssen.

Ausführen des Secure Hub-VPNs auf einem Clientgerät

Wenn das Secure Hub-VPN ordnungsgemäß ausgeführt wird, wird der Text **Verbinden** in den iOS-Einstellungen unter **Allgemein > VPN** angezeigt.

Dies ist normal und bedeutet, dass die MDX-Freigabe und -Kommunikationsmethoden normal funktionieren. Es ist keine Aktion erforderlich, wenn Benutzer diese Meldung sehen.

Registrieren von Geräten mit abgeleiteten Anmeldeinformationen

January 25, 2019

Abgeleitete Anmeldeinformationen bieten eine starke Authentifizierung für mobile Geräte. Sie werden von einer Smartcard abgeleitet und residieren auf einem Mobilgerät anstelle einer Karte. Bei der Smartcard kann es sich um eine PIV-Karte (Personal Identity Verification) oder eine CAC-Karte (Common Access Card) handeln.

Bei den abgeleiteten Anmeldeinformationen handelt es sich um ein Registrierungszertifikat, das die Benutzer-ID, z. B. den UPN, enthält. Die vom Anbieter erhaltenen Anmeldeinformationen speichert Endpoint Management in einem sicheren Tresor auf dem Gerät.

Abgeleitete Anmeldeinformationen können von Endpoint Management für die Registrierung von iOS-Geräten verwendet werden. Wenn Endpoint Management für abgeleitete Anmeldeinformationen konfiguriert ist, unterstützt es keine Registrierungseinladungen oder andere Registrierungsmodi für iOS-

Geräte. Sie können jedoch denselben Endpoint Management-Server zur Registrierung von Android-Geräten über Registrierungseinladungen oder andere Registrierungsmodi verwenden.

Schritte zur Geräteregistrierung beim Verwenden von abgeleiteten Anmeldeinformationen

Die Registrierung erfordert, dass Benutzer ihre Smartcard in einen an den Desktop angeschlossenen Smartcardleser einlegen.

1. Der Benutzer installiert Secure Hub und die App des Anbieters für abgeleitete Anmeldeinformationen. In diesem Beispiel ist die App des Identitätsanbieters Intercede MyID Identity Agent.
2. Der Benutzer startet Secure Hub. Wenn sie dazu aufgefordert werden, geben Benutzer den vollqualifizierten Domänennamen für Endpoint Management ein und klicken auf **Weiter**. Die Registrierung wird in Secure Hub gestartet. Wenn der Endpoint Management abgeleitete Anmeldeinformationen unterstützt, fordert Secure Hub den Benutzer auf, eine Citrix-PIN zu erstellen.
3. Der Benutzer folgt den Anweisungen zum Aktivieren der Smartcard-Anmeldeinformationen. Ein Begrüßungsbildschirm wird angezeigt, gefolgt von einer Eingabeaufforderung zum Scannen eines QR-Codes.
4. Der Benutzer legt die Smartcard in den Smartcardleser ein, der an den Desktop angeschlossen ist. In der Desktop-App wird dann ein QR-Code angezeigt und der Benutzer zum Scannen des Codes mit dem Mobilgerät aufgefordert.

   Der Benutzer gibt bei entsprechender Aufforderung seine Secure Hub-PIN ein.

Nach der Authentifizierung der PIN lädt Secure Hub die Zertifikate herunter. Der Benutzer folgt anschließend den Anweisungen zum Abschließen der Registrierung.

Führen Sie zum Anzeigen von Geräteinformationen in der Endpoint Management-Konsole einen der folgenden Schritte aus:

- Gehen Sie zu **Verwalten > Geräte** und wählen Sie ein Gerät zum Anzeigen eines Befehlsfelds aus. Klicken Sie auf **Mehr anzeigen**.
- Gehen Sie zu **Analysieren > Dashboard**.

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