Secure Mail

Contents

Überblick über Secure Mail

April 3, 2019

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.

Secure Mail ist mit folgender Software kompatibel:

- Exchange Server 2019 Kumulatives Update 1
- Exchange Server 2016 Kumulatives Update 12
- Exchange Server 2013 Kumulatives Update 22
- Exchange Server 2016 Kumulatives Update 11
- Exchange Server 2016 Kumulatives Update 10
- Exchange Server 2016 Kumulatives Update 9
- Exchange Server 2016 Kumulatives Update 8
- Exchange Server 2013 Kumulatives Update 21
- Exchange Server 2013 Kumulatives Update 19
- Exchange Server 2010 SP3 Update Rollup 26
- Exchange Server 2010 SP3 Update Rollup 24
- Exchange Server 2010 SP3 Update Rollup 19
- Exchange Server 2010 SP3 Update Rollup 22
- IBM Domino Mail Server version 9.0.1 FP10 HF197
- IBM Domino Mail Server Version 9.0.1 FP9
- IBM Lotus Notes Traveler, Version 9.0.1.21
- IBM Lotus Notes Traveler, Version 9.0.1.9
- 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 ausge-

führter 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.

Neue Features in Secure Mail

May 23, 2019

Die folgenden Features sind neu in Secure Mail:

Secure Mail 19.5.0

Secure Mail für Android

Verwalten von Feeds

In Secure Mail für Android können Sie Ihre **Feeds**-Karte entsprechend Ihren Anforderungen organisieren.

Weitere Informationen zum Verwalten Ihrer Feeds finden Sie unter Verwalten von Feeds.

Automatische Synchronisierung des Ordners “Entwürfe”

In Secure Mail für Android wird der Ordner “Entwürfe” automatisch synchronisiert, sodass Ihre Entwürfe auf allen Geräten verfügbar sind. Dieses Feature ist auf Geräten mit Office 365 oder Exchange Server 2016 und höher verfügbar.

> Hinweis:
>
> Wenn Ihr Entwurf in Secure Mail Anlagen enthält, werden diese nicht mit dem Server synchronisiert.

Was ist neu in früheren Releases

Secure Mail für Android 19.4.6, 19.4.5 und 19.3.5

Diese Releases enthalten Leistungsverbesserungen und Fehlerbehebungen.

Informationen zu behobenen und bekannten Problemen finden Sie unter Bekannte und behobene Probleme.

Secure Mail 19.3.0

Ab diesem Release unterstützt Secure Mail die folgenden Server:

- Exchange Server 2019 Kumulatives Update 1
- Exchange Server 2016 Kumulatives Update 12
- Exchange Server 2013 Kumulatives Update 22
- Exchange Server 2010 SP3 Update Rollup 26

Weitere Informationen und die vollständige Liste der kompatiblen Server für Secure Mail finden Sie unter Überblick über Secure Mail.

Secure Mail für iOS

Verwalten von Feeds. In Secure Mail für iOS können Sie Ihre **Feeds**-Karte entsprechend Ihren Anforderungen organisieren.

> Hinweis:
>
> Dieses Feature ist auf iPads nicht verfügbar.

Weitere Informationen zum Verwalten Ihrer Feeds finden Sie unter Verwalten von Feeds.

Secure Mail für iOS und Android

Interne Domänen. Sie können E-Mail-Empfänger identifizieren und bearbeiten, die zu externen Organisationen gehören. Um dieses Feature zu verwenden, müssen Sie die Richtlinie **Interne Domänen** in Citrix Endpoint Management aktiviert haben.

Wenn Sie eine E-Mail erstellen, beantworten oder weiterleiten, werden externe Empfänger in der Adressenliste markiert. Ein **Kontakte**-Warnsymbol wird links unten auf dem Bildschirm angezeigt. Tippen Sie auf das Symbol **Kontakte**, um die Adressenliste zu ändern.

Weitere Hinweise zu internen Domänen finden Sie unter Interne Domänen.

Ergonomische Verbesserungen. Die Aktionstasten wurden vom oberen Bildschirmrand nach unten verschoben, um den Zugriff zu erleichtern. Diese Änderung betrifft die Bildschirme **Posteingang**, **Kalender** und **Kontakte**.

> Hinweis:
>
> In Android-Geräten wurden die Bildschirme **Posteingang** und **Kalender** geändert.

Weitere Hinweise zu ergonomischen Verbesserungen finden Sie unter Ergonomische Verbesserungen.

Secure Mail 19.2.0

Secure Mail für iOS

Secure Mail 19.2.0 enthält Leistungsverbesserungen und Fehlerbehebungen.

Informationen zu behobenen und bekannten Problemen finden Sie unter Bekannte und behobene Probleme.

Secure Mail für Android

- **Verbesserungen für Kontakte.** Wenn Sie in Secure Mail für Android auf **Kontakte** tippen und einen Kontakt auswählen, werden die Details dieses Kontakts auf der Registerkarte **Kontakt** angezeigt. Wenn Sie auf die Registerkarte **Organisation** tippen, werden Angaben zur Organisationshierarchie wie **VORGESETZTE(R)**, **DIREKTE MITARBEITER** und **KOLLEGEN** angezeigt. Wenn Sie rechts oben auf dem Bildschirm auf das Symbol "Mehr" tippen, werden die folgenden Optionen angezeigt:
  - **An E-Mail anfügen**
  - **Freigeben**
  - **Löschen**

  Tippen Sie auf der Registerkarte**Organisation** rechts neben **VORGESETZTE(R)**, **DIREKTE MITARBEITER** oder **KOLLEGEN** auf das Symbol "Mehr", um eine neue E-Mail oder eine neue Kalendereinladung zu erstellen. Die Angaben aus **VORGESETZTE(R)**, **DIREKTE MITARBEITER** oder **KOLLEGEN** werden automatisch in das Feld **An:** der E-Mail oder des Kalendereereignisses eingefügt.

  Voraussetzungen:

  Exchange-Webdienste (EWS) muss auf dem Exchange Server aktiviert sein.

  Die angezeigten Kontaktdetails basieren auf den aus Active Directory abgerufenen Organisationsdetails: Damit die richtigen Details für Ihre Kontakte angezeigt werden, muss Ihr Administrator die Organisationshierarchie in Active Directory konfiguriert haben.

  > Hinweis:
  >
  > Das Feature wird von IBM Lotus Notes-Servern nicht unterstützt.

- **Netzwerkzugriffsrichtlinie**. In Secure Mail für Android gibt es für die MDX-Richtlinie "Netzwerkzugriff" die neue Option **Tunnel - Web-SSO**. Mit dieser Richtlinie können Sie den internen Datenverkehr über Secure Browse und die Secure Ticket Authority (STA) parallel tunneln. Sie können außerdem Secure Browse-Verbindungen für Authentifizierungsdienste wie NTLM, Okta und Kerberos zulassen. Wenn Sie die STA erstmals konfigurieren, müssen Sie der Richtlinie "Hintergrundnetzwerkdienste" einzelne FQDNs und Ports von Dienstadressen hinzufügen. Wenn Sie aber die Option **Tunnel - Web-SSO** konfigurieren, ist dies nicht erforderlich.

Aktivieren der Richtlinie für Secure Mail für Android in der Citrix Endpoint Management-Konsole:

1. Laden Sie die MDX-Datei für Android herunter und verwenden Sie sie. Weitere Informationen finden Sie in den Schritten unter Funktionsweise von mobilen Apps und MDX-Apps.
2. Klicken Sie für die Netzwerkzugriffsrichtlinie auf die Option **Tunnel - Web-SSO**. Weitere Informationen finden Sie unterApp-Netzwerkzugriff

Secure Mail für iOS 19.1.6

Dieses Release enthält Leistungsverbesserungen und Fehlerbehebungen.

Secure Mail 19.1.5

Ab diesem Release unterstützt Secure Mail die folgenden Server:

- Exchange Server 2016 Kumulatives Update 11
- Exchange Server 2010 SP3 Update Rollup 24

Weitere Informationen und die vollständige Liste der kompatiblen Secure Mail-Server finden Sie unter Überblick über Secure Mail.

Secure Mail 19.1.0

Secure Mail für iOS

- **Verbesserungen für Kontakte.** Wenn Sie in Secure Mail für iOS auf **Kontakte** tippen und einen Kontakt auswählen, werden die Details dieses Kontakts auf der Registerkarte **Kontakt** angezeigt. Wenn Sie auf die Registerkarte **Organisation** tippen, werden Angaben zur Organisationshierarchie wie **Vorgesetzte(r)**, **Direkte Mitarbeiter** und **Kollegen** angezeigt. Wenn Sie rechts oben auf dem Bildschirm auf das Symbol “Mehr” tippen, werden die folgenden Optionen angezeigt:

  - Bearbeiten
  - Zu VIPs hinzufügen
  - Abbrechen

  Tippen Sie auf der Registerkarte **Organisation** rechts neben **Vorgesetzte(r)**, **Direkte Mitarbeiter** oder **Kollegen** auf das Symbol “Mehr”. Mit dieser Aktion können Sie eine neue E-Mail oder ein neues Kalendereereignis erstellen. Die Angaben aus **Vorgesetzte(r)**, **Direkte Mitarbeiter** oder **Kollegen** werden automatisch in das Feld **An:** der E-Mail oder des Kalendereereignisses eingefügt. Danach können Sie die E-Mail verfassen und senden.

  Voraussetzungen:

Exchange-Webdienste (EWS) muss auf dem Exchange Server aktiviert sein.

Die angezeigten Kontaktdetails basieren auf den aus Active Directory abgerufenen Organisationsdetails (Outlook-Kontakt). Damit die richtigen Details für Ihre Kontakte angezeigt werden, muss Ihr Administrator die Organisationshierarchie in Active Directory konfiguriert haben.

> Hinweis:
>
> Das Feature wird von IBM Lotus Notes-Servern nicht unterstützt.

- **Exportieren Sie Zeit und Ort einer Besprechung in Ihren nativen Kalender.** In Secure Mail für iOS enthält die MDX-Richtlinie **Kalender exportieren** den neuen Wert **Besprechungszeit, Ort**. Durch diese Verbesserung können Sie Zeit und Ort der Besprechung von Secure Mail-Kalenderereignissen in Ihren nativen Kalender exportieren.
- Secure Mail für iOS unterstützt umfangreiche Push-Benachrichtigungen bei Setups mit Microsoft Enterprise Mobility + Security (EMS)/Intune mit moderner Authentifizierung (O365).

  Stellen Sie zum Aktivieren von Benachrichtigungen mit Rich-Inhalt sicher, dass die folgenden Voraussetzungen erfüllt sind:

  - **Pushbenachrichtigungen** müssen in der Endpoint Management-Konsole auf “EIN” festgelegt sein.
  - Die Richtlinie **Netzwerkzugriff** muss auf **Uneingeschränkt** festgelegt sein.
  - Die Richtlinie **Benachrichtigungen bei gesperrtem Bildschirm steuern** ist auf **Zulassen** oder **E-Mail-Absender oder Ereignistitel** festgelegt.
  - Navigieren Sie zu **Secure Mail** > **Einstellungen** > **Benachrichtigungen** und aktivieren Sie **E-Mail-Benachrichtigungen**.
- Secure Mail-Benutzer können die Zoom-App verwenden, um an Besprechungen teilzunehmen. Weitere Informationen zum Konfigurieren der erforderlichen Richtlinien zur Verwendung der Zoom-App finden Sie unter Teilnehmen an Besprechungen vom Kalender aus.
- Dieses Release bietet Unterstützung für iPad Pro 11” und iPad Pro 12,9”.

Secure Mail für Android

- **Verbesserung für Anlagen.** Die Anzeige von Anlagen wurde in Secure Mail für Android vereinfacht. Unwesentliche Schritte wurden zur Verbesserung der Benutzererfahrung entfernt, während vorhandene Optionen aus früheren Releases beibehalten wurden.

  Sie können Anlagen in der Secure Mail-App anzeigen. Die Anlage wird direkt geöffnet (wenn sie mit Secure Mail angezeigt werden kann) oder es wird eine Liste vorhandener Apps angezeigt. Sie können dann die erforderliche App zur Anzeige der Anlage auswählen. Einzelheiten finden Sie unter Anzeige von Anlagen.

- Secure Mail-Benutzer können die Zoom-App verwenden, um an Besprechungen teilzunehmen. Weitere Informationen zum Konfigurieren der erforderlichen Richtlinien zur Verwendung der Zoom-App finden Sie unter Teilnehmen an Besprechungen vom Kalender aus.
- **Exportieren Sie Zeit und Ort einer Besprechung in Ihren nativen Kalender.** In Secure Mail für iOS enthält die MDX-Richtlinie **Kalender exportieren** den neuen Wert **Besprechungszeit, Ort**. Damit können Sie Zeit und Ort der Besprechung von Secure Mail- Kalenderereignissen in Ihren nativen Kalender exportieren.

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

Secure Mail 18.12.0

Secure Mail 18.12.0 enthält Leistungsverbesserungen und Fehlerbehebungen.

Informationen zu behobenen und bekannten Problemen finden Sie unter Bekannte und behobene Probleme.

Secure Mail 18.11.5

Secure Mail für Android

- **Melden von Phishing-E-Mail mit ActiveSync-Kopfzeile:** Wenn ein Benutzer in Secure Mail für Android eine Phishing-E-Mail meldet, wird zu der E-Mail eine EML-Datei als Anlange erstellt. Der Empfänger der E-Mail kann die ActiveSync-Kopfzeile der gemeldeten E-Mail anzeigen.

  Um dieses Feature zu aktivieren, muss ein Administrator die Richtlinie **Phishing-E-Mail-Adressen melden** konfigurieren und **Phishingberichtmethode** in der Citrix Endpoint Management-Konsole auf **Als Anlage melden** festlegen. Einzelheiten finden Sie unter Melden von Phishing-E-Mail (als Anlage).
- **Drucken von E-Mails und Kalenderereignissen:** In Secure Mail für Android können Sie E-Mails und Kalenderereignisse von Ihrem Android-Gerät aus drucken. Zum Drucken wird das Android Print-Framework verwendet. Einzelheiten finden Sie unter Drucken von E-Mails und Kalender-ereignissen.
- **Feeds von Ihrem Manager:** In Secure Mail für Android können Sie E-Mails von Ihrem Manager im Bildschirm **Feeds** anzeigen. Je nach der Einstellungen von **E-Mail-Synchronisierungszeitraum** werden bis zu fünf E-Mails unter **Von Ihrem Manager** angezeigt. Um weitere E-Mails vom Manager anzuzeigen, tippen Sie auf **Alle anzeigen**.

  Voraussetzungen:

Exchange-Webdienste (EWS) muss auf dem Exchange Server aktiviert sein.

Die Managerkarte wird basierend auf den aus Active Directory abgerufenen Organisationsdetails (Outlook-Kontakt) angezeigt. Damit die richtigen Details im Manager- Feed angezeigt werden, stellen Sie sicher, dass Ihr Administrator Ihre Organisationshierarchie in Active Directory konfiguriert hat .

> Hinweis:
>
> Das Feature wird von IBM Lotus Notes-Servern nicht unterstützt.

Secure Mail 18.11.1

> Wichtig:
>
> Das folgende Problem wurde in Secure Mail für Android 18.11.1 behoben:
>
> In Secure Mail für Android mit Verbindungen zu IBM Notes Traveler 9.0.1 SP 10 verbleiben E-Mails mit Anlagen im Postausgang. [CXM-58962]

Secure Mail 18.11.0

Secure Mail für Android

- **Unterordnerbenachrichtigungen:** In Secure Mail für Android können Sie E-Mail-Benachrichtigungen aus Unterordnern Ihres E-Mail-Kontos erhalten. Einzelheiten finden Sie unter Unterordnerbenachrichtigungen.
- **Updates für Hintergrunddienste in Secure Mail für Android:** Zur Erfüllung der Google Play-Limits zur Ausführung im Hintergrund auf Geräten mit Android 8.0 (API-Ebene 26) oder höher wurden die Hintergrunddienste von Secure Mail aktualisiert. Zur Gewährleistung unterbrechungsfreier Synchronisierung und Benachrichtigungen auf Ihrem Gerät aktivieren Sie FCM-Push-Benachrichtigungen (Firebase Cloud Messaging). Weitere Informationen zu FCM-basierten Pushbenachrichtigungen finden Sie unter Pushbenachrichtigungen für Secure Mail.

Aktivieren Sie **E-Mail-Benachrichtigungen** in den Secure Mail-Einstellungen auf Ihrem Gerät. Weitere Informationen zu diesem Update finden Sie in diesem Support Knowledge Center-Artikel.

Einschränkungen:

- Wenn Sie keine FCM-basierten Push-Benachrichtigungen aktiviert haben, erfolgt die Hintergrundsynchronisierung alle 15 Minuten. Das Intervall kann variieren, je nachdem, ob die App im Hintergrund oder im Vordergrund ausgeführt wird.
- Wenn Benutzer die Zeit manuell über die Geräteeinstellungen aktualisieren, wird das Datum im Kalenderwidget nicht automatisch aktualisiert.

Secure Mail für iOS

- **Unterstützung für iOS 12.1:** Secure Mail für iOS unterstützt iOS Version 12.1.
- **Verbesserungen an Fehlermeldungen für Pushbenachrichtigungen mit Rich-Inhalt:** In Secure Mail für iOS werden je nach Benachrichtigungsfehler Fehlermeldungen zu Pushbenachrichtigungen in der Mitteilungszentrale auf Geräten angezeigt. Weitere Informationen zu Fehlermeldungen zu Pushbenachrichtigungen in Secure Mail für iOS finden Sie in Fehlermeldungen zu Pushbenachrichtigungen in Secure Mail für iOS.
- **Feeds von Ihrem Manager:** In Secure Mail für iOS können Sie E-Mails von Ihrem Manager im Bildschirm **Feeds** anzeigen. Je nach der Einstellungen von **E-Mail-Synchronisierungszeitraum** werden bis zu fünf E-Mails unter **Von Ihrem Manager** angezeigt. Um weitere E-Mails vom Manager anzuzeigen, tippen Sie auf **Alle anzeigen**.

  Voraussetzungen:

  Exchange-Webdienste (EWS) muss auf dem Exchange Server aktiviert sein.

  Die Managerkarte wird basierend auf den aus Active Directory abgerufenen Organisationsdetails (Outlook-Kontakt) angezeigt. Damit die richtigen Details im Manager- Feed angezeigt werden, stellen Sie sicher, dass Ihr Administrator Ihre Organisationshierarchie in Active Directory konfiguriert hat .

  > Hinweis:
  >
  > Das Feature wird von IBM Lotus Notes-Servern nicht unterstützt.

Secure Mail 18.10.5

- **Secure Mail-Integration in Slack (Vorschau):** Sie können eine E-Mail-Unterhaltung jetzt auf Geräten mit iOS oder Android in die App Slack übertragen. Einzelheiten finden Sie unter Secure Mail-Integration in Slack (Vorschau).
- **Verbesserungen am Ordner “Feeds”:** Secure Mail für iOS umfasst folgende Verbesserungen am Ordner “Feeds”:
  - Sie können jetzt bis zu fünf bevorstehende Besprechungen in Ihrer Feeds-Karte anzeigen.
  - Anstehende Besprechungen für die nächsten 24 Stunden werden in der Feeds-Karte im Abschnitt **Heute** und **Morgen** angezeigt.

Secure Mail 18.10.0

- **Secure Mail-Benachrichtigungskanäle für E-Mail- und Kalenderbenachrichtigungen:** Auf Geräten mit Android O oder höher können Sie über die Einstellungen des Benachrichtigungskanals verwalten, wie Ihre E-Mail- und Kalenderbenachrichtigungen behandelt werden.

Mit diesem Feature können Sie Ihre Benachrichtigungen anpassen und verwalten. Einzelheiten finden Sie unter Benachrichtigungskanäle.

- **Phishing-E-Mails melden (als Weiterleitung):** In Secure Mail für iOS können Sie das Feature „Als Phishing melden“ verwenden, um eine E-Mail (als Weiterleitung) zu melden, bei der Sie einen Verdacht auf Phishing haben. Sie können die verdächtigen Nachrichten an E-Mail-Adressen weiterleiten, die von Administratoren in der Richtlinie konfiguriert werden. Um dieses Feature zu aktivieren, muss ein Administrator die Richtlinie „Phishing-E-Mail-Adresse melden“ konfigurieren und **Phishing-Methode melden** als **Durch Weiterleiten melden** festlegen. Einzelheiten finden Sie unter Melden von Phishing-E-Mail als Weiterleitung.

Secure Mail 18.9.0

- Neues Versionsnummerierungsschema im Format „yy.mm.version“. Beispiel: Version **18.9.0**
- **Phishing-E-Mails melden (als Weiterleitung):** In Secure Mail für Android können Sie das Feature „Als Phishing melden“ verwenden, um eine E-Mail (als Weiterleitung) zu melden, bei der Sie einen Verdacht auf Phishing haben. Sie können die verdächtigen Nachrichten an E-Mail-Adressen weiterleiten, die von Administratoren konfiguriert werden. Um dieses Feature zu aktivieren, muss ein Administrator die Richtlinie Phishing-E-Mail-Adresse konfigurieren und „Phishing-Methode melden“ als **Durch Weiterleiten melden** festlegen. Einzelheiten finden Sie unter Melden von Phishing-E-Mail als Weiterleitung.
- **Verbesserungen an den Feeds-Karten:** Secure Mail für Android umfasst folgende Verbesserungen am Ordner **Feeds**:
  - Besprechungseinladungen aus allen automatisch synchronisierten Ordnern werden auf Ihrer Feeds-Karte angezeigt.
  - Sie können jetzt bis zu fünf bevorstehende Besprechungen in Ihrer Feeds-Karte anzeigen.
  - Bevorstehende Besprechungen werden nun basierend auf einem 24-Stunden-Zeitraum ab Ihrer aktuellen Zeit angezeigt. Diese Besprechungseinladungen werden in folgende Kategorien unterteilt: **Heute** und **Morgen**.
    In älteren Releases wurden anstehende Besprechungen bis zum Ende des Tages in den Feeds angezeigt.
- **Secure Mail-Kalenderereignisse exportieren:** Secure Mail für Android und iOS ermöglicht es Ihnen, Secure Mail-Kalenderereignisse in die native Kalenderanwendung Ihres Geräts zu exportieren. Um dieses Feature zu aktivieren, tippen Sie auf **Einstellungen**und ziehen Sie den Schieberegler für den Export von Kalenderereignissen nach rechts. Einzelheiten finden Sie unter Secure Mail-Kalenderereignisse exportieren.

Secure Mail 10.8.65

- **Verfügbar mit iOS 12:** In Secure Mail für iOS wird das Feature „Gruppenbenachrichtigungen“ unterstützt. Mit diesem Feature werden Gespräche aus einem Mail-Thread zusammengefasst. Auf dem Sperrbildschirm Ihres Geräts können Sie sich schnell gruppierte Benachrichtigungen ansehen. Die Einstellungen für Gruppenbenachrichtigungen sind standardmäßig auf dem Gerät aktiviert.
- In Secure Mail für iOS sind die Schaltflächen **Entwurf speichern** und **Entwurf löschen** größer. Diese Verbesserung erleichtert es den Kunden, eine Option von der anderen zu unterscheiden.
- In Secure Mail für iOS können Sie eingehende Anrufe von Ihren Secure Mail-Kontakten identifizieren, indem Sie die Secure Mail-Anfrufer-ID in den **Geräteeinstellungen** aktivieren. Wenn Sie diese Einstellungen aktivieren, zeigt das Gerät bei einem eingehenden Anruf den App-Namen mit der Anrufer-ID an, z. B. „Secure Mail-Anrufer-ID: Karl Schmidt“. Einzelheiten finden Sie unter Secure Mail-Anrufer-ID.

Secure Mail 10.8.60

- Secure Mail unterstützt Android P.
- Secure Mail ist jetzt auch auf Polnisch verfügbar.
- In Secure Mail für iOS können Sie Dateien über die iOS-App “Dateien” an Ihre E-Mail anhängen. Weitere Informationen finden Sie unter iOS-Features.

Secure Mail 10.8.55

Es gibt keine neuen Features in Secure Mail Version 10.8.55. Informationen zu behobenen Problemen finden Sie unter Bekannte und behobene Probleme.

Secure Mail 10.8.50

Verbesserungen beim Anhängen von Fotos. In Secure Mail für iOS können Sie Fotos über das neue **Galerie**-Symbol mühelos anhängen. Tippen Sie auf das **Galerie**-Symbol und wählen Sie Fotos zum Anhängen an E-Mail aus.

Feeds-Bildschirm in Secure Mail. Der Bildschirm **Feeds** von Secure Mail für iOS und Android enthält alle ungelesenen E-Mails und Besprechungseinladungen sowie anstehende Besprechungen.

Secure Mail 10.8.45

Ordnersynchronisierung. In Secure Mail für iOS und Android können Sie auf das Symbol **Synchronisierung** tippen, um alle Secure Mail-Inhalte zu aktualisieren. Das **Synchronisierungssymbol** ist in

Secure Mail-Ausklappmenüs wie Postfächern, Kalendern, Kontakten und Anlagen. Wenn Sie auf das **Synchronisierungssymbol** tippen, werden die Ordner aktualisiert, die Sie für die automatische Aktualisierung konfiguriert haben, z. B. Postfächer, Kalender und Kontakte. Der Zeitstempel der letzten Synchronisierung wird neben dem **Synchronisierungssymbol** angezeigt.

Verbesserungen beim Anhängen von Fotos. In Secure Mail für Android können Sie Fotos über das neue **Galerie**-Symbol mühelos anhängen. Tippen Sie auf das **Galerie**-Symbol und wählen Sie Fotos zum Anhängen an E-Mail aus.

Secure Mail 10.8.40

Durchsuchen des Kalenders In Secure Mail für iOS können Sie den Kalender nach Ereignissen, Teilnehmern oder anderem Text durchsuchen.

Secure Mail 10.8.35

Die Secure Mail-Version für iOS ist 10.8.36.

- **Antwortoptionen für Benachrichtigungen.** In Secure Mail für iOS können Benutzer auf Besprechungsbenachrichtigungen mit “Annehmen”, “Ablehnen” und “Mit Vorbehalt” antworten. Sie können auf Benachrichtigungen zu erhaltenen Nachrichten mit “Antworten” und “Löschen” reagieren.
- **Erweiterungen für die Taste “Zurück” in Secure Mail für Android.** In Secure Mail für Android können Sie auf Ihrem Gerät auf die Taste “Zurück” tippen, um die erweiterten Optionen der unverankerten Aktionstaste zu schließen. Wenn die unverankerte Aktionstaste im erweiterten Zustand ist, werden durch Antippen der Taste “Zurück” auf Ihrem Gerät die Antwortoptionen minimiert. Durch diese Aktion kehren Sie zur Ansicht der Nachrichten- oder Ereignisdetails zurück.
- **In Secure Mail für Android werden die Antworttasten für Besprechungen in der E-Mail angezeigt.** Wenn Sie eine E-Mail-Benachrichtigung zu einer Besprechungseinladung erhalten, können Sie auf die Einladung antworten, indem Sie auf eine der folgenden Optionen tippen:
  - Ja
  - Vielleicht
  - Nein

Secure Mail 10.8.25

Secure Mail für iOS unterstützt jetzt S/MIME für abgeleitete Anmeldeinformationen: Damit dieses Feature funktioniert, führen Sie folgende Schritte aus:

- Wählen Sie “Abgeleitete Anmeldeinformationen” als Quelle des S/MIME-Zertifikats aus. Einzelheiten finden Sie unter Abgeleitete Anmeldeinformationen für die Registrierung von iOS-Geräten.
- Fügen Sie die Clienteigenschaft für LDAP-Attribute in Citrix Endpoint Management hinzu. Verwenden Sie die folgenden Informationen:
  - **Schlüssel:** SEND_LDAP_ATTRIBUTES
  - **Wert:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`

Weitere Informationen zum Hinzufügen einer Clienteigenschaft finden Sie unter Clienteigenschaften (XenMobile Server) bzw. Clienteigenschaften (Endpoint Management).

Weitere Informationen zum Registrieren von Geräten mit abgeleiteten Anmeldeinformationen finden Sie unter Registrieren von Geräten mit abgeleiteten Anmeldeinformationen.

1. Navigieren Sie in der Endpoint Management-Konsole zu **Konfigurieren > Apps**.
2. Wählen Sie **Secure Mail** und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie unter der iOS-Plattform für die S/MIME-Zertifikatquelle **Abgeleitete Anmeldeinformationen** aus.

Secure Mail für iOS und Android wurden umfassend überarbeitet: Wir haben die Navigation für Benutzer einfacher und effizienter gemacht. Wir haben das Secure Mail-Menü und die Aktionstasten in Form einer Navigationsleiste neu ausgerichtet. Ein Video, das die Änderungen der Benutzernavigation zeigt, finden Sie hier:

Die folgende Abbildung zeigt die neue Navigationsleiste auf iOS-Geräten.

Die folgende Abbildung zeigt die neue Navigationsleiste auf Android-Geräten.

Folgendes hat sich geändert:

- Das Greifsymbol wurde entfernt. Secure Mail-Funktionen wie E-Mail, Kalender, Kontakte und Anlagen sind jetzt als Taste in der Tastenleiste verfügbar. Die folgende Abbildung zeigt diese Änderung.

  > Hinweis:
  >
  > Auf Android-Geräten ist die Tastenleiste nach dem Öffnen einer E-Mail-Nachricht nicht verfügbar. Wenn Sie beispielsweise eine E-Mail oder ein Kalenderereignis öffnen, ist die Tastenleiste nicht verfügbar, (siehe unten).

- Das Menü **Einstellungen** ist in allen Menüs, wie E-Mail, Kalender, Kontakte und Anlagen, verfügbar. Um zu den Einstellungen zu gelangen, tippen Sie auf das Hamburgersymbol und dann auf die Taste **Einstellungen** unten rechts, wie in der folgenden Abbildung dargestellt.

- Das Symbol **Suchen** ersetzt die Suchleiste und ist in den Ansichten “Posteingang”, “Kontakte” und “Anlagen” verfügbar.
- Auf iOS-Geräten können Sie auf eine E-Mail tippen und halten, um sie auszuwählen.
- Tippen Sie auf die unverankerte Aktionstaste **Erstellen**, um eine neue E-Mail zu erstellen (siehe Abbildung unten).
- Die folgenden Menüoptionen sind jetzt oben rechts auf Ihrem Bildschirm verfügbar:
  - **Synchronisierungsoptionen:** Tippen Sie oben rechts auf das Überlaufsymbol und navigieren Sie zu **Weitere Optionen> Synchronisierungsoptionen**, um Ihre Synchronisierungseinstellungen zu ändern.

    > Hinweis:
    >
    > Diese Option ist nur auf Android-Geräten verfügbar.

  - **Suchsymbol:** Antippen, um nach einer E-Mail zu suchen.
- **Selektierungsansichtsymbol:** Antippen, um eine Selektierungsansicht der Unterhaltung zu sehen.
- **Unverankerte Aktionstaste zum Antworten:** Tippen Sie während der Anzeige einer E-Mail auf “Weiterleiten”, “Allen antworten” oder “Antworten”, wie in der folgenden Abbildung dargestellt.
- Beim Anzeigen einer E-Mail stehen die folgenden Menüoptionen oben rechts auf dem Bildschirm zur Verfügung:
  - **Kennzeichnen:** Antippen, um die E-Mail zu kennzeichnen.
  - **Ungelesen:** Antippen, um E-Mails als ungelesen zu markieren.
  - **Löschen:** Antippen, um die E-Mail zu löschen.
  - **Weitere Optionen:** Tippen Sie auf das Überlaufsymbol, um andere verfügbare Aktionen anzuzeigen, z. B. “Verschieben”.

Kalender - Änderungen

- Im Kalender können Sie auf eine unverankerte Aktionsschaltfläche für Ereignisse tippen, um ein Ereignis zu erstellen, wie in der folgenden Abbildung dargestellt.
- Die folgenden Menüoptionen sind jetzt oben rechts auf Ihrem Bildschirm verfügbar:
  - **Heute:** Antippen, um die heutigen Ereignisse anzuzeigen.
  - **Suchen:** Antippen, um nach einem Ereignis zu suchen.
  - **Unverankerte Aktionstaste zum Antworten:** Tippen Sie während der Anzeige eines Ereignisses auf “Weiterleiten”, “Allen antworten” oder “Antworten”.

Wenn Sie ein Ereignis anzeigen, werden die Antwortaktionen für das Ereignis, wie “Ja”, “Vielleicht” und “Nein” neu ausgerichtet und sind unterhalb der Ereignisdetails verfügbar.

Kontakte - Änderungen

- Tippen Sie auf die unverankerte Aktionstaste **Neuen Kontakt erstellen**, siehe Abbildung unten.
- Die Menüoption **Suchen** ist jetzt oben rechts auf dem Bildschirm verfügbar. Tippen Sie auf die Option, um nach einem Kontakt zu suchen.
- Beim Anzeigen eines Kontakts stehen die folgenden Menüoptionen oben rechts auf dem Bildschirm zur Verfügung:

  Auf Android-Geräten:

  - **Bearbeiten:** Antippen, um den Kontakt zu bearbeiten.
  - **Weitere Optionen:** Tippen Sie auf das Bearbeitungssymbol, um weitere verfügbare Aktionen anzuzeigen, z. B. “An E-Mail anfügen”, “Freigeben” und “Löschen”.

  Auf iOS-Geräten:

  - **Bearbeiten:** Antippen, um den Kontakt zu bearbeiten.
  - **Freigeben:** Tippen Sie auf das Freigabesymbol, um weitere verfügbare Aktionen anzuzeigen, z. B. “Kontakt freigeben” und “An E-Mail anfügen”.

  > Hinweis:
  >
  > Um einen Kontakt auf iOS-Geräten zu löschen, wählen Sie den Kontakt aus, tippen Sie auf **Bearbeiten** und anschließend unten auf dem Bildschirm auf **Löschen**, wie in der folgenden Abbildung dargestellt.

Anlagen - Änderungen

Die folgenden Menüoptionen für Anlagen sind jetzt oben rechts auf Ihrem Bildschirm verfügbar:

- **Sortieren:** Tippen Sie auf das Symbol **Sortieren** und wählen Sie die entsprechenden Filter aus, um Anlagen zu sortieren.
- **Suchen:** Antippen, um nach einer Anlage zu suchen.

Secure Mail 10.8.20

- Secure Mail für iOS unterstützt jetzt die Verwendung abgeleiteter Anmeldeinformationen für die Registrierung und Authentifizierung. Weitere Informationen zu abgeleiteten Anmeldeinformationen finden Sie unter Abgeleitete Anmeldeinformationen für die Registrierung von iOS-Geräten.
- Secure Mail für iOS unterstützt Pushbenachrichtigungen mit Rich-Inhalt. Benachrichtigungen mit Rich-Inhalt gewährleisten den Erhalt von Sperrbildschirmbenachrichtigungen für den Posteingang, selbst wenn Secure Mail nicht im Hintergrund ausgeführt wird. Das Feature

wird bei Verwendung der kennwortbasierten Authentifizierung und der clientbasierten Authentifizierung unterstützt. Einzelheiten finden Sie unter Pushbenachrichtigungen mit Rich-Inhalt.

> Hinweis:
>
> Aufgrund der geänderten Architektur zur Unterstützung von Pushbenachrichtigungen mit Rich-Inhalt ist die Benachrichtigungseinstellung **Nur VIP** nicht mehr verfügbar.

- Secure Mail für Android unterstützt jetzt Rich-Text-Signaturen ebenso wie iOS. Sie können Bilder oder Links in Ihrer E-Mail-Signatur verwenden. Einzelheiten finden Sie unter Rich-Text-Signaturen.

Secure Mail 10.8.15

- **Secure Mail für iOS unterstützt jetzt Rich-Text-Signaturen.** Sie können Bilder oder Links in Ihrer E-Mail-Signatur verwenden. Einzelheiten finden Sie unter Rich-Text-Signaturen.
- **Secure Mail unterstützt Android Enterprise (zuvor "Android for Work").** Sie können ein separates Arbeitsprofil erstellen, indem Sie Android-Unternehmensapps in Secure Mail verwenden. Einzelheiten finden Sie unter Android Enterprise in Secure Mail.
- **Secure Mail gibt eingebettete Ressourcen beim Anzeigen einer E-Mail wieder.** Wenn sich die Ressourcen in Ihrem internen Netzwerk befinden (z. B. wenn Bild-URLs in einer E-Mail interne Links sind), stellt Secure Mail eine Verbindung mit dem internen Netzwerk her, um den Inhalt abzurufen und anzuzeigen.
- **Secure Mail unterstützt die moderne Authentifizierung**. Die moderne Authentifizierung ist eine OAuth-tokenbasierte Authentifizierung mit Benutzernamen und Kennwort. Diese Unterstützung umfasst Unterstützung für Office 365 für interne und externe Active Directory-Verbunddienste (AD FS) oder Identitätsanbieter (IdP).
- **Leistungsverbesserungen für das Anlagenrepository**. Sie können jetzt schneller durch das Anlagenrepository scrollen.

Secure Mail 10.8.10

- **Unterstützung für das Drucken von E-Mail-Anlagen**. Secure Mail für iOS unterstützt das Drucken von E-Mail-Anlagen.
- **Moderne Authentifizierung mit Microsoft Office 365**. Secure Mail für iOS unterstützt die moderne Authentifizierung. Die moderne Authentifizierung ist eine OAuth-tokenbasierte Authentifizierung mit Benutzernamen und Kennwort. Diese Unterstützung umfasst Unterstützung für Office 365 für interne und externe Active Directory-Verbunddienste (AD FS) und Identitätsanbieter (IdP).

> Hinweise:
>
> – Diese Version unterstützt keine moderne Authentifizierung in der Endpoint Management-Integration für Microsoft Intune-/EMS.
> – Dieses Release enthält moderne Authentifizierung in einem Szenario, in dem AD FS extern verfügbar ist.

Einzelheiten finden Sie unter Moderne Authentifizierung mit Microsoft Office 365.

Bekannte und behobene Probleme

May 23, 2019

Bekannte Probleme in Version 19.5.0

Auf Geräten mit iOS können Sie eine Verbindung zu Wi-Fi-Netzwerken herstellen, die nicht in der MDX-Richtlinie **Zulässige WiFi-Netzwerke** definiert sind. Dadurch können Sie Secure Mail und Secure Web für iOS auch über Netzwerke öffnen, die nicht in der MDX-Richtlinie aufgeführt sind. [CXM-66730]

Behobene Probleme in Version 19.5.0

- In Secure Mail für Android können Sie beim Erstellen einer neuen E-Mail keine E-Mail-Adressen kopieren und in die Felder **An:** oder **Cc/Bcc:** einfügen. Beim Beantworten einer E-Mail können Sie E-Mail-Adressen jedoch in die Felder **An:** oder **Cc/Bcc:** einfügen. [CXM-64752]
- In Secure Mail für Android können Sie beim Registrieren von Android Enterprise-Geräten keine konfigurierten Kontoeinstellungen speichern. [CXM-65138]

Bekannte und behobene Probleme in Secure Mail für Android 19.4.6

In diesem Release gibt es keine bekannten oder behobene Probleme.

Bekannte und behobene Probleme in früheren Versionen

Bekannte Probleme in Version 19.4.5

Es gibt keine bekannten Probleme in diesem Release.

Behobene Probleme in Version 19.4.5

- Wenn Sie in Secure Mail für iOS eine Besprechungsanfrage in Outlook senden und sie in Secure Mail bearbeiten, wird die Besprechung in Outlook nicht aktualisiert. Die Empfänger erhalten das Update auch nicht. Dieses Problem tritt auch auf, wenn Sie eine Besprechungsanfrage in Secure Mail erstellen und sie in Secure Mail bearbeiten. [CXM-62511]
- In Secure Mail für iOS wird der Kalender nicht synchronisiert, und der folgende Fehler wird angezeigt: "Couldn't sync Calendar". [CXM-62796]
- In Secure Mail für Android werden einige Besprechungseinladungen, die Sie mit Outlook erstellen, nicht in Ihrem Secure Mail-Kalender widergespiegelt. [CXM-63552]
- In Secure Mail für Android werden wiederkehrende Besprechungen zu einem verzögerten Zeitpunkt angezeigt, und Aktualisierungen, die an den Besprechungen vorgenommen wurden, werden nicht korrekt synchronisiert. [CXM-65263]

Bekannte Probleme in Version 19.3.5

Es gibt keine bekannten Probleme in diesem Release.

Behobene Probleme in Version 19.3.5

- In Secure Web für iOS können Sie die bitly-URL nicht in den Browser einfügen. [CXM-56276]
- In Secure Mail für iOS wird für jede empfangene E-Mail die folgende Fehlermeldung angezeigt: Nachricht konnte nicht abgerufen werden. Öffnen Sie Secure Mail. [CXM-56418]
- Wenn Benutzer in Secure Mail für iOS die App öffnen und eine PIN eingeben, wird häufig eine Meldung angezeigt, dass das Unternehmensnetzwerk nicht verfügbar ist. [CXM-59776]
- Secure Mail für iOS wird nach dem Wechsel zur Multifaktorauthentifizierung nicht synchronisiert. [CXM-62176]

Bekannte Probleme in Secure Mail 19.3.0

Es gibt keine bekannten Probleme in dieser Version.

Behobene Probleme in Version 19.3.0

Secure Mail für iOS

Wenn in Secure Mail für iOS eine ungültige Netzwerksitzung zu einem Anforderungstimeout führt, wird beim Empfang einer E-Mail kurzzeitig folgendes Benachrichtigungsbanner angezeigt: **Secure Mail kann diese Nachricht aufgrund eines Anforderungstimeouts nicht abrufen**. [CXM-62561]

Secure Mail für Android

- In Secure Mail für Android können Sie keine FCM-Benachrichtigungen (Firebase Cloud Messaging) von mozaiekwonen.xm.cloud.com empfangen. [CXM-62146]
- Wenn Sie in Secure Mail für Android ein Kalendereereignis aktualisieren, werden die Änderungen nicht mit Outlook Office 365 synchronisiert. [CXM-62227]
- In Secure Mail für Android werden E-Mails mit Anlagen bei schlechter oder fehlender Netzwerkkonnektivität nicht gesendet. Diese E-Mails verbleiben auch nach Wiederherstellung der Netzwerkkonnektivität im Postausgang. [CXM-64297]

Bekannte Probleme in Version 19.2.0

Wenn in Secure Mail für iOS die Transparenzoption mit OCSP (Online Certificate Status Protocol) für ein Zertifikat aktiviert wurde, schlägt die Secure Mail-Konfiguration unter iOS 12.1.1 und höher fehl.

Behobene Probleme in Version 19.2.0

Secure Mail für iOS

In Secure Mail für iOS können Sie keinen Text aus der Betreffzeile der App in Secure Notes 10.8.6.6 kopieren. [CXM-61060]

Secure Mail für Android

- Wenn in Secure Mail für Android die Textvorhersage auf Samsung-Geräten aktiviert ist, wird das letzte Wort des Textes unterstrichen. Das letzte Wort der Signatur wird mit einer Unterstreichung gespeichert, wenn kein Leerzeichen verwendet wird, und beim Empfänger auch so angezeigt. [CXM-60894]
- Wenn Sie in Secure Mail für Android eine E-Mail-Zusammenfassung erhalten, werden die Bilder nicht angezeigt. [CXM-62280]
- 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]

Bekannte und behobene Probleme in Secure Mail für iOS 19.1.6

Es gibt keine bekannten oder behobenen Probleme in Version 19.1.6.

Die folgenden Probleme wurden in früheren Versionen behoben:

Bekannte Probleme in Version 19.1.5

Es gibt keine bekannten Probleme in Version 19.1.5.

Behobene Probleme in Version 19.1.5

Die folgenden Probleme wurden in Version 19.1.5 behoben:

- In Secure Mail für iOS wird für jede empfangene E-Mail die folgende Fehlermeldung angezeigt: **Nachricht konnte nicht abgerufen werden. Öffnen Sie Secure Mail.** [CXM-56418]
- In Secure Mail für iOS wird, wenn Sie die App öffnen und die PIN eingeben, häufig gemeldet, dass das Unternehmensnetzwerk nicht verfügbar ist. [CXM-59766]
- Bei umschlossenen Android-Apps wird die Zeichenfolge “UserAgent” mehrfach angehängt, wodurch die Headergröße erhöht wird. Dies führt zu einem Fehler und die Seite wird nicht geladen. [CXM-59869]

Behobene Probleme in Version 19.1.0

Secure Mail für iOS

- Wenn Secure Mail keine Verbindung zum Exchange Server herstellen kann, wird die folgende Meldung im E-Mail-Benachrichtigungsbanner angezeigt:

  “Wir können diese Nachricht nicht abrufen, da Ihre Sitzung abgelaufen ist. Öffnen Sie Secure Mail, um Ihre Sitzung zu erneuern.”

  Dieses Problem wurde behoben und die Nachricht wird wie folgt aktualisiert:

  “Secure Mail kann keine Verbindung zum Netzwerk Ihrer Organisation herstellen.” Bitte kontaktieren Sie Ihren Administrator.” [CXM-59128]

- Für Benutzer mit O365-Postfach wird beim wiederholten Ausführen von Benachrichtigungsantwortaktionen wie **Ja, Nein, Vielleicht oder Löschen** Office 365 gedrosselt und es wird folgende Fehlermeldung angezeigt:

  “The server is busy. Please try again.” [CXM-60123]

Secure Mail für Android

- Wenn Sie in Secure Mail für Android die türkische Sprache verwenden, können Sie keine E-Mails an Empfänger senden, deren Adresse das Zeichen „I“ enthält. [CXM-59093]
- In Secure Mail für Android können Benutzer die Betreffzeile einer E-Mail nicht auswählen und hervorheben. [CXM-59185]

- In Secure Mail für Android schlägt die Anmeldung fehl, wenn das Kennwort das Eurozeichen (€) enthält. [CXM-59654]
- Wenn in Secure Mail für Android die Einstellung **Mit lokalen Kontakten synchronisieren** aktiviert ist, werden alle Secure Mail-Kontakte in Ihre nativen Kontakte exportiert. Nach der Synchronisierung werden Telefonfelder wie Mobil, Firma, Privat, Fax (Firma) und Fax (privat) nicht in der richtigen Reihenfolge angezeigt. Beispielsweise wird in Ihren nativen Kontakten die Faxnummer über der Mobiltelefonnummer angezeigt. Benutzer können diese Reihenfolge nicht ändern. [CXM-57994]

Behobene Probleme in Version 18.12.0

Secure Mail für iOS

- Wenn Sie in Secure Mail für iOS eine E-Mail im RTF-Format erhalten, sind bestimmte Arten von Inlineanlagen und das Anlagensymbol nicht sichtbar. [CXM-59121]
- Wenn in Secure Mail für iOS Pushbenachrichtigungen mit Rich-Inhalt aktiviert sind und Sie die Option **E-Mail- Benachrichtigungen** deaktivieren und wieder aktivieren, wird die Option **E-Mail-Typ** sporadisch angezeigt. [CXM-59122]

Secure Mail für Android

- Wenn Sie die clientbasierten Authentifizierung in Ihrer Umgebung ausführen, kann Secure Mail E-Mails sporadisch nicht automatisch synchronisieren. Beim manuellen Synchronisieren werden nur einige E-Mails abgerufen. [CXM-59650]

Behobene Probleme in Version 18.11.1

- In Secure Mail für Android mit Verbindungen zu IBM Notes Traveler 9.0.1 SP 10 verbleiben E-Mails mit Anlagen im Postausgang. [CXM-58962]

Behobene Probleme in Version 18.11.0

- In Secure Mail für Android können eingebettete Bilder nicht in der E-Mail angezeigt werden. [CXM-53556]
- Secure Mail für Android stürzt ab, wenn eine E-Mail mit einer Signatur mit eingebetteter URL (z. B. `file://C:\...jpg`. [CXM-58219]) geöffnet wird.

Behobene Probleme in Version 18.10.5

Secure Mail für iOS

- Wenn die MDX-Richtlinie “iOS-Datenschutz aktivieren” aktiviert ist, wird periodisch die Benachrichtigung “Sie haben neue E-Mail” angezeigt. [CXM-55491]
- Auf dem iPhone XS können keine Anhänge heruntergeladen oder gesendet werden und heruntergeladene Bilder können nicht angezeigt werden. [CXM-57030]

Secure Mail für Android

- Wenn Benutzer ein wiederkehrendes Meeting für Konten mit Exchange ActiveSync Version 16 und höher ändern, wird das Meeting nicht in Exchange Server aktualisiert. Daher wird das Meeting nicht zwischen Secure Mail und Outlook synchronisiert. [CXM-57200]

Behobene Probleme in Version 18.10.0

- In Secure Mail für Android können Benutzer keine Inlinebilder anzeigen, die auf andere Server als Exchange-Server verweisen. [CXM-56736] [CXM-55843]
- In Secure Mail für Android wurde die PIN-Nummer bei der Teilnahme an Webex-Besprechungen nicht mit der Einwahlnummer verknüpft. Sie müssen die PIN-Nummer manuell eingeben. [CXM-56002]
- Secure Mail für Android stürzt ab, wenn Sie versuchen, den Secure Mail-Kalender zu exportieren, wenn Ihr persönlicher Kalender nicht konfiguriert ist. [CXM-56264]
- Auf dem iPhone XS können in Secure Mail für iOS keine Anhänge heruntergeladen oder gesendet werden und heruntergeladene Bilder können nicht angezeigt werden. [CXM-57030]

Behobene Probleme in Version 18.9.0

Secure Mail für Android

- Die Clientarbeitsstation ändert sich bei jeder NT LAN Manager (NTLM)-Authentifizierungsanforderung zufällig. [CXM-55177]
- Die Secure Mail-Synchronisierung auf Android P funktioniert zeitweise nicht mehr, wenn das Gerät im Batteriesparmodus ist. [CXM-55441]
- Secure Mail stürzt ab, wenn Sie versuchen, den Secure Mail-Kalender zu exportieren, wenn Ihr persönlicher Kalender nicht konfiguriert ist. [CXM-56264]

Behobene Probleme in Version 10.8.65

Secure Mail für iOS

- Wenn FIPs aktiviert ist und Benutzer Secure Mail für iOS auf einem iOS 11.3-Gerät ausführen, funktionieren die MDX-Richtlinien für Ausschneiden, Kopieren und Einfügen nicht wie erwartet. [CXM-53993]

- Wenn Sie Secure Mail für iOS auf freigegebenen Geräten verwenden, können neue Benutzer die E-Mails eines früheren Benutzers anzeigen, obwohl dieser Benutzer sich abgemeldet hat. Wenn der neue Benutzer auf einen Ordner tippt, um die Anzeige zu aktualisieren, werden die E-Mails der vorherigen Benutzer nicht mehr angezeigt. [CXM-55176]

Behobene Probleme in Version 10.8.60

> Hinweis:
>
> Die Secure Mail-Versionen 10.8.25 bis 10.8.60 enthalten keine bekannten Probleme.

- In Secure Mail für iOS, das auf IBM Lotus Domino-Servern ausgeführt wird, können Sie das Suchsymbol nicht in Ihrem Posteingang verwenden. [CXM-53782]
- Wenn Benutzer ein Gerät mit Secure Mail für Android mit Intune Company Portal registrieren, funktioniert Secure Mail nicht mehr. [CXM-54178]
- Secure Mail für iOS stürzt ab, während eine große Anzahl von E-Mail-Ordnern vom Server während eines FTU-Flusses synchronisiert wird. [CXM-54371]
- In Secure Mail für iOS erscheint die Druckvorschau von PDFs kleiner. [CXM-54482]
- In Secure Mail for Android werden mehrere E-Mail-IDs beim Beantworten von E-Mails nicht automatisch ausgefüllt. [CXM-54811]

Behobene Probleme in Version 10.8.55

- In Secure Mail für iOS wird die Wochenansicht des Kalenders auf einem iPad Pro im Querformat falsch dargestellt. [CXM-53723]

Behobene MDX-Probleme in Version 10.8.55

- Unter Android stürzt Secure Mail ab, wenn Benutzer von Secure Hub abgemeldet werden. [CXM-53930]
- Auf iOS-Geräten stürzen Secure Web und Secure Mail 10.8.45 beim Start ab. [CXM-54089]

Behobene Probleme in Version 10.8.50

- In Secure Mail für iOS können keine Videodateien in ShareFile gespeichert werden. [CXM-42238]
- Wenn Sie Pushbenachrichtigungen in Secure Mail für Android aktivieren, erhalten Sie keine Benachrichtigungen für neue E-Mails. Das Problem tritt zeitweilig auf. [CXM-53135]

Behobene Probleme in Version 10.8.45

Secure Mail Version 10.8.45 enthielt keine behobenen Probleme.

Behobene Probleme in Version 10.8.40

In Secure Mail für iOS werden zeitweise für jede neu empfangene E-Mail zwei Benachrichtigungen angezeigt. [CXM-51473]

Behobene Probleme in Version 10.8.35

- In Secure Mail für Android bricht die automatische Synchronisierung sporadisch ab. Die Benutzer müssen dann eine manuelle Synchronisierung durchführen, damit neue, von Office 365-Servern stammende Nachrichten in Secure Mail angezeigt werden. [CXM-49354, CXM-52716]
- Auch wenn Sie in Secure Mail für Android die E-Mail-Benachrichtigungen für E-Mail- und Kalenderereignisse deaktivieren, werden die Benachrichtigungen weiterhin angezeigt und es erfolgt eine akustische Benachrichtigung. [CXM-50479]
- Wenn Sie ein ganztägiges Ereignis mit Secure Mail für Android erstellen, werden falsche Daten in Ihrem Outlook-Kalender angezeigt. [CXM-50612]
- In Secure Mail für Android werden persönliche Exchange-Kontaktgruppen nicht mit der App synchronisiert. [CXM-51190]
- Wenn SSO konfiguriert ist, schlägt SSO von Secure Mail für Android an Exchange fehl. Benutzer werden aufgefordert, sich mit einem Kennwort anzumelden. [CXM-51343]

Behobene Probleme in Version 10.8.25

- In Secure Mail für Android tritt eine Verzögerung auf, wenn Benutzer eine Kalendereinladung mit Office 365 synchronisieren. Das Problem tritt auf, wenn eine Kalendereinladung erstellt oder aktualisiert wird. [CXM-49596]
- Wenn Benutzer in Secure Mail für Android einen einzelnen Buchstaben in das Feld cc: eingeben und anschließend auf **Senden** tippen, sendet Secure Mail die Nachricht an den ersten Benutzer in der Liste der häufig verwendeten Benutzer. Stattdessen sollte die Benachrichtigung angezeigt werden, dass der Eintrag im Feld cc: ungültig ist. [CXM-50476]
- Auf Zebra T51-Geräten mit Android 7 können Benutzer die Citrix Launcher-App nicht installieren. [CXM-50621]
- Wenn NetScaler Gateway mit zertifikatbasierter Authentifizierung konfiguriert ist, wird in Secure Mail für iOS jedes Mal, wenn Benutzer eine neue Nachricht erhalten, die Meldung “Sie haben neue E-Mails” angezeigt. Stattdessen sollte die Benachrichtigung den Namen des Absenders, den Betreff und die Vorschau anzeigen. [CXM-51075]

Behobene Probleme in Version 10.8.20

- Wenn die Intune Company Portal-App auf Android-Geräten installiert ist, die im MAM-Only-Modus registriert sind, versucht Secure Mail in Endpoint Management die Umleitung zur Microsoft-Anmeldeseite. Die folgende Fehlermeldung wird angezeigt: Keine Konfiguration für die App erhalten. Wenden Sie sich an den Administrator, um die App zu konfigurieren. [CXM-48135]
- In Secure Mail für Android schlägt die Anmeldung fehl, wenn der Benutzername oder das Kennwort Sonderzeichen (ä, ö, ü oder €) enthält. [CXM-48197]
- Auf Android-Geräten ermöglicht ein Neustart das Umgehen der Authentifizierung für den Zugriff auf Secure Mail. [CXM-48444]
- Wenn Sie in Secure Mail für Android auf E-Mails antworten, bevor Inlinebilder heruntergeladen sind, bleiben E-Mails im Postausgang hängen. Das Problem tritt auf, wenn die Einstellung **Bilder anzeigen** aktiviert ist. [CXM-49222]
- Wenn in Secure Mail für iOS die IRM-Richtlinie **aktiviert** und die E-Mail-Klassifizierung auf **Geschützt** festgelegt ist, können beim Herunterladen der vollständigen E-Mail keine Anhänge angezeigt werden. [CXM-49544]

Behobene Probleme in Version 10.8.10

Secure Mail für iOS

- Nach dem Update auf Secure Mail 10.7.25 für iOS fehlen im Nachrichten-ID-Header die Klammern (< und >). [CXM-46029]
- In Secure Mail für iOS: Stürzt die App sporadisch ab, wenn Benutzer eine Kalendereinladung aus Outlook hinzufügen. Dieses Problem tritt auf, wenn die Kalendereinladung ein Emoji enthält. [CXM-46250]
- Wenn unter iOS nach dem Upgrade von mobilen Produktivitätsapps auf 10.7.30 die Einstellung “Protokollebene” auf 11 oder höher festgelegt wird, wird Secure Mail langsam ausgeführt und stürzt ab, wenn es geöffnet bleibt. [CXM-46721]
- In Secure Mail für iOS: Sporadisch werden Benachrichtigungen doppelt angezeigt, wenn die Richtlinie “Benachrichtigungen bei gesperrtem Bildschirm steuern” auf **Nur Anzahl** festgelegt ist. [CXM-47461]

Secure Mail für Android

In Secure Mail für Android: Wenn Benutzer vier oder mehr E-Mail-Adressen in das Feld “An:” kopieren, stürzt die App ab. [CXM-46578]

Bekannte Probleme in Version 19.1.0

Es gibt keine bekannten Probleme in Version 19.1.0.

Bereitstellen von Secure Mail

March 11, 2019

Das generelle Verfahren zum Bereitstellen von Citrix Endpoint Management (früher XenMobile) ist Folgendes:

1. Sie können Secure Mail in einen Exchange-Server oder einen IBM Notes Traveler-Server integrieren, damit es mit Microsoft Exchange bzw. IBM Notes synchronisiert bleibt. Wenn Sie IBM Notes verwenden, müssen Sie den IBM Notes Traveler-Server konfigurieren. Die Konfiguration verwendet Active Directory-Anmeldeinformationen für die Authentifizierung beim Exchange- bzw. IBM Notes Traveler-Server. Weitere Informationen finden Sie unter Integration von Exchange Server oder IBM Notes Traveler-Server.

   > **Wichtig:**
   >
   > Sie können mit IBM Notes Traveler (zuvor IBM Lotus Notes Traveler) keine E-Mails von Secure Mail synchronisieren. Diese Drittanbieterfunktion von Lotus Notes wird derzeit nicht unterstützt. Wenn Sie eine beantwortete Besprechungsmail aus Secure Mail löschen, wird die Mail auf dem IBM Notes Traveler-Server nicht gelöscht. Wenn Benutzer ein Kalenderereignis akzeptieren und dann das Ereignis mit einem Kommentar ablehnen oder auf einen Kommentar reagieren, fehlt der Kommentar. [CXM-47936] Informationen zu bekannten Einschränkungen bei IBM/Lotus Notes finden Sie in diesem Citrix Blogbeitrag.

2. Sie können auch Single Sign-On über Secure Hub aktivieren. Dazu konfigurieren Sie die Kontoinformationen von Citrix Files in der Endpoint Management-Konsole, um Endpoint Management als SAML-Identitätsanbieter für Citrix Files zu aktivieren. Bei der Konfiguration werden Active Directory-Anmeldeinformationen für die Authentifizierung bei Citrix Files verwendet.

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

3. Laden Sie die MDX-Datei für Secure Mail von der Citrix Downloadsite herunter.

4. Fügen Sie Secure Mail zu Endpoint Management hinzu und konfigurieren Sie MDX-Richtlinien. Weitere Informationen finden Sie unter [Apps hinzufügen].(/de-de/citrix-endpoint-management/apps.html)

> Hinweis:
>
> Ab Version 10.6.5 von Secure Mail können Sie eine neue MDX-Analyserichtlinie für Secure Mail für iOS und Android konfigurieren. Citrix sammelt Analysedaten, um die Produktqualität zu verbessern. Mit der Richtlinie "Google Analytics-Detailgrad" können Sie festlegen, ob die Daten Ihrer Unternehmensdomäne zugeordnet werden können oder anonym gesammelt werden. Durch die Auswahl von **Anonym** wird die Unternehmensdomäne der Benutzer nicht in die gesammelten Daten eingeschlossen. Diese neue Richtlinie ersetzt eine frühere Google Analytics-Richtlinie.

Wenn die Richtlinie auf "Anonym" festgelegt ist, werden folgende Datentypen erfasst. Wir haben keine Möglichkeit, diese Daten mit einem bestimmten Benutzer oder einem Unternehmen zu verknüpfen, da wir keine benutzerbezogenen Informationen erheben. Es werden keine personenbezogenen Informationen an Google gesendet.

- Gerätestatistiken, z. B. die Betriebssystemversion, Appversion und Gerätemodell
- Plattforminformationen, z. B. ActiveSync-Version und Version des Secure Mail-Servers
- Fehlerpunkte für die Produktqualität, z. B. APNs-Registrierungen, E-Mail-Synchronisierung und -Versand sowie Download von Anlagen und Kalendersynchronisierung

Wenn die Richtlinie auf **Vollständig** festgelegt ist, werden außer der Unternehmensdomäne keine anderen identifizierbaren Daten erfasst. Die Standardeinstellung ist **Vollständig**.

Konfigurieren von Secure Mail

February 11, 2019

Die folgenden Features können konfiguriert und in Secure Mail integriert werden:

- Integration von Secure Mail in Microsoft Intune/EMS
- Moderne Authentifizierung mit Office 365
- Hintergrunddienste für Secure Mail
- Integration von Exchange Server oder IBM Notes Traveler-Server
- S/MIME für Secure Mail
- SSO für Secure Mail

Integration von Secure Mail in Microsoft Intune/EMS

February 19, 2019

Durch eine solche Integration können Sie Citrix Secure Mail mit einem höheren Sicherheitsniveau verwalten und bereitstellen um haben die Möglichkeit der Produktivitätssteigerung.

Secure Mail unterstützt verschiedene Intune-Konfigurationen. Sie können Secure Mail mit On-premises-Exchange- oder Office 365-Postfächern verbinden. Informationen zur Einrichtung der Integration von Citrix Endpoint Management in Microsoft Intune/EMS finden Sie unter Integration von Endpoint Management in Microsoft Intune/EMS.

Secure Mail unterstützt die folgenden Bereitstellungsmodi:

- Intune MAM
- Intune MAM und Intune-Mobilgeräteverwaltung (MDM)
- Intune MAM mit Endpoint Management nur-MDM
- Intune MAM mit Endpoint Management MDM und MAM

Unterstützte Mailserver

- Exchange Online
- Exchange Server 2016
- Exchange Server 2013

Einschränkungen

Secure Mail unterstützt keine zertifikatbasierte Authentifizierung.

> **Wichtig:**
>
> Zur gleichzeitigen Verwendung von Secure Mail im MDM-Modus und von Citrix Endpoint Management (MDM und MAM) müssen Sie in Ihrer Umgebung Secure Hub konfigurieren.

Konfigurieren von Secure Mail für Intune

Bei einer Umgebung mit Citrix Endpoint Management im MDM-Modus füllt Secure Mail bei der Erstverwendung automatisch die Benutzernamen auf.

Um dieses Feature zu aktivieren, müssen Sie benutzerdefinierte Richtlinienin der Endpoint Management-Konsole konfigurieren. Weitere Informationen finden Sie in der Dokumentation zu Endpoint Management unter Konfigurieren von Secure Mail.

Mit Intune nicht kompatible Features

Die folgenden Secure Mail-Features sind nicht mit der Integration von Endpoint Management mit EMS/Intune kompatibel:

- Secure Ticket Authority (STA)
- E-Mail-Registrierung mit Single Sign-On
- Pushbenachrichtigungen mit Rich-Inhalt
- Citrix Files (zuvor ShareFile)
- S/MIME-Signatur und Verschlüsselung
- Verwaltung von Informationsrechten (IRM) von Microsoft
- Secure Browse + interner Exchange-Server ohne KCD-SSO

Moderne Authentifizierung mit Microsoft Office 365

February 11, 2019

Secure Mail unterstützt die moderne Authentifizierung mit Microsoft Office 365 für Active Directory-Verbunddienste (AD FS) oder Identitätsanbieter (IdP). Die moderne Authentifizierung ist eine OAuth-tokenbasierte Authentifizierung mit Benutzernamen und Kennwort. Secure Mail-Benutzer mit IOS-Geräten können die zertifikatbasierte Authentifizierung beim Herstellen einer Verbindung mit Office 365 nutzen. Bei der Anmeldung bei Secure Mail erfolgt die Authentifizierung mit einem Clientzertifikat anstelle der Anmeldeinformationen.

Bevor Sie fortfahren, führen Sie folgen Schritte aus:

1. Moderne Authentifizierung mit Microsoft Office 365 wurde aktiviert:
2. Aktivieren Sie Office 365-Endpunkte, -URLS und -IP-Adressbereiche in Ihrer Firewall, um eine optimale Netzwerkverbindung zu gewährleisten. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter URLs und IP-Adressbereiche für Office 365.

Voraussetzungen bezüglich Richtlinien in Citrix Endpoint Management

Aktivieren Sie die folgenden Richtlinien in der Citrix Endpoint Management-Konsole:

Für iOS-Geräte:

- **Office 365-Authentifizierungsmethode:** Über diese Richtlinie geben Sie den OAuth-Mechanismus an, der beim Konfigurieren eines Kontos in Office 365 für die Authentifizierung verwendet werden soll. Für die Richtlinie müssen Sie die folgenden Werte konfigurieren:
  - **Nicht OAuth verwenden:** Verwenden Sie diese Richtlinie für die Standardauthentifizierung bei der Kontokonfiguration.
  - **OAuth mit Benutzername und Kennwort verwenden:** Verwenden Sie diese Richtlinie für das OAuth-Protokoll bei der Authentifizierung. Die Benutzer müssen ihren Benutzernamen und ihr Kennwort sowie optional einen Multifaktor-Authentifizierungscode für den OAuth-Fluss angeben.

  - **OAuth mit Clientzertifikat verwenden** Verwenden Sie diese Richtlinie, wenn Office 365 für die zertifikatsbasierte Authentifizierung konfiguriert ist. Die Standardkonfiguration ist **Nicht OAuth verwenden**.

Android-Geräte:

- **Moderne Authentifizierung für Office 365 verwenden:** Verwenden Sie diese Richtlinie für das OAuth-Protokoll bei der Authentifizierung.
- **Benutzerdefinierter Benutzeragent für moderne Authentifizierung:** Verwenden Sie diese Richtlinie zum Ändern der Standard-Benutzeragent-Zeichenfolge für die moderne Authentifizierung.

Richtlinien für iOS- und Android-Geräte:

- **Vertrauenswürdige Exchange Online-Hostnamen:** Verwenden Sie diese Richtlinie zum Definieren einer Liste vertrauenswürdiger Exchange Online-Hostnamen, die den OAuth-Mechanismus für die Authentifizierung beim Konfigurieren eines Kontos verwenden. Verwenden Sie Kommas zum Trennen der Einträge, beispielsweise server.firma.de, server.firma.com. Die Liste kann einen Standardwert oder Vanity-URLs enthalten, sie darf jedoch nicht leer sein. Der Standardwert ist **outlook.office365.com**.
- **Vertrauenswürdige AD FS-Hostnamen:** Definieren Sie eine Liste mit Namen vertrauenswürdiger AD FS-Hosts für Webseiten, auf denen das Kennwort bei der Office 365-OAuth-Authentifizierung eingetragen wird. Die Angabe erfolgt durch Kommas getrennt, z. B. `sts.companyname.com`, `sts.company.co.uk`. Wenn die Liste leer ist, trägt Secure Mail Kennwörter nicht automatisch ein. Secure Mail vergleicht die aufgelisteten Hostnamen mit dem Hostnamen der Webseite, die bei der Office 365-Authentifizierung erkannt wird, und überprüft, ob die Seite HTTPS verwendet. Ist beispielsweise der Hostname `sts.company.com` in der Liste enthalten und ein Benutzer navigiert zu `https://sts.company.com`, trägt Secure Mail das Kennwort ein, wenn die Seite ein Kennwortfeld enthält. Der Standardwert ist `login.microsoftonline.com`.
- **Secure Mail Exchange Server:** Verwenden Sie diese Richtlinie zum Angeben der Adresse Ihres Exchange-Servers.

Die moderne Authentifizierung kann jetzt für Secure Mail für iOS verwendet werden, sobald die Richtlinien auf dem Gerät aktualisiert wurden.

Einschränkungen

- Wenn Sie die moderne Authentifizierung verwenden, sind keine Pushbenachrichtigungen mit Rich-Inhalt unter iOS möglich. Informationen zu Pushbenachrichtigungen mit Rich-Inhalt finden Sie unter Pushbenachrichtigungen für Secure Mail.
- Mehrfachkonten werden bei Verwendung der zertifikatbasierten Authentifizierung nicht unterstützt.

Secure Mail-Richtlinien

Die folgenden Tabellen enthalten die je nach Exchange-Infrastruktur erforderlichen Secure Mail-Richtlinien:

Exchange-Infrastruktur	Moderne Authentifizierung mit Office 365	Vertrauenswürdige AD FS-Hostnamen	Vertrauenswürdige Exchange Online-Hostnamen
On-premise	AUS	Nicht verfügbar	Nicht verfügbar
Hybrid*	EIN	AD FS/IDP	`Outlook.office365.com` oder Vanity-URL
Exchange Online	EIN	AD FS/IDP	`Outlook.office365.com` oder Vanity-URL

Exchange-Infrastruktur	Secure Mail Exchange Server	Hintergrundnetzwerkdienste (iOS)	Hintergrundnetzwerkdienste (Android)
On-premise	On-Premises-Exchange-Hostname	On-premise	On-premise
Hybrid*	On-Premises, Exchange Online-Hostnamen	On-Premises, On-Premises-Exchange-Hostname	On-Premise, On-Premise-Exchange-Hostname, AD FS/IDP (nur intern)
Exchange Online	`Outlook.office365.com`	Exchange Online-Hostnamen	On-Premise-Exchange-Hostname, AD FS, IDP

*Secure Mail unterstützt eine hybride Exchange-Infrastruktur mit migrierten Postfächern.

Wird ein On-Premise-Postfach zu Exchange Online migriert, erkennt Secure Mail dies automatisch und fordert den Benutzer zur modernen Authentifizierung auf, ohne dass sein Konto neu konfiguriert werden muss.

> **Hinweis:**
>
> Konfigurieren Sie Hintergrundnetzwerkdienste nur dann, wenn der E-Mail-Server und AD FS intern sind.

Matrix: Secure Mail mit OAuth-Unterstützung

Die folgende Tabelle enthält die Matrix der Secure Mail-OAuth-Unterstützung für iOS- und Android-Geräte:

Authentifizierungstyp	IDP/AD FS extern	IDP/AD FS intern	Azure AD	Intune
Benutzername und Kennwort	Ja	Ja	Ja	Ja
Clientzertifikat	Ja	Nur Android	Nein	Nein

Hintergrunddienste für Secure Mail

April 26, 2019

Für den Zugriff auf den E-Mail-Server über Citrix Gateway müssen Sie Hintergrunddienste für Secure Mail konfigurieren. Wenn Sie Secure Mail zu Citrix Endpoint Management (zuvor "XenMobile") hinzufügen, konfigurieren Sie Hintergrunddienste in MDX-App-Richtlinieneinstellungen.

Konfigurieren von Hintergrunddiensten für Secure Mail

1. Melden Sie mit Administrator-Anmeldeinformationen bei der Endpoint Management-Konsole an.
2. Klicken Sie in der Konsole auf die Registerkarte **Konfigurieren** gefolgt von **Apps**, wählen Sie die Secure Mail-App aus und klicken Sie dann auf **Bearbeiten**.
3. Wählen Sie auf der Seite **MDX-Richtlinieneinstellungen** im Bereich **Plattform** iOS oder Android aus.
4. Konfigurieren Sie unter **App-Einstellungen** die Richtlinien.

MDX-App-Richtlinien für die Konfiguration von Hintergrunddiensten

Die nachfolgend aufgeführten MDX-App-Richtlinien wirken sich auf die Secure Mail-Kommunikation mit Citrix Gateway, dem Citrix Endpoint Management-Server, STA-Servern (Secure Ticket Authority) und dem E-Mail-Server aus.

Netzwerkzugriff: Die Netzwerkzugriffsrichtlinie legt fest, ob Secure Mail ein VPN für den Zugriff auf Hintergrund-Netzwerkdienste verwenden kann oder ob der gesamte Datenverkehr uneingeschränkt über das Internet läuft.

- Wenn die Netzwerkzugriffsrichtlinie auf **Tunnel zum internen Netzwerk**festgelegt ist, wird nur der Datenverkehr von in Hintergrund-Netzwerkdiensten aufgeführten URLs durch Citrix Gateway geleitet. Der restliche Datenverkehr läuft uneingeschränkt über das Internet. Standardmäßig ist der Secure Mail-Zugriff auf **Tunnel zum internen Netzwerk** festgelegt.
- Wenn die Netzwerkzugriffsrichtlinie auf **Uneingeschränkt**festgelegt ist, wird der gesamte von Secure Mail ausgehende Datenverkehr uneingeschränkt über das Internet geleitet. Das VPN wird nicht für den Zugriff auf Hintergrunddienste verwendet.

Secure Mail Exchange Server: Legen Sie die Richtlinie **Secure Mail Exchange Server** auf den vollqualifizierten Domänennamen (FQDN) des E-Mail-Servers fest.

Hintergrundnetzwerkdienste: Die Richtlinie "Hintergrundnetzwerkdienste" enthält die Liste der E-Mail-Server, die Zugriff über Citrix Gateway haben. Listen Sie die Hostnamen und Portnummern durch Kommas getrennt auf. Zwischen den Werten dürfen keine Leerzeichen stehen. Verwenden Sie für E-Mail-Server-Adressen `hostnameFQDN:portnumber`. Beispiel: `mail1.example.com:443,mail2.example.com:443` (kein Leerzeichen vor oder nach dem Komma).

Gateway für Hintergrundnetzwerkdienst: Mit der Richtlinie "Gateway für Hintergrundnetzwerkdienst" können Sie das Citrix Gateway zur Verwendung durch Secure Mail für die Verbindung mit dem E-Mail-Server angeben. Verwenden Sie als Citrix Gateway-Adresse `citrixgatewayFQDN:portnumber`. Beispiel: `gateway3.example.com:443`.

Ticketablauf für Hintergrunddienste: Mit dieser Richtlinie legen Sie die Gültigkeitsdauer des Hintergrund-Netzwerkdiensttickets fest. Wenn Secure Mail über Citrix Gateway die Verbindung mit einem E-Mail-Server herstellt, stellt Citrix Endpoint Management einen Token aus, der für die Verbindung mit dem internen E-Mail-Server verwendet wird. Diese Einstellung bestimmt die Zeitdauer, die Secure Mail den Token verwenden kann. Wenn der Token aktiv ist, ist kein neuer Token für die Authentifizierung und die Verbindung zum Mailserver erforderlich. Wenn das Zeitlimit abläuft, müssen Benutzer sich neu anmelden, damit ein neues Token generiert wird. Die Standardeinstellung für den Token ist 168 Stunden (7 Tage).

Weitere Informationen zu MDX-App-Richtlinien für Hintergrunddienste finden Sie unter:

- Richtlinien für Secure Mail-App-Einstellungen für Android
- Richtlinien für Secure Mail-App-Einstellungen für iOS

Die folgende Abbildung zeigt den Kommunikationsfluss und die Punkte, an denen die Richtlinien wirksam werden.

Die folgenden Abbildungen zeigen die Arten der Secure Mail-Verbindungen mit einem Mailserver. Nach jeder Abbildung finden Sie eine Liste mit zugehörigen Richtlinieneinstellungen.

Direkte Verbindung mit einem E-Mail-Server:

Richtlinien für eine direkte Verbindung mit einem Mailserver:

- Netzwerkzugriff: **Uneingeschränkt**

Bei uneingeschränktem Netzwerkzugriff werden die folgenden Richtlinien nicht angewendet:

- Hintergrundnetzwerkdienste
- Ticketablauf für Hintergrunddienste
- Gateway für Hintergrundnetzwerkdienst

Verbindung mit einem E-Mail-Server über die STA:

Richtlinien für die Verbindung mit einem E-Mail-Server über die STA:

- Netzwerkzugriff: **Tunnel zum internen Netzwerk**
- Hintergrundnetzwerkdienste: `mail.example.com:443,mail1.example1.com:443`
- Ticketablauf für Hintergrunddienste: **168**
- Gateway für Hintergrundnetzwerkdienst: `gateway3.example.com:443`

> Hinweis:
>
> Citrix empfiehlt die Verwendung einer STA-Verbindung für Secure Mail, da sie Sitzungsverbindungen von langer Dauer unterstützt.

Weitere Informationen zur STA finden Sie in diesem Citrix Knowledge Center-Artikel.

Integration von Exchange Server oder IBM Notes Traveler-Server

February 11, 2019

Damit Secure Mail mit Ihren E-Mail-Servern synchronisiert bleibt, können Sie es in einen Exchange- oder IBM Notes Traveler-Server im internen Netzwerk oder hinter Citrix Gateway integrieren.

- Informationen zum Konfigurieren von Hintergrunddiensten für Secure Mail finden Sie unter Hintergrunddienste für Secure Mail.
- Informationen zum Konfigurieren von IBM Notes Traveler Server für Secure Mail finden Sie unter Konfigurieren eines IBM Notes Traveler-Servers für Secure Mail.

> **Wichtig:**
>
> Sie können mit IBM Notes Traveler (zuvor IBM Lotus Notes Traveler) keine E-Mails von Secure Mail synchronisieren. Diese Drittanbieterfunktion von Lotus Notes wird derzeit nicht unterstützt. Wenn Sie beispielsweise eine Besprechungsmail aus Secure Mail löschen, wird die Mail auf dem IBM Notes Traveler-Server nicht gelöscht. [CXM-47936]
> Informationen zu bekannten Einschränkungen bei IBM/Lotus Notes finden Sie in diesem Citrix Blogbeitrag.

Die Synchronisierung ist auch für Secure Notes und Secure Tasks verfügbar. Beachten Sie jedoch, dass Secure Notes und Secure Tasks am 31. Dezember 2018 das Ende des Lebenszyklus (End Of Life, EOL) erreicht haben. Weitere Informationen finden Sie unter Ende des Lebenszyklus und veraltete Apps.

- Zum Synchronisieren von Secure Notes für iOS integrieren Sie es in einen Exchange-Server.
- Zum Synchronisieren von Secure Notes und Secure Tasks für Android verwenden Sie das Secure Mail für Android-Konto.

Wenn Sie Secure Mail, Secure Notes und Secure Tasks zu Citrix Endpoint Management (zuvor "XenMobile") hinzufügen, konfigurieren Sie die MDX-Richtlinien wie unter MDX-App-Richtlinien für die Konfiguration von Hintergrunddiensten beschrieben.

> **Hinweis:**
>
> Secure Mail für Android und Secure Mail für iOS unterstützen den vollständigen Pfad eines Notes Traveler-Servers. Beispiel: `https://mail.example.com/traveler/Microsoft-Server-ActiveSync`.
>
> Es ist nicht mehr erforderlich, das Domino-Verzeichnis mit Website-Ersetzungsregeln für den Traveler-Server zu konfigurieren.

Konfigurieren eines IBM Notes Traveler-Servers für Secure Mail

In IBM Notes-Umgebungen müssen Sie den IBM Notes Traveler-Server konfigurieren, bevor Sie Secure Mail bereitstellen. Dieser Abschnitt enthält eine Darstellung der Bereitstellung dieser Konfiguration und die Systemanforderungen.

> **Wichtig:**
>
> Notes Traveler-Server, die SSL 3.0 verwenden, können durch einen POODLE-Angriff (Padding Oracle On Downgraded Legacy Encryption) gefährdet sein. Dies ist ein Man-in-the-middle-Angriff, der sich auf alle Apps auswirkt, die eine Verbindung zum Server mit SSL 3.0 herstellen. Um einem POODLE-Angriff vorzubeugen, deaktiviert Secure Mail standardmäßig die SSL 3.0-Verbindungen und verwendet für Verbindungen mit dem Server TLS 1.0. Daher kann Secure Mail keine Verbindung mit einem Notes Traveler-Server herstellen, der SSL 3.0 verwendet. Informationen zu einem empfohlenen Workaround finden Sie im Abschnitt "Konfigurieren der SSL/TLS-Sicherheitsebene unter Integration von Exchange Server oder IBM Notes Traveler-Server.

In IBM Notes-Umgebungen müssen Sie den IBM Notes Traveler-Server konfigurieren, bevor Sie Secure Mail bereitstellen.

Im folgenden Diagramm ist die Netzwerkplatzierung von IBM Notes Traveler-Servern und einem IBM Domino-Mailserver in einer Beispielbereitstellung dargestellt.

Systemanforderungen

Anforderungen an den Infrastrukturserver

- IBM Domino Mail Server
- IBM Notes Traveler 9.0.1

Authentifizierungsprotokolle

- Domino-Datenbank
- Lotus Notes-Authentifizierungsprotokoll
- Lightweight Directory Authentication Protocol

Portanforderungen

- Exchange: Der SSL-Standardport ist 443.
- IBM Notes: SSL wird auf Port 443 unterstützt. Andere Protokolle als SSL werden standardmäßig auf Port 80 unterstützt.

Konfigurieren der SSL/TLS- Sicherheitsebene

Citrix hat Änderungen an Secure Mail zur Beseitigung eines durch den POODLE-Angriff entstandenen Sicherheitsrisikos (siehe “Wichtiger Hinweis” oben) vorgenommen. Daher wird als Workaround für Notes Traveler-Server 9.0, die SSL 3.0 verwenden, zum Aktivieren von Verbindungen die Verwendung von TLS 1.2 auf dem Traveler-Server empfohlen.

IBM haben einen Patch, der die Verwendung von SSL 3.0 für die sichere Kommunikation zwischen Servern mit Notes Traveler verhindert. Dieser im November 2014 veröffentlichte Patch ist als vorläufiger Fix in Updates für die folgenden Versionen von Notes Traveler-Server enthalten: 9.0.1 IF7, 9.0.0.1 IF8 und 8.5.3 Upgrade Pack 2 IF8 (einschließlich allen zukünftigen Releases). Weitere Informationen zu diesem Patch finden unter LO82423: DISABLE SSLV3 FOR TRAVELER SERVER TO SERVER COMMUNICATION.

Sie können dieses Problem auch umgehen, indem Sie beim Hinzufügen von Secure Mail zu Endpoint Management die Einstellung der Richtlinie “Connection security level” in **SSLv3 und TLS** ändern. Aktuelle Informationen zu diesem Problem finden Sie unter SSLv3 Connections Disabled by Default on Secure Mail 10.0.3.

Die folgenden Tabellen enthalten die von Secure Mail unterstützten Protokolle nach Betriebssystem, basierend auf dem Wert der Richtlinie “Verbindungssicherheitsstufe”. Der E-Mail-Server muss das Protokoll ebenfalls verwenden können.

Die folgende Tabelle enthält die unterstützten Protokolle für Secure Mail bei der Verbindungssicherheitsstufe SSLv3 und TLS.

Betriebssystemtyp	SSLv3	TLS
iOS 9 und höher	Nein	Ja
Älter als Android M	Ja	Ja
Android M und Android N	Ja	Ja
Android O	Nein	Ja

Die folgende Tabelle enthält die unterstützten Protokolle für Secure Mail bei der Verbindungssicherheitsstufe TLS.

Betriebssystemtyp	SSLv3	TLS
iOS 9 und höher	Nein	Ja
Älter als Android M	Nein	Ja
Android M und Android N	Nein	Ja
Android O	Nein	Ja

Konfigurieren von Notes Traveler-Server

Die folgenden Informationen entsprechen den Konfigurationsseiten im IBM Domino Administrator Client.

- **Security:** Die Internetauthentifizierung ist auf “Fewer name variations with higher security” festgelegt. Mit dieser Einstellung erfolgt die Zuordnung von UID zu AD User ID in LDAP-Authentifizierungsprotokollen.
- **NOTES.INI Settings:** Fügen Sie **NTS_AS_ENFORCE_POLICY**=**false** hinzu. Dadurch können Secure Mail-Richtlinien über Endpoint Management statt Traveler verwaltet werden. Diese Einstellung kann einen Konflikt mit aktuellen Kundenbereitstellungen auslösen, doch sie vereinfacht die Geräteverwaltung in Endpoint Management-Bereitstellungen.
- **Synchronization protocols:** SyncML unter IBM Notes und die Synchronisierung von Mobilgeräten werden derzeit von Secure Mail nicht unterstützt. Secure Mail synchronisiert E-Mail-, Kalender- und Kontaktobjekte über das in den Traveler-Server integrierte Microsoft ActiveSync-Protokoll. Wird SyncML als primäres Protokoll erzwungen, kann Secure Mail keine Rückverbindung über die Traveler-Infrastruktur herstellen.

- **Domino Directory Configuration - Web Internet Sites:** Override Session Authentication für /traveler zur Deaktivierung der formularbasierten Authentifizierung

S/MIME für Secure Mail

April 4, 2019

Secure Mail unterstützt Secure/Multipurpose Internet Mail Extensions (S/MIME), sodass Benutzer Nachrichten zur Erhöhung der Sicherheit signieren und verschlüsseln können. Durch die Signatur kann der Empfänger sicher sein, dass die Nachricht von dem identifizierten Absender gesendet wurde und nicht von einem Betrüger. Bei Verschlüsselung können nur die Empfänger mit einem kompatiblen Zertifikat die Nachricht öffnen.

Weitere Informationen zu S/MIME finden Sie unter Microsoft TechNet.

In der folgenden Tabelle bedeutet ein X, dass ein S/MIME-Feature von Secure Mail auf einem Gerätebetriebssystem unterstützt wird.

S/MIME-Feature	iOS	Android
Integration mit digitalen Identitätsanbietern: Sie können Secure Mail in einen unterstützten digitalen Identitätsanbieter (Drittanbietertool) integrieren. Der Identitätsanbieterhost stellt einer Identitätsanbieter-App auf Benutzergeräten Zertifikate zur Verfügung. Diese Anwendung sendet Zertifikate an den freigegebenen Endpoint Management-Tresor, ein sicherer Speicher für vertrauliche Anwendungsdaten. Secure Mail ruft Zertifikate aus dem freigegebenen Tresor ab. Weitere Informationen finden Sie unter Integration mit einem digitalen Identitätsanbieter.	X	
Unterstützung für abgeleitete Anmeldeinformationen	Secure Mail unterstützt die Verwendung von abgeleiteten Anmeldeinformationen als Zertifikatquelle. Weitere Informationen zu abgeleiteten Anmeldeinformationen finden Sie unter Abgeleitete Anmeldeinformationen für iOS.	

S/MIME-Feature	iOS	Android
Zertifikatbereitstellung per E-Mail: Zum Bereitstellen von Zertifikaten per E-Mail müssen Sie Zertifikatvorlagen erstellen und mit diesen Vorlagen Benutzerzertifikate anfordern. Nach der Installation und Überprüfung der Zertifikate exportieren Sie die Benutzerzertifikate und senden sie per E-Mail an die Benutzer. Die Benutzer öffnen dann die E-Mail in Secure Mail und importieren die Zertifikate. Weitere Informationen finden Sie unter Verteilen von Zertifikaten per E-Mail.	X	X
Automatischer Import von Einzweckzertifikaten: Secure Mail erkennt, ob ein Zertifikat nur zum Signieren oder nur zum Verschlüsseln ist. Dann wird das Zertifikat automatisch importiert und der Benutzer wird benachrichtigt. Wenn ein Zertifikat für beide Zwecke ist, werden die Benutzer aufgefordert, es zu importieren.	X	

Integration mit einem digitalen Identitätsanbieter

Das folgende Diagramm zeigt den Weg des Zertifikats vom digitalen Identitätsanbieterhost zu Secure Mail. Dieser ergibt sich, wenn Sie Secure Mail in einen unterstützten digitalen Identitätsanbieter (Drit-

tanbietertool) integrieren.

Der freigegebene MDX-Tresor ist ein sicherer Speicher für vertrauliche App-Daten wie etwa Zertifikate. Nur die von Endpoint Management aktivierte App kann auf den freigegebenen Tresor zugreifen.

Voraussetzungen

Secure Mail unterstützt die Integration in Entrust IdentityGuard.

Konfigurieren der Integration

1. Bereiten Sie die Identitätsanbieter-App vor und stellen Sie diese den Benutzern bereit:
    - Wenden Sie sich an Entrust, um die IPA-Datei zum Umschließen zu erhalten.
    - Umschließen Sie die App mit dem MDX Toolkit.

      Verwenden Sie eine eindeutige App-ID für die App, wenn Sie sie für Benutzer bereitstellen, die bereits über eine Version dieser App außerhalb der Endpoint Management-Umgebung verfügen. Verwenden Sie das gleiche Provisioningprofil für diese App und für Secure Mail.
    - Fügen Sie die App zu Endpoint Management hinzu und veröffentlichen Sie sie im Endpoint Management App Store.
    - Teilen Sie den Benutzern mit, dass sie die Identitätsanbieter-App über Secure Hub installieren müssen. Geben Sie nach Bedarf Anleitungen zu Schritten, die nach der Installation ausgeführt werden müssen.

      Abhängig davon, wie Sie die S/MIME-Richtlinien für Secure Mail im nächsten Schritt konfigurieren, fordert Secure Mail Benutzer u. U. zur Installation von Zertifikaten oder zum Aktivieren von S/MIME in den Secure Mail-Einstellungen auf. Schrittweise Anleitungen für diese beiden Verfahren finden Sie in Aktivieren von S/MIME für Secure Mail für iOS.
2. Wenn Sie Secure Mail zu Endpoint Management hinzufügen, konfigurieren Sie die folgenden Richtlinien:
    - Legen Sie die Richtlinie für die S/MIME-Zertifikatquelle auf **Freigegebener Tresor** fest. Secure Mail verwendet dann die im freigegebenen Tresor gespeicherten Zertifikate des digitalen Identitätsanbieters.
    - Damit S/MIME während des ersten Starts von Secure Mail aktiviert wird, konfigurieren Sie die Richtlinie “S/MIME bei erstem Secure Mail-Start aktivieren”. Die Richtlinie legt fest, ob Secure Mail S/MIME aktiviert, wenn Zertifikate im freigegebenen Tresor sind. Wenn keine Zertifikate verfügbar sind, fordert Secure Mail die Benutzer zum Importieren von Zertifikaten auf. Wenn die Richtlinie nicht aktiviert ist, können die Benutzer S/MIME in den

Secure Mail-Einstellungen aktivieren. Standardmäßig aktiviert Secure Mail S/MIME nicht, daher müssen die Benutzer S/MIME in den Secure Mail-Einstellungen aktivieren.

Verwenden von abgeleiteten Anmeldeinformationen

Statt einer Integration mit einem digitalen Identitätsanbieter können Sie die Verwendung von abgeleiteten Anmeldeinformationen zulassen.

Wenn Sie Secure Mail zu Endpoint Management hinzufügen, legen Sie für die Richtlinie "S/MIME-Zertifikatquelle" die Option **Abgeleitete Anmeldeinformationen** fest. Weitere Informationen zu abgeleiteten Anmeldeinformationen finden Sie unter Abgeleitete Anmeldeinformationen für iOS.

Verteilen von Zertifikaten per E-Mail

Statt der Integration mit einem digitalen Identitätsanbieter oder der Verwendung von abgeleiteten Anmeldeinformationen können Sie Benutzern Zertifikate per E-Mail bereitstellen. Für diese Option sind die folgenden allgemeinen Schritte erforderlich.

1. Aktivieren Sie mit dem Server-Manager die Webregistrierung für die Microsoft-Zertifikatdienste und überprüfen Sie die Authentifizierungseinstellungen in IIS.
2. Erstellen Sie Zertifikatvorlagen zum Signieren und Verschlüsseln von E-Mail-Nachrichten. Fordern Sie mit diesen Vorlagen Benutzerzertifikate an.
3. Installieren und validieren Sie die Zertifikate. Exportieren Sie dann die Benutzerzertifikate und senden Sie sie an die Benutzer.
4. Die Benutzer öffnen die E-Mail in Secure Mail und importieren die Zertifikate. Die Zertifikate sind daher nur für Secure Mail verfügbar. Sie werden nicht unter dem iOS-Profil für S/MIME angezeigt.

Voraussetzungen

Die Anweisungen in diesem Abschnitt basieren auf den folgenden Komponenten:

- XenMobile Server 10 und höher
- Eine unterstützte Version von Citrix Gateway (bisher "NetScaler Gateway")
- Secure Mail für iOS (Mindestversion 10.8.10); Secure Mail für Android-Geräte (Mindestversion 10.8.10)
- Microsoft Windows Server 2008 R2 oder höher mit Microsoft-Zertifikatdiensten als Stammzertifizierungsstelle (ZS)
- Microsoft Exchange:
  - Exchange Server 2016 Kumulatives Update 4

  - Exchange Server 2013 Kumulatives Update 15
  - Exchange Server 2010 SP3 Update Rollup 16

Sorgen Sie vor dem Konfigurieren von S/MIME dafür, dass die folgenden Voraussetzungen erfüllt sind:

- Stellen Sie das Stamm- und Zwischenzertifikat auf den mobilen Geräten manuell oder über eine Anmeldeinformationsrichtlinie für Geräte in Endpoint Management bereit. Weitere Informationen finden Sie unter Anmeldeinformationsrichtlinie.
- Wenn Sie private Serverzertifikate zum Sichern des ActiveSync-Datenverkehrs an Exchange Server verwenden, müssen alle Stamm- und Zwischenzertifikate auf den mobilen Geräten installiert sein.

Aktivieren der Webregistrierung für Microsoft-Zertifikatdienste

1. Wechseln Sie zu **Verwaltungstools** und wählen Sie dann **Server-Manager**.
2. Prüfen Sie unter **Active Directory-Zertifikatdienste**, ob die **Zertifizierungsstellen-Webregistrierung** installiert ist.
3. Klicken Sie auf **Rollendienste hinzufügen**, um die Zertifizierungsstellen-Webregistrierung, falls erforderlich, hinzuzufügen.
4. Aktivieren Sie das Kontrollkästchen für **Zertifizierungsstellen-Webregistrierung** und klicken Sie auf **Weiter**.
5. Klicken Sie auf **Schließen** oder **Fertig stellen**, wenn die Installation abgeschlossen ist.

Überprüfen der Authentifizierungseinstellungen in IIS

- Stellen Sie sicher, dass die Site für die Webregistrierung, die zum Anfordern von Benutzerzertifikaten verwendet wird (z. B. `https://ad.domain.com/certsrv/`), mit einem privaten oder öffentlichen HTTPS-Serverzertifikat gesichert ist.
- Sie müssen auf die Webregistrierungssite über HTTPS zugreifen.

1. Wechseln Sie zu **Verwaltungstools** und wählen Sie dann **Server-Manager**.
2. Überprüfen Sie unter **Webserver (IIS)** die **Rollendienste**. Stellen Sie sicher, dass Clientzertifikatzuordnung-Authentifizierung und IIS Clientzertifikatzuordnung-Authentifizierung installiert sind. Falls nicht, installieren Sie diese Rollendienste.
3. Wechseln Sie zu **Verwaltungstools** und wählen Sie **Internetinformationsdienste (IIS)-Manager**.
4. Wählen Sie im linken Bereich des Fensters des **IIS-Managers** den Server aus, auf dem die IIS-Instanz für die Webregistrierung ausgeführt wird.
5. Klicken Sie auf **Authentifizierung**.
6. Stellen Sie sicher, dass für **Active Directory-Clientzertifikatauthentifizierung** der Status **Aktiviert** angezeigt wird.

7. Klicken Sie im rechten Bereich auf **Sites > Standardsite für Microsoft Internetinformationsdienste > Bindungen**.
8. Fügen Sie eine HTTPS-Bindung hinzu, wenn keine vorhanden ist.
9. Wechseln Sie zu Standardwebsite-Startseite.
10. Klicken Sie auf **SSL-Einstellungen** und dann auf **Clientzertifikate akzeptieren**.

Erstellen von Zertifikatvorlagen

Für die Signatur und Verschlüsselung von E-Mail empfiehlt Citrix, dass Sie Zertifikate unter Microsoft Active Directory-Zertifikatdienste erstellen. Wenn Sie dasselbe Zertifikat für beide Zwecke verwenden und das Verschlüsselungszertifikat archivieren, sind die Wiederherstellung des Signaturzertifikats und ein Identitätswechsel möglich.

Mit der folgenden Vorgehensweise werden die Zertifikatvorlagen auf dem Zertifizierungsstellenserver (ZS-Server) dupliziert:

- Nur Exchange-Signatur (zum Signieren)
- Exchange-Benutzer (zur Verschlüsselung)

1. Öffnen Sie das Zertifizierungsstellen-Snap-In.
2. Erweitern Sie die Zertifizierungsstelle und wechseln Sie zu **Zertifikatvorlagen**.
3. Klicken Sie mit der rechten Maustaste auf **Verwalten**.
4. Suchen Sie die Vorlage “Nur Exchange-Signatur”, klicken Sie mit der rechten Maustaste auf die Vorlage und klicken Sie dann auf **Doppelte Vorlage**.
5. Weisen Sie einen Namen zu.
6. Aktivieren Sie das Kontrollkästchen für **Zertifikat in Active Directory veröffentlichen**.

   > **Hinweis:**
   >
   > Wenn Sie das Kontrollkästchen **Zertifikat in Active Directory veröffentlichen** nicht aktivieren, müssen die Benutzer die Benutzerzertifikate für Signatur und Verschlüsselung manuell veröffentlichen. Dies ist möglich über **Outlook-E-Mail-Client > Vertrauensstellungscenter > E-Mail-Sicherheit > In GAL veröffentlichen**.

7. Klicken Sie auf die Registerkarte **Anforderungsverarbeitung** und legen Sie folgende Parameter fest:
   - **Zweck:** Signatur
   - **Minimale Schlüsselgröße:** 2048
   - Kontrollkästchen **Exportieren von privatem Schlüssel zulassen** aktiviert
   - Kontrollkästchen **Antragsteller ohne Benutzereingabe registrieren** aktiviert

8. Klicken Sie auf die Registerkarte **Sicherheit** und stellen Sie sicher, dass unter **Gruppen- oder Benutzernamen** die Gruppe **Authentifizierte Benutzer** (oder nach Wunsch eine andere Domänensicherheitsgruppe) hinzugefügt ist. Stellen Sie außerdem sicher, dass unter **Berechtigungen für authentifizierte Benutzer** die Kontrollkästchen **Lesen und Registrieren** für **Zulassen** aktiviert sind.
9. Für alle anderen Registerkarten und Parameter behalten Sie die Standardeinstellungen bei.
10. Klicken Sie für **Zertifikatvorlagen** auf **Exchange-Benutzer** und wiederholen Sie die Schritte 4 bis 9.

    Verwenden Sie für die neue Exchange-Benutzervorlage die gleichen Standardeinstellungen wie für die Originalvorlage.
11. Klicken Sie auf die Registerkarte **Anforderungsverarbeitung** und legen Sie folgende Parameter fest:
    - **Zweck:** Verschlüsselung
    - **Minimale Schlüsselgröße:** 2048
    - Kontrollkästchen **Exportieren von privatem Schlüssel zulassen** aktiviert
    - Kontrollkästchen **Antragsteller ohne Benutzereingabe registrieren** aktiviert
12. Wenn beide Vorlagen erstellt sind, geben Sie beide aus. Klicken Sie auf **Neu** und klicken Sie dann auf **Auszustellende Zertifikatvorlage**.

Anfordern von Benutzerzertifikaten

Bei dieser Vorgehensweise wird “User1” zum Navigieren zur Webregistrierungsseite, z. B. `https://ad.domain.com/certsrv/`, verwendet. Bei der Vorgehensweise werden zwei neue Benutzerzertifikate für sichere E-Mail angefordert: eines für die Signierung und das zweite für die Verschlüsselung. Sie können die Vorgehensweise für andere Domänenbenutzer, die die Verwendung von S/MIME über Secure Mail benötigen, wiederholen.

Zum Erstellen der Benutzerzertifikate für die Signierung und Verschlüsselung wird die manuelle Registrierung über die Webregistrierungssite (z. B. `https://ad.domain.com/certsrv/`) auf Microsoft-Zertifikatdienste verwendet. Eine Alternative wäre das Konfigurieren einer automatischen Registrierung über eine Gruppenrichtlinie für die Gruppe von Benutzern, die das Feature verwenden sollen.

1. Öffnen Sie auf einem Windows-Computer Internet Explorer und navigieren Sie zu der Webregistrierungssite, um ein Benutzerzertifikat anzufordern.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie sich unter dem richtigen Domänenbenutzerkonto anmelden, um das Zertifikat anzufordern.

2. Wenn Sie angemeldet sind, klicken Sie auf **Zertifikat anfordern**.
3. Klicken Sie auf **Erweiterte Zertifikatanforderung**.
4. Klicken Sie auf **Eine Zertifikatanforderung an diese Zertifizierungsstelle erstellen und einreichen**.
5. Erstellen Sie das Benutzerzertifikat zum Signieren. Wählen Sie den entsprechenden Vorlagennamen aus, geben Sie Ihre Benutzereinstellungen ein, und wählen Sie neben **Anforderungsformat** die Option **PKCS10** aus.

   Die Anforderung wurde gesendet.
6. Klicken Sie auf **Dieses Zertifikat installieren**.
7. Vergewissern Sie sich, dass das Zertifikat erfolgreich installiert wurde.
8. Wiederholen Sie das Verfahren zur Verschlüsselung von E-Mail. Bleiben Sie als der gleiche Benutzer bei der Webregistrierungssite angemeldet und klicken Sie auf den Link Startseite, um ein neues Zertifikat anzufordern.
9. Wählen Sie die neue Vorlage für die Verschlüsselung aus und legen Sie dann die gleichen Benutzereinstellungen wie in Schritt 5 fest.
10. Stellen Sie sicher, dass das Zertifikat erfolgreich installiert wurde, und wiederholen Sie das Verfahren zum Erstellen eines Benutzerzertifikatpaars für einen weiteren Domänenbenutzer. Bei diesem Verfahren werden die gleichen Schritte ausgeführt und ein Zertifikatpaar für “User2” erstellt.

    > **Hinweis:**
    >
    > Bei dem Verfahren wird der gleiche Windows-Computer zum Anfordern des zweiten Zertifikatpaars für “User2” verwendet.

Überprüfen veröffentlichter Zertifikate

1. Um sich zu vergewissern, dass die Zertifikate im Domänenbenutzerprofil richtig installiert sind, wechseln Sie zu **Active Directory-Benutzer und -Computer > Anzeigen > Erweiterte Funktionen**.
2. Wechseln Sie zu den Eigenschaften des Benutzers (User1 für dieses Beispiel) und klicken Sie dann auf die Registerkarte **Veröffentlichte Zertifikate**. Vergewissern Sie sich, dass beide Zertifikate verfügbar sind. Sie können auch sicherstellen, dass jedes Zertifikat einen bestimmten Zweck hat.

Diese Abbildung zeigt ein Zertifikat für die Verschlüsselung von E-Mail.

Diese Abbildung zeigt ein Zertifikat zum Signieren von E-Mail.

Stellen Sie Sicher, dass dem Benutzer das richtige verschlüsselte Zertifikat zugewiesen ist. Sie können dies unter **Active Directory-Benutzer und -Computer > Benutzereigenschaften** prüfen.

Secure Mail prüft das Benutzerobjektattribut userCertificate über LDAP-Abfragen. Sie können diesen Wert auf der Registerkarte **Attribut-Editor** ablesen. Wenn dieses Feld leer ist oder das falsche Benutzerzertifikat für die Verschlüsselung enthält, kann Secure Mail Nachrichten weder verschlüsseln noch entschlüsseln.

Exportieren von Benutzerzertifikaten

Mit diesem Verfahren werden die Zertifikatpaare für “User1” und “User2” im PFX-Format (PKCS #12) mit dem privaten Schlüssel exportiert. Nach dem Export werden die Zertifikate per E-Mail und unter Verwendung von Outlook Web Access (OWA) an den Benutzer gesendet.

1. Öffnen Sie die MMC-Konsole und wechseln Sie zu dem Snap-In für **Zertifikate – aktueller Benutzer**. Es werden die Zertifikatpaare für “User1” und “User2” angezeigt.
2. Klicken Sie mit der rechten Maustaste auf das Zertifikat und dann auf **Alle Aufgaben > Exportieren**.
3. Exportieren Sie den privaten Schlüssel durch Auswahl von **Ja, privaten Schlüssel exportieren**.
4. Aktivieren Sie die Kontrollkästchen **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen** und **Alle erweiterten Eigenschaften exportieren**.
5. Wiederholen Sie beim Exportieren des ersten Zertifikats das gleiche Verfahren für die restlichen Zertifikate für die Benutzer.

> **Hinweis:**
>
> Geben Sie durch die Bezeichnung deutlich an, welches Zertifikat zum Signieren und welches für die Verschlüsselung verwendet wird. Im Beispiel erhalten die Zertifikate die Bezeichnung “userX-sign.pfx” und “userX-enc.pfx”.

Senden von Zertifikaten per E-Mail

Wenn alle Zertifikate im PFX-Format exportiert wurden, können Sie sie über Outlook Web Access (OWA) per E-Mail versenden. Der Anmeldename in diesem Beispiel lautet “User1” und die E-Mail enthält beide Zertifikate.

Wiederholen Sie diesen Vorgang für “User2” bzw. weitere Benutzer in der Domäne.

Aktivieren von S/MIME für Secure Mail (iOS und Android)

Nach dem Empfang der E-Mail muss diese mit Secure Mail geöffnet und dann S/MIME mit den entsprechenden Zertifikaten zum Signieren und Verschlüsseln aktiviert werden.

Aktivieren von S/MIME mit einzelnen Signatur- und Verschlüsselungszertifikaten

1. Öffnen Sie Secure Mail und navigieren Sie zu der E-Mail mit den S/MIME-Zertifikaten.
2. Tippen Sie auf das Signaturzertifikat, um es herunterzuladen und zu importieren.
3. Geben Sie das dem privaten Schlüssel zugewiesene Kennwort ein, wenn das Signaturzertifikat vom Server exportiert wurde.

   Ihr Zertifikat wurde importiert.
4. Tippen Sie auf **Signatur aktivieren**
5. Alternativ dazu können Sie auch zu **Einstellungen** > **S/MIME** navigieren und auf “S/MIME” tippen, um das Signaturzertifikat zu aktivieren.
6. Stellen Sie im Bildschirm **Signieren** sicher, dass das richtige Signaturzertifikat importiert wurde.
7. Wechseln Sie zurück zu der E-Mail und tippen Sie auf das Verschlüsselungszertifikat, das heruntergeladen und importiert werden soll.
8. Geben Sie das dem privaten Schlüssel zugewiesene Kennwort ein, wenn das Verschlüsselungszertifikat vom Server exportiert wurde.

   Ihr Zertifikat wurde importiert.
9. Tippen Sie auf **Verschlüsselung aktivieren**
10. Alternativ dazu können Sie auch zu **Einstellungen** > **S/MIME** navigieren und auf “S/MIME” tippen, um die Option **Standardmäßig verschlüsseln** zu aktivieren.
11. Stellen Sie im Bildschirm **Verschlüsselung** sicher, dass das richtige Verschlüsselungszertifikat importiert wurde.

> **Hinweis:**
>
> a) Wenn eine mit S/MIME digital signierte E-Mail Anlagen hat und der Empfänger S/MIME nicht aktiviert hat, werden die Anlagen nicht empfangen. Dieses Verhalten ist eine Einschränkung von Active Sync. Damit Sie mit S/MIME signierte E-Mails wirklich erhalten, aktivieren Sie S/MIME in den Secure Mail-Einstellungen.
>
> b) Mit der Option **Standardmäßig verschlüsseln** können Sie für die Verschlüsselung Ihrer E-Mail erforderlichen Schritte minimieren.
> Wenn diese Funktion aktiviert ist, befindet sich Ihre E-Mail beim Verfassen im ver-

> schlüsselten Zustand.
> Wenn diese Funktion deaktiviert ist, befindet sich Ihre E-Mail während des Verfassens im unverschlüsselten Zustand und Sie müssen zum Verschlüsseln auf das Symbol **Sperren** tippen.

Aktivieren von S/MIME mit einem einzelnen Signatur- und Verschlüsselungszertifikat

1. Öffnen Sie Secure Mail und navigieren Sie zu der E-Mail mit dem S/MIME-Zertifikat.
2. Tippen Sie auf das S/SMIME-Zertifikat, um es herunterzuladen und zu importieren.
3. Geben Sie das dem privaten Schlüssel zugewiesene Kennwort ein, wenn das Zertifikat vom Server exportiert wurde.
4. Tippen Sie in den angezeigten Zertifikatsoptionen auf die entsprechende Option, um das Signaturzertifikat oder Verschlüsselungszertifikat zu importieren.
   Tippen Sie auf **Zertifikat öffnen**, um die Details zum Zertifikat anzuzeigen.

   Ihr Zertifikat wurde importiert.

   Sie können die importierten Zertifikate anzeigen, indem Sie zu **Einstellungen > S/MIME** navigieren.

Testen von S/MIME in iOS und Android

Nachdem Sie die im vorherigen Abschnitt aufgeführten Schritte durchgeführt haben, kann Ihr Empfänger Ihre signierte und verschlüsselte E-Mail lesen.

Die folgende Abbildung zeigt ein Beispiel einer verschlüsselten E-Mail, die vom Empfänger gelesen wird.

Die folgende Abbildung zeigt ein Beispiel für die Überprüfung des signierten vertrauenswürdigen Zertifikats.

Secure Mail durchsucht die Active Directory-Domäne nach den öffentlichen Verschlüsselungszertifikaten der Empfänger. Wenn ein Benutzer eine verschlüsselte Nachricht an einen Empfänger sendet, der keinen gültigen öffentlichen Verschlüsselungsschlüssel hat, wird die Nachricht unverschlüsselt gesendet. Wenn bei einer Gruppennachricht nur ein Empfänger keinen gültigen Schlüssel hat, wird die Nachricht an alle Empfänger unverschlüsselt gesendet.

Konfigurieren von öffentlichen Zertifikatquellen

Zur Verwendung öffentlicher S/MIME-Zertifikate müssen Sie die öffentliche S/MIME-Zertifikatquelle, die LDAP-Serveradresse, den LDAP-Basis-DN und die Richtlinien für den anonymen LDAP-Zugriff konfigurieren.

Führen Sie zusätzlich zu den App-Richtlinien folgende Schritte aus.

- Stellen Sie bei öffentlichen LDAP-Servern sicher, dass der Datenverkehr direkt an die LDAP-Server gesendet wird. Legen Sie für die Netzwerkrichtlinie für Secure Mail die Einstellung **Tunnel zum internen Netzwerk** fest und konfigurieren Sie Split DNS für Citrix ADC.
- Befinden sich die LDAP-Server in einem internen Netzwerk, führen Sie folgende Schritte aus:
  - iOS: Stellen Sie sicher, dass Sie nicht die Richtlinie “Gateway für Hintergrundnetzwerkdienst” konfigurieren. Bei Konfiguration dieser Richtlinie erhalten Benutzer häufige Authentifizierungsaufforderungen.
  - Android: Stellen Sie sicher, dass Sie die **LDAP-Server-URL** in die Liste für die Richtlinie “Gateway für Hintergrundnetzwerkdienst” aufnehmen.

SSO für Secure Mail

April 26, 2019

Sie können Endpoint Management so konfigurieren, dass Benutzer automatisch bei Secure Mail registriert werden, wenn sie sich bei Secure Hub registrieren. Die Benutzer müssen für die Registrierung bei Secure Mail keine weiteren Informationen eingeben und keine zusätzlichen Schritte ausführen. Damit sich Benutzer mit E-Mail-Anmeldeinformationen bei Secure Hub registrieren können, muss Autodiscovery für dieses Feature aktiviert sein. Wenn Autodiscovery nicht aktiviert ist, können Sie das Feature für die folgenden Registrierungsmethoden aktivieren:

- Die Endpoint Management-Serveradresse wird von Secure Hub an Secure Mail weitergegeben.
- Benutzer geben die Endpoint Management-Serveradresse ein, wenn sie sich bei Secure Hub registrieren.

Aktivieren der automatischen Registrierung bei Secure Mail

1. Führen Sie in den Endpoint Management-Clienteigenschaften auf der Seite **Einstellungen** folgende Schritte aus:

   a. Wählen Sie für folgende Werte die Einstellung **true**:

   - ENABLE_PASSCODE_AUTH
   - ENABLE_PASSWORD_CACHING
   - ENABLE_CREDENTIAL_STORE

   b. Fügen Sie diese Konfiguration hinzu:

   - **Anzeigename**: SEND_LDAP_ATTRIBUTES

- **Wert**: userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName= ${ user.displayName} ,mail= ${ user.mail}

2. Fügen Sie auf der Seite **Einstellungen** diese Konfiguration zur Servereigenschaft hinzu:

   MAM_MACRO_SUPPORT - auf **true** festgelegt

3. Konfigurieren Sie diese Secure Mail-Eigenschaften:
   - Legen Sie “Anfänglicher Authentifizierungsmechanismus” auf **Benutzer-E-Mail-Adresse** fest.
   - Legen Sie “Anfangsanmeldeinformationen für die Authentifizierung” auf **userPrincipalName** fest.
4. Konfigurieren Sie den Dienst für die E-Mail-basierte AutoErmittlung für das Exchange Server-Postfach des Benutzers. Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren Microsoft Exchange-Administrator. In dem Artikel wird davon ausgegangen, dass Sie den AutoErmittlungsdienst unter Abfrage eines SRV-Eintrags beim DNS konfigurieren.

Konfigurieren der App-Richtlinie für Secure Mail

Laden Sie die Secure Mail-App in Endpoint Management hoch. Laden Sie die MDX-Datei der richtigen Version von Secure Mail hoch. Konfigurieren Sie anschließend die folgenden App-Einstellungen für Secure Mail:

1. Klicken Sie für “Anfänglicher Authentifizierungsmechanismus” auf **Benutzer-E-Mail-Adresse**.
2. Klicken Sie für **Anfangsanmeldeinformationen für die Authentifizierung** auf **userPrincipalName** oder **sAMAccountName**. Die Auswahl hängt von dem für den Exchange-E-Mail-Server des Benutzers konfigurierten Authentifizierungstyp ab.
3. Lassen Sie die Felder für Secure Mail-Exchange Server und Secure Mail-Benutzerdomäne leer.
4. Konfigurieren Sie andere Richtlinien für die Secure Mail-App nach Bedarf und nehmen Sie die erforderlichen Bereitstellungsgruppenzuweisungen vor.

End-to-End-SSO bei Secure Mail mit automatischer Bereitstellung

Es müssen die nachfolgend aufgeführten Voraussetzungen erfüllt sein.

1. Installieren Sie Secure Hub im App Store von Apple (iOS) oder in Google Play (Android).
2. Öffnen Sie Secure Hub und geben Sie eine E-Mail-Adresse und ein Kennwort für die Registrierung bei Endpoint Management ein.
3. Installieren Sie Secure Mail im App Store von Apple (iOS) oder in Google Play (Android).

4. Öffnen Sie Secure Mail und tippen Sie auf **OK**. Durch diesen Schritt kann Secure Hub Secure Mail verwalten. Beim Öffnen wird Secure Mail automatisch konfiguriert.

Der der Postfachdatenbank des Benutzers zugewiesene Exchange Server wird von dem von Ihnen konfigurierten AutoErmittlungsdienst abgerufen. Bei der Abfrage des DNS-SRV-Datensatzes wird die E-Mail-Adresse des Benutzers, die von Secure Hub abgerufen wurde, verwendet.

Alle zur Kontokonfiguration erforderlichen Details (E-Mail-Adresse, userPrincipalName/sAMAccountName und Kennwort) werden von Secure Hub abgerufen.

Wenn das Konto konfiguriert ist, können Benutzer unter **Secure Mail** > **Einstellungen** > **Konto** Details zum Gerät anzeigen.

Problembehandlung

Treten bei der SSO-Konfiguration Probleme auf, können Folgendes versuchen:

1. Prüfen Sie, ob XenMobile Server in Version 10.5 oder höher vorliegt.
2. Prüfen Sie, ob Endpoint Management für den AutoErmittlungsdienst und die Benutzerregistrierung für die Verwendung mit einer E-Mail-Adresse konfiguriert ist.
3. Prüfen Sie, ob die Exchange Server-Domäne mit AutoErmittlung konfiguriert ist. Prüfen Sie, ob die Abfrage des SRV-Eintrags die erwarteten E-Mail-Serverdetails für ActiveSync-E-Mail-Clients zurückgibt.
4. Bei einem Problem mit diesen Funktionen sammeln Sie die folgenden Informationen und wenden Sie sich an den technischen Support von Citrix:
    - Laden Sie Endpoint Management-Diagnoseprotokolle herunter.
    - Secure Mail-Diagnoseprotokolle mit der höchsten Protokollebene
    - IIS-Protokolle aus dem Verzeichnis C:\inetpub\logs\LogFiles\W3SVC1 auf dem Exchange Server, der den AutoErmittlungsdienst hostet Weitere Informationen zum AutoErmittlungsdienst von Microsoft finden Sie unter AutoErmittlungsdienst in Exchange Server.

Sicherheitsüberlegungen

February 19, 2019

In diesem Artikel werden die Sicherheitsaspekte von Secure Mail erläutert und bestimmte Einstellungen, die Sie aktivieren können, um die Datensicherheit zu verbessern.

Unterstützung von E-Mails mit Microsoft IRM- und AIP-Schutz

Secure Mail für Android und iOS unterstützen Nachrichten, die durch Microsoft IRM (Information Rights Management) und AIP (Azure Information Protection) geschützt sind. Hierfür muss die IRM-Richtlinie unter Citrix Endpoint Management konfiguriert sein.

Mit diesem Feature können Organisationen Nachrichteninhalte über die Verwaltung von Informationsrechten schützen. Benutzer von Mobilgeräten können mit dem Feature ebenfalls geschützte Inhalte erstellen und verwenden. Standardmäßig ist die Unterstützung für IRM auf **Off** festgelegt. Um die IRM-Unterstützung zu aktivieren, **aktivieren** Sie die Informationen Rights Management-Richtlinie.

Aktivieren der Verwaltung von Informationsrechten (IRM) in Secure Mail

1. Melden Sie sich bei Endpoint Management an, navigieren Sie zu **Konfigurieren** > **Apps** und klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf der Seite **Add App** auf **MDX**.
3. Geben Sie im Fenster **App-Informationen** die App-Details ein und klicken Sie auf **Weiter**.
4. Wählen Sie die MDX-Datei für Ihr Gerätebetriebssystem aus und laden Sie sie hoch.
5. Aktivieren Sie unter **App-Einstellungen** die Option “Verwaltung von Informationsrechten (IRM)”.

> Hinweis:
>
> Aktivieren Sie IRM für iOS und Android.

Empfang einer geschützten E-Mail

Wenn Benutzer eine E-Mail mit geschütztem Inhalt erhalten, wird der folgende Bildschirm angezeigt:

Tippen Sie auf **Details**, um die für den Benutzer festgelegten Rechte anzuzeigen.

Verfassen einer geschützten E-Mail

Beim Verfassen einer E-Mail können Benutzer Einschränkungsprofile festlegen, um den E-Mail-Schutz zu aktivieren.

Festlegen von Einschränkungen für Ihre E-Mail:

1. Melden Sie sich in Secure Mail an und tippen Sie auf das Symbol **Verfassen**.
2. Tippen Sie im Bildschirm zum Verfassen einer E-Mail auf das Symbol zur **E-Mail-Beschränkung**.

3. Tippen Sie im Bildschirm **Einschränkungsprofile** auf die Einschränkungen, die für die E-Mail gelten sollen, und klicken Sie auf “Zurück”.

   Die angewendeten Einschränkungen werden unterhalb der Betreffzeile angezeigt.

In manchen Organisationen ist eine strikte Einhaltung der IRM-Richtlinie erforderlich. Benutzer mit Zugriff auf Secure Mail könnten eine Umgehung der IRM-Richtlinie durch Manipulation von Secure Mail, des Betriebssystems oder sogar der Hardwareplattform versuchen.

Endpoint Management erkennt zwar bestimmte Angriffe, es empfiehlt sich jedoch, die Sicherheit durch folgende Vorsichtsmaßnahmen zu erhöhen:

- Lesen Sie die Sicherheitsinformationen des Geräteherstellers.
- Konfigurieren Sie die Geräte entsprechend, entweder über Endpoint Management-Funktionen oder alternative Funktionen.
- Informieren Sie die Benutzer über die richtige Verwendung von IRM-Features, einschließlich Secure Mail.
- Implementieren Sie zusätzliche Sicherheitssoftware von Drittanbietern zum Schutz vor entsprechenden Angriffen.

E-Mail-Sicherheitsklassifizierungen

Secure Mail für iOS und Android unterstützt E-Mail-Klassifizierungsmarkierungen, mit denen Benutzer beim Senden von E-Mails Security (SEC) und Dissemination Limiting Markers (DLM) festlegen. SEC-Markierungen umfassen Protected, Confidential und Secret. DLM umfassen Sensitive, Legal oder Personal. Beim Erstellen einer E-Mail kann ein Secure Mail-Benutzer eine Markierung auswählen, die die Klassifizierungsebene der E-Mail angibt (siehe Abbildungen unten).

Empfänger können die Klassifizierungsmarkierung im Betreff der E-Mail sehen. Zum Beispiel:

- Betreff: Planung [SEC = PROTECTED, DLM = Sensitive]
- Betreff: Planung [DLM = Sensitive]
- Betreff: Planung [SEC = UNCLASSIFIED]

E-Mail-Kopfzeilen enthalten Klassifizierungsmarkierungen als eine Internet Message Header Extension, die im folgenden Beispiel fett dargestellt ist:

Datum: Fr, 1. Mai 2015 12:34:50 +530

Thema: Planung [SEC = PROTECTED, DLM = Sensitive]

Priorität: normal

X-Priorität: normal **X-Protective-Marking: VER-2012.3, NS=gov.au,SEC = PROTECTED, DLM = Sensitive,ORIGIN=operations@example.com**

Von: **operations@example.com**

An: Team <mylist@example.com>

MIME-Version: 1.0 Inhaltstyp: multipart/alternative;boundary="_com.example.email_6428E5E4-9DB3-4133-9F48-155913E39A980"

Secure Mail zeigt Klassifizierungsmarkierungen nur an. Die App führt basierend auf den Markierungen keine Aktionen aus.

Wenn ein Benutzer eine E-Mail mit Klassifizierungsmarkierungen beantwortet oder weiterleitet, enthält die E-Mail standardmäßig die SEC- und DLM-Werte der ursprünglichen E-Mail. Der Benutzer kann eine andere Markierung wählen. Secure Mail überprüft Änderungen im Vergleich zur ursprünglichen E-Mail nicht.

Sie konfigurieren E-Mail-Klassifizierungen mit den folgenden MDX-Richtlinien.

- **E-Mail-Klassifizierung:** Bei der Einstellung **Ein** unterstützt Secure Mail E-Mail-Klassifizierungsmarkierungen für SEC und DLM. Klassifizierungsmarkierungen werden in der E-Mail-Kopfzeile als "X-Protective-Marking"-Werte angezeigt. Konfigurieren Sie auch die zugehörigen E-Mail-Klassifizierungsrichtlinien. Der Standardwert ist **Aus**.
- **E-Mail-Klassifizierungsnamespace:** Gibt den Klassifizierungsnamespace an, den der Klassifizierungsstandard in der E-Mail-Kopfzeile erfordert. Beispielsweise wird der Namespace "gov.au" in der Kopfzeile als "NS=gov.au" angezeigt. Der Standardwert ist leer.
- **E-Mail-Klassifizierungsversion:** Gibt die Klassifizierungsversion an, die der Klassifizierungsstandard in der E-Mail-Kopfzeile erfordert. Beispielsweise wird die Version "2012.3" in den Kopfzeile als "VER=2012.3" angezeigt. Der Standardwert ist leer.
- **E-Mail-Standardklassifizierung:** Gibt die Schutzmarkierung an, die Secure Mail auf eine E-Mail anwendet, wenn ein Benutzer keine Markierung wählt. Dieser Wert muss in der Liste für die Richtlinie "E-Mail-Klassifizierungsmarkierungen" sein. Der Standardwert ist **UNOFFICIAL**.
- **E-Mail-Klassifizierungsmarkierungen:** Gibt die Klassifizierungsmarkierungen an, die für Endbenutzer verfügbar sind. Wenn die Liste leer ist, verwendet Secure Mail keine Liste mit Schutzmarkierungen. Die Markierungsliste enthält durch Semikola getrennte Wertpaare. Jedes Paar enthält den in Secure Mail angezeigten Listenwert und den Markierungswert, wobei es sich um den Text handelt, der in Secure Mail an den E-Mail-Betreff und die Kopfzeile angehängt wird. Beispiel: Im Markierungspaar "UNOFFICIAL, SEC=UNOFFICIAL" ist der Listenwert "UNOFFICIAL" und der Markierungswert "SEC=UNOFFICIAL".

Der Standardwert ist eine Liste mit Klassifizierungsmarkierungen, die Sie ändern können. Die folgenden Markierungen werden mit Secure Mail bereitgestellt.

- UNOFFICIAL,SEC=UNOFFICIAL
- UNCLASSIFIED,SEC=UNCLASSIFIED
- For Official Use Only,DLM=For-Official-Use-Only
- Sensitive,DLM=Sensitive

- Sensitive:Legal,DLM=Sensitive:Legal
- Sensitive:Personal,DLM=Sensitive:Personal
- PROTECTED,SEC=PROTECTED
- PROTECTED+Sensitive,SEC=PROTECTED
- PROTECTED+Sensitive:Legal,SEC=PROTECTED DLM=Sensitive:Legal
- PROTECTED+Sensitive:Personal,SEC=PROTECTED DLM=Sensitive:Personal
- PROTECTED+Sensitive:Cabinet,SEC=PROTECTED,DLM=Sensitive:Cabinet
- CONFIDENTIAL,SEC=CONFIDENTIAL
- CONFIDENTIAL+Sensitive,SEC=CONFIDENTIAL,DLM=Sensitive
- CONFIDENTIAL+Sensitive:Legal,SEC=CONFIDENTIAL DLM=Sensitive:Legal
- CONFIDENTIAL+Sensitive:Personal,SEC=CONFIDENTIAL,DLM=Sensitive:Personal
- CONFIDENTIAL+Sensitive:Cabinet,SEC=CONFIDENTIAL DLM=Sensitive:Cabinet
- SECRET,SEC=SECRET
- SECRET+Sensitive,SEC=SECRET,DLM=Sensitive
- SECRET+Sensitive:Legal,SEC=SECRET,DLM=Sensitive:Legal
- SECRET+Sensitive:Personal,SEC=SECRET,DLM=Sensitive:Personal
- SECRET+Sensitive:Cabinet,SEC=SECRET,DLM=Sensitive:Cabinet
- TOP-SECRET,SEC=TOP-SECRET
- TOP-SECRET+Sensitive,SEC=TOP-SECRET,DLM=Sensitive
- TOP-SECRET+Sensitive:Legal,SEC=TOP-SECRET DLM=Sensitive:Legal
- TOP-SECRET+Sensitive:Personal,SEC=TOP-SECRET DLM=Sensitive:Personal
- TOP-SECRET+Sensitive:Cabinet,SEC=TOP-SECRET DLM=Sensitive:Cabinet

Schutz von iOS-Daten

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

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

Zum Ändern der Richtlinie “iOS-Datenschutz aktivieren” gehen Sie folgendermaßen vor

1. Laden Sie mit der Endpoint Management-Konsole die MDX-Dateien von Secure Web und Secure Mail in Endpoint Management: Bei neuen Apps navigieren Sie zu **Konfigurieren > Apps**

> Hinzufügen und klicken Sie auf **MDX**. Bei Upgrades gehen Sie wie unter Durchführen eines Upgrades von MDX- oder Unternehmensapps beschrieben vor.

2. Navigieren Sie für Secure Mail zu den **App**-Einstellungen und legen Sie die Richtlinie **iOS-Datenschutz aktivieren** auf **Ein** fest. Auf Geräte mit älteren Betriebssystemversionen hat die Aktivierung dieser Richtlinie keine Auswirkungen.
3. Navigieren Sie für Secure Web zu den **App**-Einstellungen und legen Sie die Richtlinie **iOS-Datenschutz aktivieren** auf **Ein** fest. Auf Geräte mit älteren Betriebssystemversionen hat die Aktivierung dieser Richtlinie keine Auswirkungen.
4. Konfigurieren Sie die App-Richtlinien wie gewohnt und speichern Sie die Einstellungen, um die App im Endpoint Management App Store bereitzustellen.

Datenschutz gemäß Australian Signals Directorate

Secure Mail unterstützt den Datenschutz gemäß den Vorgaben des Australian Signals Directorate (ASD) für Unternehmen, die die entsprechenden ASD-Sicherheitsanforderungen erfüllen müssen. Standardmäßig ist die Richtlinie "iOS-Datenschutz aktivieren" auf **Aus** festgelegt und Secure Mail bietet Datenschutz der Klasse C oder den im Provisioningprofil festgelegten Datenschutz.

Wenn die Richtlinie auf **Ein** festgelegt ist, wird die Schutzebene von Secure Mail beim Erstellen und Öffnen von Dateien in der App-Sandbox festgelegt. Secure Mail legt Datenschutz der Klasse A für folgende Elemente fest:

- Elemente im Postausgang
- Fotos aus der Kamera bzw. Kamerarolle
- Aus anderen Apps eingefügte Bilder
- Heruntergeladene Dateianlagen

Secure Mail legt Datenschutz der Klasse B für folgende Elemente fest:

- Gespeicherte E-Mail
- Kalenderelemente
- Kontakte
- ActiveSync-Richtliniendateien

Schutz der Klasse B gestattet einem gesperrten Gerät die Synchronisierung und den Abschluss von Downloads, sofern das Gerät nach dem Start des Downloads gesperrt wurde.

Bei aktiviertem Datenschutz werden Postausgangselemente in der Warteschlange nicht gesendet, wenn ein Gerät gesperrt wird, da die Dateien nicht geöffnet werden können. Wird Secure Mail auf einem Gerät beendet und startet dann bei gesperrtem Gerät neu, erfolgt keine Synchronisierung, bis das Gerät entsperrt wird und Secure Mail startet.

Citrix empfiehlt, bei Aktivierung dieser Richtlinie die Protokollierung nur dann zu aktivieren, wenn sie unbedingt erforderlich ist, um das Erstellen von gemäß Klasse C geschützten Protokolldateien zu vermeiden.

Android-Features

May 23, 2019

Dieser Artikel beschreibt die Android-Features, die von Secure Mail unterstützt werden.

Verwalten von Feeds

In Secure Mail für Android können Sie jetzt Ihre **Feeds**-Karte entsprechend Ihren Anforderungen organisieren.

Die Verbesserungen an Feeds umfassen die folgenden Optionen:

- Hinzufügen von bis zu drei E-Mail-Ordnern.
- Hinzufügen von Karten für Kollegen und direkte Mitarbeiter bzw. von Ordnern wie “VIP” und “Gekennzeichnet”.
- Suche nach Karten oder Ordnern.
- Neuanordnen vorhandener Karten.
- Entfernen einer vorhandenen Karte.

Tippen Sie in der **Feeds**-Ansicht auf die Schaltfläche **Feeds verwalten**, um Ihre Karten zu verwalten.

Alternativ können Sie in den Einstellungen unter **E-Mail** auf **Feeds verwalten** tippen, um Ihre Karten zu verwalten.

Sie können neue Karten hinzufügen und Ihre Karten neu anordnen oder löschen.

Hinzufügen einer Karte

1. Tippen Sie auf die Registerkarte **Alle Karten** oder **Alle Ordner**.
2. Tippen Sie auf das **Pluszeichen** (+) rechts oben im Bildschirm, um die gewünschten Karten auszuwählen.
3. Tippen Sie auf **Fertig**.

Die ausgewählten Karten werden hinzugefügt und in Ihren Feeds angezeigt.

Neuanordnen Ihrer Karten

1. Tippen Sie auf die Schaltfläche **Feeds verwalten**.
2. Durch Tippen und Halten wählen Sie eine vorhandene Karte aus.
3. Ziehen Sie die Karte an die gewünschte Position.

Löschen einer Karte

1. Tippen Sie auf die Schaltfläche **Feeds verwalten**.
2. Tippen Sie auf das Minuszeichen (-) neben den Karten.
3. Tippen Sie auf **Fertig**.

Die Karten werden aus den Feeds entfernt.

Anzeige von Anlagen

Secure Mail für Android ermöglicht die einfache Anzeige von E-Mail- und Kalenderanlagen. Die Anlage wird entweder direkt in der App geöffnet oder es wird eine Liste der unterstützten Apps angezeigt. Sie können dann die erforderliche App zur Anzeige der Anlage auswählen.

Secure Mail unterstützt TXT-, Word-, Audio-, Video-, HTML- und ZIP-Dateien sowie Bilder, EML-Dateien und VCF-Dateien für Kontakte.

Voraussetzungen

Folgende MDX-Richtlinien sind vom Administrator in der Citrix Endpoint Management-Konsole zu konfigurieren:

- Für die Richtlinie “Dokumentaustausch (Öffnen in)” ist die Einstellung **Uneingeschränkt** festzulegen.
- Für die Richtlinie “Offlinedokumente zulassen” ist die Einstellung **Unbegrenzt** festzulegen.

Weitere Informationen zu diesen Richtlinien finden Sie in den MDX-Richtlinien unter Interaktion von Apps.

Aktionen beim Anzeigen von Anlagen

Sie können beim Anzeigen der Anlagen die folgenden Aktionen ausführen:

- Wählen Sie eine vorhandene Nachricht in Ihren Postfächern, an die Sie die Datei anfügen möchten.
- Erstellen Sie eine Nachricht, an die Sie die Datei anfügen möchten.

- Speichern Sie eine Anlage für den Offlinezugriff.
- Löschen Sie eine Anlage aus den Offlinedateien.
- Öffnen Sie eine Anlage mit einer anderen Anwendung, wenn Sie dazu aufgefordert werden.
- Zeigen Sie die Quell-E-Mail oder das Kalenderereignis der Anlage an.

Sie können während folgender Aktionen eine Vorschau der Anlage anzeigen:

- Anzeigen einer Nachricht
- Verfassen einer neuen Nachricht
- Weiterleiten einer Nachricht

Sie können eine Vorschau für Anlagen aus folgenden Quellen anzeigen:

- Ordner**Anlagen**
- Kalenderereignisse

Anfügen von Dateien an eine vorhandene oder neue E-Mail

Sie können Dateien an eine vorhandene E-Mail anfügen oder eine E-Mail erstellen, um Dateien anzufügen.

1. Tippen Sie auf den Ordner **Anlagen**, wählen Sie mehrere Anlagen durch langen Fingerdruck aus oder tippen Sie auf eine einzelne Anlage, um sie auszuwählen.
2. Tippen Sie im Bildschirm auf das Symbol **Anfügen**. Das Postfach wird angezeigt.
3. Sie können eine der folgenden Aktionen ausführen:
    - Wählen Sie eine vorhandene E-Mail, um die Datei daran anzufügen.
    - Tippen Sie auf **Neue Nachricht**, um die Datei an eine neue E-Mail anzufügen.

Speichern Sie die Datei für den Offlinezugriff

1. Öffnen Sie die Anlage.
2. Tippen Sie rechts oben auf der Seite auf das Symbol **Mehr** und dann auf **Für Offlinezugriff speichern**.

Löschen Sie die Anlage aus den Offlinedateien

1. Öffnen Sie die Anlage.
2. Tippen Sie rechts oben auf der Seite auf das Symbol **Mehr** und dann auf **Aus Offlinedateien entfernen**.

Öffnen der Anlage mit anderen Apps

1. Öffnen Sie die Anlage.
2. Tippen Sie rechts oben auf der Seite auf das Symbol **Mehr** und dann auf **Öffnen mit**.
3. Tippen Sie unter den angezeigten Optionen auf die App, mit der Sie die Anlage öffnen möchten.
4. Sie können auch nach links wischen, um eine Liste aller zum Anzeigen oder Öffnen einer Anlage verfügbaren Aktionen anzuzeigen.

Zeigen Sie die Quell-E-Mail oder das Kalenderereignis der Anlage an

1. Tippen Sie rechts unten auf dem Bildschirm auf das Symbol **Anlagen**.
2. Tippen Sie auf die Anlage und dann oben rechts auf dem Bildschirm auf das Symbol **Mehr**.
3. Tippen Sie auf **Ursprüngliche E-Mail anzeigen** oder **Ursprüngliches Ereignis anzeigen**, um die Quelle einer E-Mail oder eines Kalenderereignisses anzuzeigen.

Drucken von E-Mails und Kalenderereignissen

In Secure Mail für Android können Sie E-Mails und Kalenderereignisse von Ihrem Android-Gerät aus drucken. Zum Drucken wird das Android Print-Framework verwendet.

Voraussetzungen

- Vergewissern Sie sich, dass ein Administrator die Richtlinie **Drucken blockieren** in der Citrix Endpoint Management-Konsole auf **Aus** festgelegt hat. Weitere Informationen zu dieser Richtlinie für Android finden Sie unter Richtlinie “Drucken blockieren”.
- Wenn eine E-Mail mit IRM geschützt ist, stellen Sie sicher, dass Sie in der E-Mail die Option **Benutzern das Drucken gestatten** aktivieren.

Wenn diese Richtlinien nicht richtig festgelegt sind, können Sie keine E-Mail und Kalenderereignisse drucken.

> Hinweis:
>
> Für diese Druckfunktion gelten die folgenden bekannten Einschränkungen:
>
> - Inlinebilder werden nur dann gedruckt, wenn sie durch Antippen von **Bilder anzeigen** heruntergeladen wurden. Wenn Sie nicht auf **Bilder anzeigen** tippen, werden nur die Bildplatzhalter gedruckt.
> - In Secure Mail werden große E-Mails abgeschnitten. Tippen Sie vor dem Drucken auf **Vollständige Nachricht herunterladen**, damit die E-Mail vollständig gedruckt wird. Wenn die

> vollständige Nachricht nicht heruntergeladen wird, wird sie nur teilweise gedruckt.
> - Beim Drucken von E-Mail oder Ereignissen werden keine enthaltenen Metadaten hinzugefügt.

Drucken von E-Mail

1. Öffnen Sie die E-Mail, die Sie drucken möchten.
2. Tippen Sie auf oben links auf dem Bildschirm auf das Symbol “Mehr”. Die folgenden Optionen werden angezeigt:
    - Verschieben
    - Drucken

> Hinweis:
>
> Auf Tablets können Sie das Drucksymbol oben links auf dem Bildschirm verwenden, um eine E-Mail zu drucken.

1. Tippen Sie auf **Drucken**. Eine Vorschau der E-Mail wird angezeigt.
2. Tippen Sie auf die Liste, um folgende Optionen anzuzeigen:
    - Als PDF speichern
    - Alle Drucker
3. Tippen Sie auf **Als PDF speichern**, um die E-Mail im PDF-Format zu speichern.
4. Tippen Sie auf **Alle Drucker**. Installieren Sie den Drucker gemäß Ihren Anforderungen.
5. Tippen Sie nach der Installation des Druckers auf **Drucker auswählen**, um einen Drucker auszuwählen. Der Bildschirm **Drucker** wird angezeigt.

    > Hinweis:
    >
    > Die Druckoptionen variieren je nach ausgewähltem Drucker. Die folgende Abbildung der Optionen eines Canon E480 hat lediglich Beispielcharakter.

6. Wählen Sie den Drucker, auf dem Sie drucken möchten. Verwenden Sie die folgenden Druckoptionen:
    - Geben Sie die Anzahl der zu druckenden Exemplare ein.
    - Wählen Sie das Papierformat aus der Liste aus.
    - Wählen Sie die Farbe aus der Liste aus.
    - Wählen Sie die Seitenausrichtung.
    - Wählen Sie eine Seite aus oder einen Seitenbereich unter Eingabe der Seiten des Bereichs.
7. Tippen Sie nach dem Festlegen der Druckoptionen auf das Drucksymbol.

Drucken von Inlinebildern

- Tippen Sie in der E-Mail auf **Bilder anzeigen** und folgen Sie den Anweisungen im Abschnitt Drucken von E-Mail oben.

Drucken von Kalenderereignissen

1. Navigieren Sie zum Kalender und tippen Sie auf ein Ereignis.
2. Tippen Sie auf das Symbol “Drucken” und folgen Sie den Anweisungen im Abschnitt Drucken von E-Mail oben.

Melden von Phishing-E-Mail mit ActiveSync-Kopfzeile

Wenn ein Benutzer in Secure Mail für Android eine Phishing-E-Mail meldet, wird zu der E-Mail eine EML-Datei als Anlange erstellt. Der Empfänger der E-Mail kann die ActiveSync-Kopfzeile der gemeldeten E-Mail anzeigen.

Um dieses Feature zu aktivieren, muss ein Administrator die Richtlinie “Phishing-E-Mail-Adressen melden” konfigurieren und “Phishingberichtmethode” in der Citrix Endpoint Management-Konsole auf **Als Anlage melden** festlegen. Einzelheiten finden Sie unter Melden von Phishing-E-Mail (als Anlage).

Unterordnerbenachrichtigungen

In Secure Mail für Android können Sie E-Mail-Benachrichtigungen aus Unterordnern Ihres E-Mail-Kontos erhalten.

> Hinweis:
>
> - Stellen Sie sicher, dass FCM-basierte Pushbenachrichtigungen in der Endpoint Management-Konsole aktiviert sind, um Benachrichtigungen für Unterordner zu erhalten. Schritte zur Konfiguration von FCM-basierten Pushbenachrichtigungen finden Sie unter Pushbenachrichtigungen für Secure Mail.
> - Die Benachrichtigungsfunktion für Unterordner ist für Lotus Notes Server nicht verfügbar.

Aktivieren von Unterordnerbenachrichtigungen

1. Gehen Sie zu **Einstellungen** und tippen Sie unter **Allgemein** auf **Benachrichtigungen**.
2. Tippen im Bildschirm **Benachrichtigungen** auf **E-Mail-Ordner**. Eine Liste der Unterordner des Posteingangs wird angezeigt.

3. Wählen Sie die Unterordner aus, für die Sie Benachrichtigungen erhalten möchten. Der Posteingang ist standardmäßig ausgewählt.

   > **Hinweis:**
   >
   > Wenn Sie Benachrichtigungen für Unterordner aktivieren, wird die automatische Synchronisierung aktiviert.

Zum Deaktivieren von Benachrichtigungen für spezifische Unterordner deaktivieren Sie deren Kontrollkästchen.

Benachrichtigungskanäle

Auf Geräten mit Android O oder höher können Sie über die Einstellungen des Benachrichtigungskanals verwalten, wie Ihre E-Mail- und Kalenderbenachrichtigungen behandelt werden. Mit diesem Feature können Sie Ihre Benachrichtigungen anpassen und verwalten.

Um Benachrichtigungen für E-Mail- oder Kalendererinnerungen zu konfigurieren, öffnen Sie Secure Mail und navigieren Sie zu **Einstellungen > Benachrichtigungen** und wählen Sie die gewünschte Benachrichtigungsoption aus.

Sie können dann entweder zu **E-Mail Benachrichtigungen verwalten** oder **Kalenderbenachrichtigungen verwalten** navigieren, um Ihre E-Mail- bzw. Kalenderbenachrichtigungen zu verwalten.

Alternativ können Sie auch lange auf das Symbol der Secure Mail-App auf Ihrem Gerät drücken, **App-Info** auswählen und dann auf **Benachrichtigungen** tippen.

Wenn Ihre Vibrationseinstellung zuvor auf **Nur bei 'Lautlos'** eingestellt war, wechselt sie mit diesem Feature zur Standardeinstellung (**Aus**).

> Hinweis:
>
> Die Benachrichtigungen auf dem Sperrbildschirm sind verfügbar, je nachdem, wie Ihr Administrator die MDX-Richtlinie Benachrichtigungen bei gesperrtem Bildschirm steuern konfiguriert hat.

Anhängen von Dateien in Android

In Secure Mail 10.3.5 und höher können Benutzer keine Bilder direkt aus der Gallery-App anhängen, wenn die Richtlinie "Eingehender Dokumentaustausch (Öffnen in)" auf **Eingeschränkt** festgelegt ist. Wenn Sie die Einstellung **Eingeschränkt** für diese Richtlinie beibehalten und Benutzern ermöglichen möchten, Fotos aus der Gallery-App anzuhängen, führen Sie die nachfolgenden Schritte in der Endpoint Management-Konsole aus.

1. Legen Sie **Gallery blockieren** auf **Aus** fest.
2. Rufen Sie die Gallery-Paket-ID für Geräte ab. Beispiele:
   - **LG Nexus 5:**
     com.google.android.gallery3d, com.google.android.apps.photos
   - **Samsung Galaxy Note 3:**
     com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.p
   - **Sony Expire:**
     com.sonyericsson.album, com.google.android.apps.photos
   - **HTC:**
     com.google.android.apps.photos, com.htc.album
   - **Huawei:**
     com.android.gallery3d, com.google.android.apps.photos
3. Machen Sie die ausgeblendete Richtlinie InboundDocumentExchangeWhitelist sichtbar:
   - Laden Sie die WorxMail-APK-Datei herunter und umschließen Sie die Datei mit dem MDX Toolkit.
   - Suchen Sie die MDX-Datei auf Ihrem Computer und ändern Sie die Dateierweiterung in ".zip".
   - Öffnen Sie die ZIP-Datei, und suchen Sie die Datei policy_metadata.xml.
   - Suchen Sie "InboundDocumentExchangeWhitelist" und ändern Sie den Wert von `PolicyHidden>**true**</PolicyHidden>` in `<PolicyHidden>**false**</PolicyHidden>`.
   - Speichern Sie die Datei policy_metadata.xml.
   - Wählen Sie alle Dateien in dem Ordner aus und erstellen Sie daraus eine ZIP-Datei.

     > **Hinweis:**
     >
     > Komprimieren Sie nicht den äußeren Ordner. Wählen Sie alle Dateien im Ordner aus und komprimieren Sie die ausgewählten Dateien.

   - Klicken Sie auf die komprimierte Datei.
   - Wählen Sie **Informationen abrufen** und ändern Sie die Dateierweiterung zurück in ".mdx".
4. Laden Sie die geänderte MDX-Datei in die Endpoint Management-Konsole hoch und fügen Sie die Liste der Gallery-Paket-IDs der nun sichtbaren Richtlinie Positivliste für Austausch eingehender Dokumente hinzu.

   Stellen Sie sicher, dass die Paket-IDs durch Kommas getrennt sind:

   com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photo
5. Speichern Sie die Datei und stellen Sie Secure Mail bereit.

Android-Benutzer können nun Bilder aus der Gallery-App anhängen.

Unterstützte Dateiformate

Ein X bedeutet, das Dateiformat kann in Secure Mail angehängt, angezeigt und geöffnet werden.

Format	iOS	Android
Video: H.263 AMR NB codec_Mp4		X
Video: H.263 AMR NB codec_3gp		X
Video: H.264 AAC codec_3gp	X	X
Video: H.264 AAC codec_mp4	X	X
Video: H.264 Acclc codec_mp4	X	X
GTM recorded_wmv		X
AVI		X
WAV	X	X
MP4	X	X
3GP	X	X
Flac		X
AAC	X	X
M4A	X	X
3GP (AMR-NB)	X	X
MP3	X	X
WAV	X	X
OGG		X
ICO	X	X
JPEG	X	X
PNG	X	X
TIF (einseitig)	X	
BMP	X	X

Format	iOS	Android
GIF	X	X
WebP		X
.dot	X	X
PDF	X	
PPT	X	X
PPTX	X	X
DOC	X	X
DOCX	X	X
XLS	X	X
XLSM	X	X
XLSX	X	X
TXT	X	X
POT	X	X
HTM	X	X
HTML	X	X
ZIP	X	X
EML	X	X

Mehrere Exchange-Konten unter Android

Über **Einstellungen** in Secure Mail können Sie nun mehrere Exchange-E-Mail-Konten hinzufügen und zwischen diesen wechseln. Mit diesem Feature können Sie alle E-Mails, Kontakte und Kalender zentral sehen.

Voraussetzungen

Ein Benutzernamen und ein Kennwort sind erforderlich, um weitere Konten zu konfigurieren. Die Konfiguration für die automatische Registrierung bzw. den Anmeldeinformationenspeicher gelten nur für das erste in der App eingerichtete Konto. Geben Sie den Benutzernamen und das Kennwort für alle zusätzliche Konten ein.

- Wenn das erste Konto, das Sie erstellen, zertifikatbasiert ist, können nicht Sie keine weiteren zertifikatbasierten Konten hinzufügen.
- Damit weitere Konten eine Verbindung mit einer Domäne oder einem Exchange Server in einem externen Netzwerk herstellen können, müssen Sie Split-Tunneling in Citrix ADC auf **ON** festlegen.
- Secure Mail für iOS unterstützt nur Exchange- und Office 365-Mailserver.

Hinzufügen eines Exchange-E-Mail-Kontos für Android

1. Öffnen Sie Secure Mail und tippen Sie auf das Hamburgersymbol und dann auf das Symbol **Einstellungen**.
2. Tippen Sie unter **Konten** auf **Konto hinzufügen**.
3. Geben Sie im Bildschirm **Konto hinzufügen** die Anmeldeinformationen für das neue Konto ein.

   Legen Sie optional Werte für die folgenden Parameter fest:

   - **Mail-Sync-Zeitraum:** Tippen Sie auf einen Wert für den Zeitraum für die E-Mail-Synchronisierung. Der festgelegte Wert repräsentiert den Zeitraum in Tagen, für den E-Mail in Secure Mail synchronisiert werden soll. Der Administrator legt den Standardwert fest.
   - **Zum Standardkonto machen:** Tippen Sie auf diese Option, um das neue Konto als Standardkonto festzulegen. Der Wert ist standardmäßig auf **AUS** festgelegt.
4. Tippen Sie auf **Anmelden**, um das Konto zu erstellen.

   Das neue Konto wird im Bildschirm **Einstellungen** im Menü **Konten** angezeigt.

> **Hinweis:**
>
> Für zusätzliche Konten muss die Authentifizierung über Active Directory verwendet werden. Secure Mail unterstützt keine zertifikatbasierte Authentifizierung, wenn Sie mehrere Konten konfigurieren.

Bearbeiten eines Kontos

Sie können Kennwort und Beschreibung von E-Mail-Konten unter Android bearbeiten.

1. Öffnen Sie Secure Mail und tippen Sie auf das Hamburgersymbol und dann auf das Symbol **Einstellungen**.
2. Tippen Sie unter **Konten** auf das Konto, das Sie bearbeiten möchten.
3. Bearbeiten Sie auf dem Bildschirm **Konto** die Angaben.

4. Tippen Sie auf **Speichern** zum Bestätigen der Aktion oder auf **Abbrechen**, um zum Bildschirm **Einstellungen** zurückzukehren.

Löschen eines Kontos unter Android

1. Öffnen Sie Secure Mail und tippen Sie auf das Hamburgersymbol und dann auf das Symbol **Einstellungen**.
2. Tippen Sie unter **Konten** auf das Konto, das Sie löschen möchten.
3. Tippen Sie im Bildschirm **Konto** unten auf **Konto löschen** oder auf **Abbrechen**, um zum Bildschirm **Einstellungen** zurückzukehren.
4. Tippen Sie auf **LÖSCHEN**, um die Aktion zu bestätigen.

> Hinweis:
>
> Wenn Sie das Standardkonto löschen, wird das nächste Konto zum Standardkonto.

Festlegen des Standardkontos unter Android

In Secure Mail wird das Standardkonto für Folgendes verwendet:

- **Verfassen von E-Mail:** Im Feld **Von:** wird automatisch die E-Mail-Adresse des Standardkontos eingetragen.
- **Erstellen von Kalendererereignissen:** Im Feld **Organisator** wird automatisch die E-Mail-Adresse des Standardkontos eingetragen.

Wenn Sie mehrere E-Mail-Konten hinzufügen, gilt das erste Konto, das Sie erstellen, als Standardkonto. Zum Ändern des Standardkontos navigieren Sie zu **Einstellungen** und tippen dann unter **Allgemein** auf **Standard**.

Tippen Sie im Bildschirm **Standardkonto** auf das Konto, das Sie als Standard festlegen möchten.

Einstellungen für mehrere Exchange-Konten unter Android

Wenn Sie mehrere Exchange-Konten konfiguriert haben, stehen einige Secure Mail-Einstellungen für einzelne Konten zur Verfügung, andere Einstellungen sind global. Die folgenden Einstellungen sind kontospezifisch:

- Standard
- Benachrichtigungen
- Abwesend
- Synchronisierungshäufigkeit - Posteingang
- E-Mail-Synchronisierungszeitraum

- E-Mails synchronisieren
- S/MIME
- Offlinedateien
- Signatur
- Kurzantworten
- Kalender synchronisieren
- Kontakte synchronisieren
- Mit lokalen Kontakten synchronisieren
- Einstellungen exportieren

Diese Einstellungen sind mit dem Symbol > gekennzeichnet. Tippen Sie auf das Symbol >, um die Konten auf dem Gerät anzuzeigen.

Um eine Einstellung auf ein bestimmtes Konto anzuwenden, erweitern Sie diese durch Tippen auf **>** und wählen Sie das E-Mail-Konto.

Bildschirm "Postfächer"

Auf dem Bildschirm **Postfächer** werden alle Konten angezeigt. Es gibt folgende Ansichten:

- **Alle Konten:** enthält E-Mail aller Exchange-Konten, die Sie konfiguriert haben.
- **Einzelkonten:** enthält E-Mail und Ordner eines einzelnen Kontos. Die Konten werden in Form einer Liste angezeigt, die Sie zum Anzeigen der Unterordner erweitern können.

Um Ihre Postfächer anzuzeigen, öffnen Sie Secure Mail und tippen Sie auf das Hamburger-Symbol. Tippen Sie im Bildschirm **Postfächer** auf das Konto, um die Optionen zu erweitern.

In der Ansicht **Alle Konten** werden die E-Mails aus mehreren Konten angezeigt. Bei folgenden Aktionen wird die E-Mail-Adresse des Standardkontos verwendet:

- Neue Nachricht
- Neues Ereignis

Zum Ändern der Absenderadresse bei der Erstellung neuer E-Mails über die Ansicht **Alle Konten** tippen Sie auf die Standardadresse im Feld **Von:** und wählen Sie ein anderes Konto aus der angezeigten Liste aus.

> Hinweis:
>
> Beim Erstellen einer E-Mail über die Konversationsansicht wird das Feld **Von:** automatisch mit der E-Mail-Adresse ausgefüllt, die an der Konversation beteiligt ist.

Einzelkonten

Das Standardkonto wird immer als erstes angezeigt, danach folgen die weiteren Konten in alphabetischer Reihenfolge.

Für die einzelnen Konten werden alle Unterordner, die Sie ggf. erstellt haben, angezeigt.

Die folgenden Aktionen werden nur auf einzelne Konten angewendet:

- Verschieben von Elementen
- Verfassen von E-Mail über die Konversationsansicht
- Speichern von Kontakten

Kontakte

Tippen Sie in der Registerkartenleiste auf das Symbol **Kontakte** und tippen Sie dann in der oberen rechten Ecke des Bildschirms auf das Hamburgersymbol. Der Bildschirm **Kontakte** enthält die folgenden Elemente:

- **Alle Kontakte:** enthält alle Kontakte aus mehreren E-Mail-Konten. Diese Option wird nur angezeigt, wenn mehrere E-Mail-Konten konfiguriert sind.
- **Einzelkonten:** enthält Kontakte der einzelnen Konten, die Sie konfiguriert haben.
- **Kategorien:** enthält Kontaktkategorien, die Sie ggf. erstellt oder aus der vordefinierten Liste ausgewählt haben, um Kontakte zu gruppieren.

Anzeigen des Kontaktordners

> Hinweis:
>
> Kontaktunterordner werden in Secure Mail für Android nicht unterstützt. Wenn Sie für Ihre Kontakte in Microsoft Outlook Ordner oder Unterordner erstellt haben, können Sie sie in Secure Mail nicht anzeigen.

1. Führen Sie im Bildschirm “Kontakte” folgende Schritte aus:
    - Tippen Sie auf “Alle Kontakte”, um alle Kontakte aus mehreren E-Mail-Konten anzuzeigen.
    - Tippen Sie auf ein einzelnes E-Mail-Konto, um die mit diesem verknüpften Kontakte anzuzeigen.
2. Tippen Sie auf Kategorien, um die zugehörigen Kontakte anzuzeigen. Sie können Kontakte nach einer von Ihnen erstellten Kategorie oder nach einer vordefinierten Kategorie gruppieren.

Sie können Kontakte einzelner Konten mit Ihren lokalen Kontakten synchronisieren.

Synchronisieren mit lokalen Kontakten

1. Öffnen Sie Secure Mail.
2. Tippen Sie auf das Symbol “Einstellungen” und navigieren Sie dann zu **Kontakte > Mit lokalen Kontakten synchronisieren** und tippen Sie auf das >-Symbol, um das Menü zu erweitern.
3. Aktivieren Sie im Bildschirm **Lokale Kontakte synchronisieren** das Konto, dessen Kontakte Sie synchronisieren möchten.
4. Tippen Sie auf **OK**.
5. Wenn Sie aufgefordert werden, den Zugriff durch Secure Mail auf Ihre Kontakte zuzulassen, tippen Sie auf **OK**.

Die Kontakte werden dann für das Konto exportiert.
Um diese Aktion rückgängig zu machen, navigieren Sie zu **Einstellungen > Kontakte > Mit lokalen Kontakten synchronisieren** und tippen Sie auf den Schalter neben dem Konto zum Deaktivieren des Features. Tippen Sie auf **OK**, um die Aktion zu bestätigen.

Kalender

Im Kalender werden alle Ereignisse für alle Konten auf dem Gerät angezeigt. Sie können zur einfacheren Unterscheidung Farben für einzelne Konten festlegen.

> Hinweis:
>
> Der persönliche Kalender ist immer Ihrem primären oder Standardkonto zugeordnet, falls aktiviert.

Festlegen von Farben für Kalenderereignisse

1. Tippen Sie in der Fußzeilenleiste auf das Symbol **Kalender** und tippen Sie dann oben links auf das Hamburgersymbol.
   Im Bildschirm **Kalender** werden alle konfigurierten Konten angezeigt.
2. Tippen Sie auf die Standardfarbe rechts neben einem Exchange-Konto.
   Es werden nun die verfügbaren Farben für das Konto angezeigt.
3. Wählen Sie eine Farbe und tippen Sie auf **Speichern**.
4. Um zum vorigen Bildschirm zurückzukehren, tippen Sie auf **Abbrechen**.
   Die ausgewählte Farbe wird nun auf alle Ereignisse des Exchange-Kontos angewendet.

Wenn Sie Kalenderereignisse oder Einladungen erstellen, wird im Feld **Organisator** automatisch die E-Mail-Adresse des Standardkontos eingetragen. Zum Ändern des E-Mail-Kontos tippen Sie auf die E-Mail-Adresse und wählen Sie ein anderes Konto.

Suchen

Sie können über die Ansicht **Postfächer** oder **Alle Kontakte** eine globale Suche durchführen. Durch diese Aktion werden die entsprechenden Ergebnisse nach Durchsuchen aller Konten in der App angezeigt.

Alle Suchanfragen innerhalb eines einzelnen Kontos zeigen nur Ergebnisse an, die sich auf dieses Konto beziehen.

Android Enterprise in Secure Mail

Secure Mail und Secure Web für Android sind kompatibel mit Android Enterprise, früher bekannt als Android for Work.

Voraussetzungen

- Damit Sie dieses Feature nutzen können, muss Android 5.0 oder höher auf Ihrem Gerät ausgeführt werden.
- Bei on-premises Bereitstellungen muss die Endpoint Management-Eigenschaft **afw.accounts** auf **TRUE** festgelegt sein.

Nachdem Sie Android Enterprise in Endpoint Management eingerichtet haben, sind die mobilen Produktivitätsapps auf Ihrem Gerät verfügbar. Das Android Enterprise-Symbol identifiziert die Apps, wie im folgenden Bild markiert.

Mit Android Enterprise kompatible Features

In der folgenden Tabelle sind die Secure Mail-Features aufgeführt, die mit Android Enterprise kompatibel sind.

Feature	Support
Autodiscovery von Exchange Server	X
Secure Ticket Authority (STA)	X
Kontakte exportieren	X
Verwaltung von Informationsrechten (IRM) von Microsoft	X
Benachrichtigungen auf dem Sperrbildschirm	X
E-Mail-Synchronisierung	X

Feature	Support
E-Mail-Klassifizierung	X
S/MIME-Signatur und Verschlüsselung	X
Firebase Cloud Messaging-Dienst (FCM)	X
Moderne Authentifizierung (OAuth)	
Mehrere Exchange-Konten	X
Persönlicher Kalender	
Export von E-Mail-Einstellungen	X
Gemeinsam genutzte Geräte	
Integration von Endpoint Management in Microsoft Intune/EMS	
Office 365	X
LDAP Exchange Server 2010, 2013 und 2016	X
Zertifikatbasierte Authentifizierung	
GoToMeeting	X
Skype for Business	
Persönliche Verteilerliste	X
Citrix Files-Kompatibilität	X
E-Mail-Registrierung mit Single Sign-On	X

In der folgenden Tabelle sind die Secure Web-Features aufgeführt, die mit Android Enterprise kompatibel sind.

Feature	Support
Secure Browse-Modus	X
Vollständiger VPN-Modus	X
Alle App-Features	X
Kompatibilität mit Secure Mail	X

Einschränkungen

- Wenn die Geräteeinschränkungsrichtlinie **Verwendung der Statusleiste zulassen** für Android Enterprise im Arbeitsprofilmodus auf **EIN** festgelegt ist, werden der Fortschritt beim Kalenderexport und Pushbenachrichtigungen in Secure Mail für Android nicht in der Statusleiste angezeigt. Die Benachrichtigungen werden jedoch auf dem gesperrten Bildschirm angezeigt, wenn dies zugelassen ist. Weitere Informationen finden Sie unter Android Enterprise-Einstellungen.

Secure Mail-Integration in Slack (Vorschau)

April 3, 2019

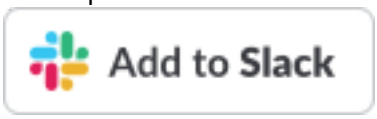
Sie können eine E-Mail-Unterhaltung jetzt auf Geräten mit iOS oder Android in die App Slack übertragen.

Wenn Sie das Feature aktivieren, haben Sie folgende Möglichkeiten:

- Nahtloser Wechsel zwischen E-Mail und Slack-Unterhaltungen
- Erstellen von Slack-Gruppenunterhaltungen mit E-Mail-Empfängern
- Erstellen direkter Nachrichten in Slack für E-Mail-Empfänger

Voraussetzungen

- Administratoren:
  - Vergewissern Sie sich, dass Sie Secure Mail in Ihrem Slack-Workspace installiert haben.

    Klicken Sie unten auf die Schaltfläche **Zu Slack hinzufügen**. 

  - Vergewissern Sie sich, dass die Richtlinie **Slack aktivieren** auf **Ein** eingestellt ist. Richtliniendetails finden Sie unter:
    * Aktivieren der Slack-Richtlinie für iOS
    * Aktivieren der Slack-Richtlinie für Android
- Benutzer: Bevor Sie fortfahren, stellen Sie sicher, dass Sie ein Slack-Konto haben und die Slack-App auf Ihrem Gerät installiert ist.

Aktivieren dieses Features auf Ihrem Gerät

1. Öffnen Sie Secure Mail und tippen Sie auf das Hamburgersymbol.
2. Tippen Sie im Bildschirm **Postfächer** auf das Einstellungssymbol unten rechts.

3. Tippen Sie auf dem Bildschirm **Einstellungen** auf **Slack**. Die Option wird unter **Integrationen** aufgeführt.
4. Geben Sie Ihre Workspace-Slack-URL an und tippen Sie auf **Weiter**.
5. Geben Sie Ihre Anmeldeinformationen ein und tippen Sie auf **Anmelden**.
6. Wenn Sie aufgefordert werden, den Zugriff auf Informationen durch Secure Mail zuzulassen, tippen Sie auf **Autorisieren**.

Sie sind jetzt mit Slack verbunden.

Verwenden des Features

1. Öffnen Sie eine E-Mail-Unterhaltung in Secure Mail und tippen Sie auf die unverankerte Aktionsschaltfläche.
2. Tippen Sie **Chat**.
3. Die Unterhaltung wechselt mit den Empfängern der E-Mail zu Slack.

Berücksichtigen Sie dabei Folgendes:

- Auf Geräten mit Secure Mail für iOS oder Android können Sie eine Slack-Unterhaltung mit maximal acht Empfängern aus einer E-Mail erstellen. Wenn eine E-Mail mehr als acht Empfänger hat, werden standardmäßig die ersten acht Empfänger ausgewählt.

Benachrichtigungen und Synchronisierung

February 20, 2019

Dieser Artikel beschreibt Benachrichtigungs- und E-Mail-Synchronisierungsfunktionen und -konfigurationen für Secure Mail.

Secure Mail für iOS - Hintergrundaktualisierung von Apps

Wenn Secure Mail für iOS so konfiguriert ist, dass Benachrichtigungen über die iOS-Hintergrundaktualisierung (nicht APNs) angezeigt werden, funktioniert die E-Mail-Aktualisierung von Secure Mail wie folgt:

- Wenn Benutzer die **Hintergrundaktualisierung für Apps** auf dem Gerät über das Menü **Einstellungen** aktivieren und Secure Mail im Hintergrund ausgeführt wird, werden E-Mails mit dem Server synchronisiert. Die Häufigkeit der Synchronisierung hängt von verschiedenen Faktoren ab.

- Wenn Benutzer die **Hintergrundaktualisierung von Apps** deaktivieren, erhält die App keine E-Mails, solange sie im Hintergrund ausgeführt wird.
- Verschieben Benutzer Secure Mail in den Hintergrund, wird Secure Mail für kurze Zeit weiter ausgeführt und dann ausgesetzt.
- Wenn Secure Mail im Vordergrund ausgeführt wird, werden die E-Mail-Aktivitäten in Echtzeit angezeigt, unabhängig davon, wie die **Hintergrundaktualisierung** eingestellt ist.

Secure Mail und ActiveSync

Secure Mail wird über das ActiveSync-Nachrichtenprotokoll mit Exchange Server synchronisiert. Diese Funktionalität gibt Benutzern Echtzeitzugriff auf ihre E-Mail, Kontakte und Kalenderereignisse, automatisch erstellte Postfächer und selbst erstellte Ordner in Outlook.

> **Hinweis:**
>
> ActiveSync unterstützt das Synchronisieren öffentlicher Exchange-Ordner nicht. In Exchange Server 2013 wird der Ordner "Entwürfe" von ActiveSync nicht synchronisiert.

Zur Synchronisierung der von Benutzern erstellten Ordner führen Sie die folgenden Schritte aus:

iOS

1. Wechseln Sie zu **Einstellungen > Automatisch aktualisieren**.
2. Legen Sie **Automatisch aktualisieren** auf **Ein** fest.
3. Tippen Sie auf **Ein**. Eine Liste aller Postfächer wird angezeigt.
4. Tippen Sie auf die zu synchronisierenden Ordner.

Android

1. Navigieren Sie zur Postfachliste.
2. Tippen Sie auf das Postfach, das Sie synchronisieren möchten.
3. Tippen Sie auf das Symbol "Mehr" unten rechts.
4. Tippen Sie auf **Synchronisierungsoptionen**.
5. Wählen Sie unter **Häufigkeit des Datenabgleichs** die Häufigkeit der Synchronisierung aus.

Exportieren von Kontakten in Secure Mail

Secure Mail-Benutzer können ihre Kontakte kontinuierlich mit dem Adressbuch des Telefons synchronisieren, einen Kontakt aus Secure Mail exportieren und in das Adressbuch des Telefons importieren oder einen Kontakt als vCard-Anlage teilen.

Damit diese Features verfügbar sind, legen Sie in der Endpoint Management-Konsole die Richtlinie “Kontakte exportieren” für Secure Mail auf **EIN** fest.

Wenn für die Richtlinie **EIN** festgelegt ist, sind die folgenden Optionen in Secure Mail aktiviert:

- **Mit lokalen Kontakten synchronisieren** in den Einstellungen
- Exportieren einzelner Kontakte
- Teilen von Kontakten als vCard-Anlagen

Wenn die Richtlinie “Kontakte exportieren” auf **AUS** festgelegt ist, werden diese Optionen nicht in der App angezeigt.

Wenn die Richtlinie aktiviert ist, müssen Benutzer **Mit lokalen Kontakten synchronisieren** auf **EIN** festlegen, damit Kontakte kontinuierlich vom Mailserver zum Adressbuch des Telefons synchronisiert werden. Solange **Mit lokalen Kontakten synchronisieren** auf **EIN** festgelegt ist, lösen Aktualisierungen in Exchange oder Secure Mail eine Aktualisierung der lokalen Kontakte aus.

Wenn ein Exchange- oder Hotmail-Konto bereits Synchronisierungen mit lokalen Kontakten durchführt, kann Secure Mail aufgrund von Einschränkungen in Android die Kontakte nicht synchronisieren.

Unter iOS können Secure Mail-Kontakte auch dann exportiert und mit den Telefonkontakten synchronisiert werden, wenn Benutzer ein Hotmail- oder Exchange-Konto auf dem Gerät eingerichtet haben. Konfigurieren Sie dieses Feature in Endpoint Management über die Richtlinie “Prüfung auf native Kontakte überschreiben” für Secure Mail. Mit dieser Richtlinie legen Sie fest, ob die in der nativen Kontakte-App konfigurierte Prüfung auf Kontakte aus einem Exchange-/Hotmail-Konto von Secure Mail überschrieben wird. Bei Einstellung **Ein** werden die Kontakte auf dem Gerät synchronisiert, selbst wenn die native Kontakte-App mit dem Exchange-/Hotmail-Konto konfiguriert ist. Bei der Einstellung **Aus** wird das Synchronisieren der Kontakte weiterhin blockiert. Die Standardeinstellung ist **Ein**.

Secure Mail-Benachrichtigungen

In der folgenden Tabelle wird aufgeführt, wie Benachrichtigungen für die unterstützten Mobilgeräte behandelt werden, wenn Secure Mail im Vordergrund oder Hintergrund ausgeführt wird:

Beim Ausführen von Secure Mail im Vordergrund oder Hintergrund:	Verarbeitung von Benachrichtigungen unter iOS	Verarbeitung von Benachrichtigungen unter Android
Vordergrund	Secure Mail unterhält eine persistente ActiveSync-Verbindung zum Synchronisieren der E-Mail- und Kalenderaktivitäten.	Secure Mail unterhält eine persistente ActiveSync-Verbindung zum Synchronisieren der E-Mail- und Kalenderaktivitäten.

Beim Ausführen von Secure Mail im Vordergrund oder Hintergrund:	Verarbeitung von Benachrichtigungen unter iOS	Verarbeitung von Benachrichtigungen unter Android
Hintergrund (oder beendet)	Secure Mail erhält Benachrichtigungen über die iOS-Funktion zur Hintergrundaktualisierung oder über APNs, sofern konfiguriert.	Secure Mail unterhält eine beständige ActiveSync-Verbindung.

Weitere Informationen zur Konfiguration finden Sie unter Pushbenachrichtigungen für Secure Mail für iOS.

Pushbenachrichtigungen mit Rich-Inhalt

Secure Mail für iOS unterstützt Pushbenachrichtigungen mit Rich-Inhalt. Benachrichtigungen mit Rich-Inhalt gewährleisten den Erhalt von Sperrbildschirmbenachrichtigungen für den Posteingang, selbst wenn Secure Mail nicht im Hintergrund ausgeführt wird. Das Feature wird bei Verwendung der kennwortbasierten Authentifizierung und der clientbasierten Authentifizierung unterstützt.

> **Hinweis:**
>
> Aufgrund der geänderten Architektur zur Unterstützung dieses Features ist “Benachrichtigung nur für VIPs” nicht mehr verfügbar.

Stellen Sie zum Aktivieren von Benachrichtigungen mit Rich-Inhalt sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Pushbenachrichtigungen müssen in der Endpoint Management-Konsole auf **EIN** festgelegt sein.
- Die Netzwerkzugriffsrichtlinie ist auf **Uneingeschränkt** oder **Tunnel zum internen Netzwerk** eingestellt. Wenn die Netzwerkzugriffsrichtlinie auf **Tunnel zum internen Netzwerk** festgelegt ist, vergewissern Sie sich, dass der Exchange Web Services-Host (EWS-Host) in der Richtlinie “Hintergrundnetzwerkdienste” konfiguriert ist. Sind EWS- und ActiveSync-Host identisch, stellen Sie sicher, dass der ActiveSync-Host in der Richtlinie “Hintergrundnetzwerkdienste” konfiguriert ist.
- Die Richtlinie “Benachrichtigungen bei gesperrtem Bildschirm steuern” ist auf **Zulassen** oder **E-Mail-Absender oder Ereignistitel** festgelegt.
- Navigieren Sie zu **Secure Mail > Einstellungen > Benachrichtigungen** und aktivieren Sie **E-Mail-Benachrichtigungen**.

Das Feature wird für folgende Konfigurationen nicht unterstützt:

- Moderne Authentifizierung mit Microsoft Office 365 (Oauth)
- Über eine Integration von Endpoint Management in Microsoft InTune/EMS verwaltete Apps
- Mit abgeleiteten Anmeldeinformationen registrierte Geräte

Gründe für die Benachrichtigung “Sie haben neue E-Mails” auf iOS-Geräten

Die Benachrichtigung “Sie haben neue E-Mails” wird auf iOS-Geräten angezeigt, wenn Secure Mail von den Exchange-Webdiensten (EWS) innerhalb der festgelegten Zeit von 30 Sekunden für das Abrufen der Nachrichtendetails keine Antwort erhält.

Grund für dieses Verhalten auf Ihrem Gerät kann auch schlechte WLAN- oder Datenkonnektivität sein.

Abgesehen von der verzögerten EWS-Antwort zeigt Secure Mail auch in folgenden Situationen die Benachrichtigung “Sie haben neue E-Mails” an:

- Wenn Secure Mail die erforderlichen Informationen nicht aus dem sicheren Container lesen kann. Dieses Szenario tritt im Allgemeinen nach dem Neustart des Geräts und vor dem Entsperren des Geräts auf.
- Wenn Secure Mail keine Verbindung oder keinen sicheren Kanal zu Citrix Gateway oder EWS herstellen kann.
- Wenn Ihre Anmeldeinformationen abgelaufen sind oder Sie die Anmeldeinformationen geändert haben, diese jedoch noch nicht in Secure Mail aktualisiert wurden. Die folgende Abbildung zeigt, wie die Benachrichtigung in diesem Szenario angezeigt wird.
- Wenn Secure Mail eine unerwartete Antwort vom Exchange-Server für eine gültige Anforderung von Secure Mail erhält. Weitere Informationen über EWS-Antwortcodes finden Sie in der Dokumentation von Microsoft.

Fehlermeldungen zu Pushbenachrichtigungen in Secure Mail für iOS

In Secure Mail für iOS werden Fehlermeldungen zu Pushbenachrichtigungen in der Mitteilungszentrale auf Geräten angezeigt. Diese Meldungen werden je nach Art des Benachrichtigungsfehlers angezeigt.

Es können die folgenden Meldungen angezeigt werden:

- **Secure Mail kann keine Verbindung zum Netzwerk Ihrer Organisation herstellen.** Diese Meldung wird angezeigt, wenn Secure Mail keine SOCKS5-Verbindung mit Citrix Gateway herstellen kann.
- **Secure Mail kann keine Verbindung zum Netzwerk Ihrer Organisation herstellen. Wenden Sie sich an den Administrator.** Diese Meldung wird angezeigt, wenn Citrix Gateway nicht er-

reichbar ist. Stellen Sie sicher, dass der Citrix ADC einwandfrei konfiguriert und von externen Netzwerken aus erreichbar ist.

- **Secure Mail kann keine sichere Verbindung zum Netzwerk IhrerOrganisation herstellen. Bitte kontaktieren Sie Ihren Administrator.** Diese Meldung wird angezeigt, wenn Secure Mail keine SSL-Verbindung mit Citrix Gateway herstellen kann. Vergewissern Sie sich, dass Ihr SSL-Zertifikat gültig ist.
- **Secure Mail kann keine sichere Verbindung zum Mailserver herstellen. Bitte kontaktieren Sie Ihren Administrator.** Diese Meldung wird angezeigt, wenn Secure Mail keine SSL-Verbindung mit Exchange Server herstellen kann. Vergewissern Sie sich, dass das SSL-Zertifikat auf dem Exchange Server gültig ist. Soll die App eine Verbindung zum Exchange Server herstellen, selbst wenn das Zertifikat ungültig ist, müssen Sie die MDX-Richtlinie "Alle SSL-Zertifikate akzeptieren" aktivieren.
- **Secure Mail kann Nachrichten aufgrund eines Mailserverfehlers nicht abrufen. Bitte kontaktieren Sie Ihren Administrator.** Diese Meldung wird angezeigt, wenn Secure Mail die EWS-Antwort von Exchange Server nicht analysieren kann.
- **Secure Mail kann Nachrichten aufgrund eines Anforderungstimeouts nicht abrufen.** Diese Meldung wird angezeigt, wenn Secure Mail nicht innerhalb von 30 Sekunden eine Antwort vom Server erhält. Der Fehler kann durch eine schlechte Mobil- oder einer Wi-Fi-Verbindung des Geräts verursacht werden. Versuchen Sie es nach ein paar Minuten noch einmal.
- **Nachricht konnte nicht abgerufen werden. Öffnen Sie Secure Mail.** Diese Meldung wird angezeigt, wenn Secure Mail die Anmeldeinformationen aus dem sicheren Container nicht lesen kann. Der Fehler kann auftreten, wenn das Gerät neu gestartet aber noch nicht entsperrt wurde. Entsperren Sie das Gerät, um Secure Mail automatisch Zugriff auf den sicheren Container zu gewähren. Wird der Fehler weiterhin gemeldet, öffnen Sie Secure Mail, um Ihre Anmeldeinformationen im sicheren Container automatisch zu aktualisieren.

Pushbenachrichtigungen für Secure Mail

March 11, 2019

Secure Mail für iOS und Secure Mail für Android können Benachrichtigungen zu E-Mail- und Kalenderaktivitäten erhalten, wenn die App im Hintergrund ausgeführt oder geschlossen wird. Secure Mail für iOS unterstützt Benachrichtigungen über die Hintergrundaktualisierung oder Pushbenachrichtigungen, die über den Apple Dienst für Push-Benachrichtigungen (APNs) bereitgestellt werden. Secure Mail für Android unterstützt Benachrichtigungen, die über den Firebase Cloud Messaging-Dienst (FCM) bereitgestellt werden.

Funktionsweise von Pushbenachrichtigungen

Secure Mail sendet Pushbenachrichtigungen für die folgenden Posteingangsaktivitäten:

- **Neue E-Mails, Besprechungsanfragen, Besprechungsabsagen, Besprechungsupdates:** Wenn der APNs Benachrichtigungen an einen Posteingang sendet, aktualisiert Secure Mail alle Ordner, einschließlich des Kalenders, damit die Änderungen an Besprechungen sofort in den Kalendern der Benutzer übernommen werden.
- **Für iOS ändert sich der Status von Secure Mail von gelesen in ungelesen und umgekehrt.** Das Secure Mail-Symbol zeigt nur die Anzahl der ungelesenen und neuen Nachrichten im Exchange-Posteingangsordner an. Das Symbol wird aktualisiert, wenn Benutzer E-Mails auf einem Desktop oder Laptop gelesen haben.

  Unter iOS zeigt Secure Mail weiterhin die Anzahl der ungelesenen E-Mails im Posteingang für die Synchronisierungsperiode an. Wenn die Richtlinie "Benachrichtigungen bei gesperrtem Bildschirm steuern" auf **Ein** festgelegt ist, werden Pushbenachrichtigungen auf einem gesperrten Bildschirm angezeigt, wenn iOS Secure Mail zum Synchronisieren aktiviert hat.

  Bei einer Installation oder einem Upgrade fordert Secure Mail für iOS die Benutzer auf, Pushbenachrichtigungen zuzulassen. Benutzer können Pushbenachrichtigungen auch später über die iOS-Einstellungen zulassen.

Damit Pushbenachrichtigungen für iOS und Android angezeigt werden, hostet Citrix einen Listenerdienst auf Amazon Web Services (AWS) für die folgenden Funktionen:

- Abhören von Exchange Web Services (EWS) nach Pushbenachrichtigungen, die bei Posteingangsaktivität von Exchange Server gesendet werden. Exchange sendet keinen E-Mail-Inhalt an den Citrix Dienst.

  Vom Citrix Dienst werden keine personenbezogenen Daten gespeichert. Das Gerät und der in Secure Mail zu aktualisierende Posteingangsordner werden stattdessen durch ein Gerätetoken und eine Abonnement-ID identifiziert.
- Senden von APNs-Benachrichtigungen, die ausschließlich Kennzeichenzähler enthalten, an Secure Mail auf iOS-Geräten.
- Senden von FCM-Benachrichtigungen an Secure Mail auf Android-Geräten.

Der Citrix Listenerdienst hat keine Auswirkungen auf den Datenverkehr, der weiter über ActiveSync zwischen Benutzergeräten und Exchange Server fließt. Der Listenerdienst, der für hohe Verfügbarkeit und Notfallwiederherstellung konfiguriert wird, ist in drei Regionen verfügbar:

- Nord- und Südamerika
- Europa, Naher Osten und Afrika (EMEA)
- Asien-Pazifik (APAC)

Systemanforderungen für Pushbenachrichtigungen

Wenn die Citrix Gateway-Konfiguration Secure Ticket Authority (STA) umfasst und Split-Tunneling deaktiviert ist, muss Citrix Gateway Datenverkehr (wenn von Secure Mail getunnelt) zu den folgenden Citrix Listenerdienst-URLs zulassen:

Region	URL	IP-Adresse
Nord- und Südamerika	`https://us-east-1.pushreg.xm.citrix.com`	52.7.65.6; 52.7.147.0
EMEA	`https://eu-west-1.pushreg.xm.citrix.com`	54.154.200.233; 54.154.204.192
APAC	`https://ap-southeast-1.pushreg.xm.citrix.com`	52.74.236.173; 52.74.25.245

Konfigurieren von Secure Mail für Pushbenachrichtigungen

Um Apple-Pushbenachrichtigungen oder FCM für Secure Mail über App-Stores zu verteilen, aktivieren Sie Pushbenachrichtigungen in der Endpoint Management-Konsole mit der Einstellung **Ein** und wählen anschließend Ihre Region aus. Die folgende Abbildung zeigt die Einstellung für iOS.

Für Android wird die entsprechende **Einstellung für Pushbenachrichtigungen** wie für iOS in folgender Abbildung angezeigt. Hier legen Sie zusätzlich den **EWS-Hostnamen** fest, falls sich Exchange-Webdienste (EWS) und Mailserver nicht in derselben Region befinden. Der Standardwert ist leer. Wenn Sie keine Einstellung vornehmen, verwendet Endpoint Management den Hostnamen des Mailservers.

Konfigurieren Sie Exchange und Citrix ADC so, dass sie Datenverkehr an den Listenerdienst zulassen.

Konfigurieren von Exchange Server

Lassen Sie ausgehendes SSL (über Port 443) von Ihrer Firewall zur URL des Citrix Listenerdiensts für die Region zu, in der sich der Exchange Server befindet. Zum Beispiel:

Region	URL	IP-Adresse
Nord- und Südamerika	`https://us-east-1.mailboxlistener.xm.citrix.com`	52.6.252.176; 52.4.180.132

Region	URL	IP-Adresse
EMEA	https://eu-west-1.mailboxlistener.xm.citrix.com	54.77.174.172; 52.17.147.220
APAC	https://ap-southeast-1.mailboxlistener.xm.citrix.com	52.74.231.240; 54.169.87.20

Wenn Sie einen Proxyserver zwischen den Exchange-Webdiensten (EWS) und dem Citrix Listenergerät haben, bestehen folgende Möglichkeiten:

- Senden des EWS-Datenverkehrs über den Proxy an das Listenergerät
- Direktes Senden des EWS-Datenverkehrs zum Listenergerät unter Umgehung des Proxys

EWS-Datenverkehr über den Proxyserver senden: Konfigurieren Sie im Ordner ClientAccess\exchweb\ews die Datei web.config für EWS folgendermaßen:

```
<configuration>
<system.net>
<defaultProxy>
<proxy usesystemdefault=”true” bypassonlocal=”true” />
</defaultProxy>
</system.net>
</configuration>
```

Weitere Informationen zum Konfigurieren von Proxys finden Sie unter Proxykonfiguration.

Für Exchange 2013-Umgebungen müssen Sie den Abschnitt `system.net` manuell zur Datei “web.config” hinzufügen. Davon abgesehen sollten hier beschriebene Konfigurationen für Exchange 2013 funktionieren. Wenden Sie sich für die Problembehandlung an Ihren Exchange-Administrator.

Proxyserver umgehen: Konfigurieren Sie die Umgehungsliste, sodass Exchange Verbindungen mit dem Citrix Listenerdienst herstellen kann.

Wenn Secure Hub mit zertifikatbasierter Authentifizierung registriert wird, müssen Sie Exchange Server für die zertifikatbasierte Authentifizierung ebenfalls konfigurieren. Weitere Informationen finden Sie in Artikel Endpoint Management – Erweiterte Konzepte.

Konfigurieren von Citrix Gateway

Während der Exchange-Server den Datenverkehr an den Listenerdienst zulassen muss, muss Citrix ADC Datenverkehr an den Registrierungsdienst zulassen. Auf diese Weise können Geräte eine

Verbindung zur Registrierung für Pushbenachrichtigungen herstellen.

Wenn EWS und ActiveSync nicht auf demselben Server ausgeführt werden, konfigurieren Sie die Citrix ADC-Richtlinie für den Datenverkehr so, dass EWS-Datenverkehr zulässig ist.

Problembehandlung

Überprüfen Sie zur Problembehandlung von ausgehenden Verbindungen die Exchange-Ereignisprotokolle, die Protokolleinträge aufweisen, wenn eine Abonnementanforderung oder die Benachrichtigung für ein Abonnement ungültig ist oder fehlschlägt. Sie können auch Wireshark-Traces auf dem Exchange Server ausführen, um ausgehenden Datenverkehr zum Citrix Listenerdienst zu verfolgen.

Informationen zu anderen Problemen finden Sie unter Secure Mail Test Tool.

Häufig gestellte Fragen zu Secure Mail-Pushbenachrichtigungen

Wann übermittelt iOS Benachrichtigungen an Secure Mail

Wenn Secure Mail im Vordergrund ausgeführt wird, werden Benachrichtigungen *immer* an Secure Mail übermittelt. Dies ist der einzige Zeitpunkt, zu dem Citrix die Übermittlung von Benachrichtigungen garantieren kann. Wenn Secure Mail im Hintergrund ist, wird der Kennzeichenzähler der Anwendung immer aktualisiert. Benachrichtigungen (Sperrbildschirmbenachrichtigungen und Banner) erfordern jedoch die Hintergrundaktualisierung von Apps und können daher nicht garantiert werden, besonders, wenn iOS die App anhält oder beendet. Citrix hat über folgende Faktoren keine Kontrolle.

In den folgenden Fällen kann die Übermittlung von Benachrichtigungen betroffen sein:

- Der Akkustand ist niedrig.
- Secure Mail wird nicht häufig verwendet und ist selten im Vordergrund.
- E-Mails, die außerhalb der Kernzeiten empfangen werden, wenn die App für einen längeren Zeitraum im Hintergrund ist, z. B. zwischen Mitternacht und 6 Uhr morgens.

Benachrichtigungen werden in den folgenden Fällen *nicht* an Secure Mail übermittelt:

- Wenn der Benutzer Secure Mail schließt, bis die App manuell wieder geöffnet wird.
- Wenn das System Secure Mail beendet hat und die App nicht automatisch neu gestartet wurde.
- Wenn Secure Mail nicht aktiv ist.

> **Wichtig:**
>
> Benachrichtigungen können aus vielen Gründen nicht an Secure Mail übermittelt werden, wenn Secure Mail nicht aktiv ist. Folgendes sind nur einige Beispiele:
>
> - Wenn das Gerät im Energiesparmodus ist und Secure Mail im Hintergrund ausgeführt wird. Dies ist der häufigste Fall, in dem Benachrichtigungen nicht übermittelt werden.

> - Wenn die Hintergrundaktualisierung für Secure Mail deaktiviert ist und wenn Secure Mail im Hintergrund ausgeführt wird. Diese Einstellung wird von den Benutzern gesteuert.
> - Wenn das Gerät keine gute Netzwerkverbindung hat. Diese Situation hängt vom iOS-Gerät ab.

Wenn Secure Mail keine Benachrichtigung erhält, synchronisiert Secure Mail keine neuen Daten mit dem Gerät. Dies kann folgende Konsequenzen haben:

- Secure Mail synchronisiert Daten nur, wenn Benutzer die App in den Vordergrund holen.
- Benachrichtigungen für neue E-Mails werden nicht mehr auf dem Sperrbildschirm angezeigt. Kalendererinnerungen werden jedoch weiterhin angezeigt.

Wann übermittelt Android Benachrichtigungen an Secure Mail

In Android werden Benachrichtigungen stets an Secure Mail gesendet.

Wie wirkt sich FCM auf die E-Mail-Benachrichtigungen aus, die auf dem Sperrbildschirm angezeigt werden

Auf dem Sperrbildschirm angezeigte neue E-Mail-Benachrichtigungen werden anhand von Daten generiert, die von Secure Mail mit dem Gerät synchronisiert werden. Diese Informationen stammen jedoch nicht vom Listenerdienst.

Damit Benachrichtigungen über neue E-Mails angezeigt werden, muss Secure Mail Daten von Exchange synchronisieren können, um die Informationen zum Erstellen der Benachrichtigungen zu haben.

Wenn Sie eine neue E-Mail erhalten, wird die FCM-Benachrichtigung **Sie haben neue Nachrichten** angezeigt. Sobald die E-Mail-Synchronisierung im Hintergrund abgeschlossen ist, wird die neue E-Mail in Secure Mail angezeigt.

Wie wirkt sich die Hintergrundaktualisierung auf Secure Mail und den APNs aus

Wenn Benutzer die Hintergrundaktualisierung deaktivieren, sind folgende Konsequenzen möglich:

- Secure Mail erhält keine Benachrichtigungen, wenn Secure Mail nicht im Hintergrund ist.
- Secure Mail aktualisiert den Sperrbildschirm nicht mit neuen E-Mail-Benachrichtigungen.

Das Deaktivieren der Hintergrundaktualisierung hat gravierende Auswirkungen auf das Verhalten von Secure Mail. Wie zuvor erläutert wird der Kennzeichenzähler basierend auf dem APNs weiterhin aktualisiert, aber in diesem Modus werden keine E-Mails mit dem Gerät synchronisiert.

Wie wirkt sich der Energiesparmodus auf Secure Mail und den APNs aus

Im Hinblick auf Secure Mail verhält sich das System im Energiesparmodus genauso wie bei deaktivierter Hintergrundaktualisierung. Im Energiesparmodus führt das Gerät keine periodische Aktualisierung von Apps aus und übermittelt keine Benachrichtigungen an Apps im Hintergrund. Die Auswirkungen sind die gleichen wie die zuvor im Abschnitt zur Hintergrundaktualisierung aufgeführten Auswirkungen. Im Energiesparmodus werden Kennzeichenzähler basierend auf APNs-Benachrichtigungen weiterhin aktualisiert.

Wie wirkt sich der APNs auf die E-Mail-Benachrichtigungen aus, die auf dem Sperrbildschirm angezeigt werden

Auf dem Sperrbildschirm angezeigte neue E-Mail-Benachrichtigungen werden anhand von Daten generiert, die von Secure Mail mit dem Gerät synchronisiert werden. Diese Informationen stammen jedoch nicht vom Listenerdienst.

Damit Benachrichtigungen über neue E-Mails angezeigt werden, muss Secure Mail Daten von Exchange synchronisieren können, um die Informationen zum Erstellen der Benachrichtigungen zu haben.

Wenn APNs-Benachrichtigungen nicht im Hintergrund an Secure Mail übermittelt werden, erkennt Secure Mail die Benachrichtigungen nicht und synchronisiert daher keine neuen Daten. Weil Secure Mail keine neuen Daten zur Verfügung stehen, werden keine E-Mail-Benachrichtigungen auf dem Sperrbildschirm des Geräts generiert, selbst wenn keine APNs-Benachrichtigungen übermittelt werden.

Welche anderen Gründe kann es für das Fehlschlagen von FCM-gesteuerter Synchronisierung im Hintergrund geben

Verschiedene Probleme können dazu führen, dass FCM-gesteuerte Synchronisierungsanfragen fehlschlagen, einschließlich der Folgenden:

- Ein ungültiges STA-Ticket.
- Wenn Secure Mail im Standbymodus aktiviert wird, hat die App 10 Sekunden Zeit, um alle Daten vom Server zu synchronisieren.

Wenn eine der zuvor erläuterten Bedingungen auftritt, kann die Datensynchronisierung nicht durchgeführt werden. Das Resultat ist, dass Benachrichtigungen nicht auf dem Sperrbildschirm angezeigt werden.

Welche anderen Gründe kann es für das Fehlschlagen von APNs-gesteuerter Synchronisierung im Hintergrund geben

Verschiedene Probleme können dazu führen, dass APNs-gesteuerte Synchronisierungsanfragen fehlschlagen, einschließlich der Folgenden:

- Ein ungültiges STA-Ticket.
- Eine langsame Netzwerkverbindung. Wenn Secure Mail im Hintergrund aktiviert wird, hat die App 30 Sekunden Zeit, um alle Daten vom Server zu synchronisieren.
- Wenn die Datenschutzrichtlinie aktiviert ist und Secure Mail durch eine APNs-Benachrichtigung aktiviert wird, kann Secure Mail bei gesperrtem Gerät nicht auf den Datenspeicher zugreifen und die Synchronisierung wird nicht ausgeführt. Dies tritt nur auf, wenn das System versucht, einen Kaltstart von Secure Mail auszuführen. Wenn ein Benutzer Secure Mail nach dem Entsperren des Geräts bereits gestartet hat, wird die APNs-gesteuerte Synchronisierung auch bei gesperrtem Gerät erfolgreich durchgeführt.

Wenn eine der zuvor erläuterten Bedingungen auftritt, kann Secure Mail keine Daten synchronisieren und daher keine Benachrichtigungen auf dem Sperrbildschirm anzeigen.

Wie generiert Secure Mail Sperrbildschirmbenachrichtigungen, wenn Benachrichtigungen nicht übermittelt werden oder der APNs nicht verwendet wird

Wenn der APNs deaktiviert ist, wird Secure Mail durch regelmäßige App-Hintergrundaktualisierungen von iOS reaktiviert, vorausgesetzt die Hintergrundaktualisierung ist aktiviert und das Gerät ist nicht im Energiesparmodus.

Während dieser Reaktivierungsereignisse synchronisiert Secure Mail neue E-Mails vom Exchange-Server. Mit diesen neuen E-Mails können dann E-Mail-Benachrichtigungen auf dem Sperrbildschirm generiert werden. Auf diese Weise kann Secure Mail Daten im Hintergrund synchronisieren, selbst wenn APNs-Benachrichtigungen nicht übermittelt werden oder APNs deaktiviert ist.

Dies erfolgt nicht so zeitnah wie bei der Verwendung des APNs und wenn APNs-Benachrichtigungen an Secure Mail übermittelt werden. Wenn iOS APNs-Benachrichtigungen an Secure Mail weiterleitet, synchronisiert die App sofort Daten vom Server und die Sperrbildschirmbenachrichtigungen werden in Echtzeit angezeigt.

Wenn die Reaktivierung durch Hintergrundaktualisierung erforderlich ist, werden Sperrbildschirmbenachrichtigungen nicht in Echtzeit übermittelt. In diesem Fall wird Secure Mail mit einer Frequenz reaktiviert, die vollständig von iOS bestimmt wird. Daher kann einige Zeit zwischen der Ankunft einer E-Mail im “Posteingang” auf Exchange und der Synchronisierung der Nachricht sowie dem Generieren der Sperrbildschirmbenachrichtigung durch Secure Mail vergehen.

Secure Mail wird regelmäßig reaktiviert, selbst wenn APNs verwendet wird. Immer wenn die Hintergrundaktualisierung Secure Mail reaktiviert, versucht Secure Mail, Daten von Exchange zu synchronisieren.

Wie unterscheidet sich Secure Mail von anderen Apps, die auf dem Sperrbildschirm Inhalte anzeigen

Ein bedeutender Unterschied zwischen Secure Mail und Gmail, Microsoft Outlook und anderen Apps ist, dass neue E-Mails nicht immer in Echtzeit auf dem Sperrbildschirm angezeigt werden. Die primäre Ursache für diesen Unterschied ist der Aspekt der Sicherheit. Damit Secure Mail sich wie andere Apps verhält, müssten die Anmeldeinformationen des Benutzers von Exchange authentifiziert werden, um den Inhalt der E-Mail abzurufen und diesen Inhalt über den Citrix Listenerdienst sowie den Apple Dienst für Push-Benachrichtigungen weiterzuleiten. Die von Citrix gewählte Methode für APNs-Benachrichtigungen erfordert kein Abrufen oder Speichern des Kennworts der Benutzer durch den Citrix Listenerdienst. Der Listenerdienst hat keinen Zugriff auf das Postfach oder Kennwort von Benutzern.

Hinweis zur nativen iOS-Mail-App: iOS erlaubt der eigenen Mail-App eine ständige Verbindung mit dem Mailserver, die sicherstellt, dass Benachrichtigungen immer übermittelt werden. Diese Funktion wird Apps von Drittanbietern nicht erlaubt.

App-Verhalten von Gmail: Google ist Eigentümer der Gmail-App und des Gmail-Servers und hat daher die Kontrolle über beide. Daher kann Google den Inhalt von Nachrichten lesen und der APNs-Benachrichtigungsnutzlast hinzufügen. Wenn iOS die APNs-Benachrichtigung von Gmail empfängt, führt iOS folgende Schritte aus:

- Der Kennzeichenzähler wird auf den Wert festgelegt, der in der Benachrichtigungsnutzlast angegeben ist.
- Mit dem in der Benachrichtigungsnutzlast enthaltenen Nachrichtentext wird die Sperrbildschirmbenachrichtigung angezeigt.

Der wesentliche Unterschied ist, dass nicht die Gmail-App sondern iOS die Sperrbildschirmbenachrichtigung anzeigt, die anhand der in der Nutzlast enthaltenen Daten generiert wurde. iOS reaktiviert die Gmail-App möglicherweise gar nicht, ähnlich wie iOS Secure Mail u. U. nicht reaktiviert, wenn eine Benachrichtigung empfangen wird. Aber weil die Nutzlast den Nachrichtenausschnitt enthält, kann iOS die Sperrbildschirmbenachrichtigung anzeigen, ohne dass E-Mail-Daten auf das Gerät synchronisiert werden.

In Secure Mail ist die Situation anders. Secure Mail muss zuerst Nachrichtendaten von Exchange synchronisieren, bevor die App die Sperrbildschirmbenachrichtigung anzeigen kann.

App-Verhalten von Outlook für iOS: Microsoft steuert Outlook für iOS. Die Organisation, zu der der Benutzer gehört, kontrolliert jedoch den Exchange-Server, von dem die Daten abgerufen werden. Un-

abhängig von diesem Setup kann Outlook Sperrbildschirmbenachrichtigungen basierend auf Daten anzeigen, die Microsoft in den APNs-Benachrichtigungen übermittelt, da Outlook für iOS ein Modell nutzt, in dem Microsoft die Anmeldeinformationen von Benutzern speichert. Microsoft greift dann direkt über seinen Cloud-Dienst auf das Postfach des Benutzers zu und prüft, ob neue E-Mails vorhanden sind.

Wenn neue E-Mails vorhanden sind, generiert der Microsoft Cloud-Dienst eine APNs-Benachrichtigung mit den neuen Nachrichtendaten. Dieses Modell funktioniert ähnlich wie das Gmail-Modell, indem sich iOS einfach die Daten nimmt und damit eine Sperrbildschirmbenachrichtigung generiert. Die Outlook-App von iOS ist an dem Vorgang nicht beteiligt.

Wichtiger Sicherheitshinweis zu Outlook für iOS: Die Methode von Outlook für iOS bringt klare Sicherheitsrisiken mit sich. Organisationen müssen Microsoft die Kennwörter ihrer Benutzer anvertrauen, damit Microsoft auf die Postfächer von Benutzern zugreifen kann. Dies stellt ein Sicherheitsrisiko dar. Weitere Informationen darüber, wie Microsoft Benutzerkennwörter verwaltet, finden Sie unter Microsoft TechNet.

Weitere, von Administratoren häufig gestellte Fragen zu Pushbenachrichtigungen finden Sie in diesem Support Knowledge Center-Artikel. Benutzerspezifische Fragen finden Sie in diesem Support Knowledge Center-Artikel.

Interaktivität zwischen Secure Mail und anderen mobilen Produktivitätsapps und Citrix Files

February 11, 2019

Die Interaktivität zwischen Secure Mail und anderen mobilen Produktivitätsapps sowie Citrix Files ermöglicht den nahtlosen Zugriff sowie das Bearbeiten, Freigeben und Speichern von Dokumenten, ohne dass die Benutzer die durch die Unternehmensrichtlinien geschaffene sichere Umgebung verlassen müssen. Beispielsweise wird durch Tippen auf einen Link in Secure Mail die zugehörige Website in Secure Web geöffnet. Benutzer können Anlagen mit Citrix QuickEdit für Endpoint Management öffnen und bearbeiten. Anlagen werden in den für den Benutzer konfigurierten Citrix Files-Bereich für Endpoint Management heruntergeladen.

Eine vollständige Liste der Secure Mail-Features für die einzelnen Plattformen finden Sie unter Features nach Plattform.

Testen und Problembehandlung von Secure Mail

March 11, 2019

Wenn Secure Mail nicht richtig funktioniert, ist die Ursache meistens ein Problem mit der Verbindung. In diesem Artikel wird beschrieben, wie Sie Verbindungsprobleme vermeiden. Darüber hinaus wird in diesem Artikel die Problembehandlung von eventuellen Problemen erläutert.

Testen von ActiveSync-Verbindungen, Benutzerauthentifizierung und APNs-Konfiguration

Mit Endpoint Management Analyzer können Sie die Funktion des Autodiscovery-Diensts von Secure Mail prüfen. Endpoint Management Analyzer unterstützt Sie beim Herunterladen der Testanwendung für Endpoint Management Exchange ActiveSync. Die Mail-Testoption überprüft allgemeine Verbindungseinstellungen zum Mailserver. Sie können damit auch prüfen, ob die ActiveSync-Server für die Bereitstellung in einer Endpoint Management-Umgebung geeignet sind. Weitere Informationen finden Sie unter Endpoint Management Analyzer.

Die Mail-Testoption im Analyzer überprüft Folgendes:

- iOS- und Android-Geräteverbindungen mit Microsoft Exchange- oder IBM Traveler-Servern.
- Benutzerauthentifizierung.
- Konfiguration für Pushbenachrichtigungen für iOS, einschließlich Exchange Server, Exchange Web Services (EWS), Citrix Gateway, APNs-Zertifikate und Secure Mail. Informationen zum Konfigurieren von Pushbenachrichtigungen finden Sie unter Pushbenachrichtigungen für Secure Mail für iOS.

Das Tool bietet eine umfassende Liste mit Empfehlungen für die Behebung von Problemen.

> Hinweis:
>
> Die E-Mail-Test-App MailTest.ipa ist veraltet. Nutzen Sie stattdessen die entsprechende Funkion in Endpoint Management Analyzer.

Voraussetzungen für Tests

- Stellen Sie sicher, dass die Richtlinie “Netzwerkzugriff” nicht blockiert wird.
- Legen Sie die Richtlinie “Verfassen von E-Mails blockieren” auf **Aus** fest.

Verwenden von Secure Mail-Protokollen zum Beheben von Verbindungsproblemen

Mit den folgenden Schritte rufen Sie Secure Mail-Protokolle ab.

1. Navigieren Sie zu **Secure Hub > Hilfe > Problem melden**.
2. Wählen Sie **Secure Mail** aus der Liste der Apps.

   Eine an den Helpdesk Ihrer Organisation adressierte E-Mail wird geöffnet.
3. Geben Sie einen Betreff an und beschreiben Sie mit einigen Wörtern das Problem.
4. Wählen Sie den Zeitraum, in dem das Problem auftrat.
5. Ändern Sie die Protokolleinstellungen nur, wenn das Supportteam Sie dazu angewiesen hat.
6. Klicken Sie auf **Senden**.

   Die vollständige Nachricht wird einschließlich der in einer Zip angefügten Protokolldateien geöffnet.
7. 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-Infoprotokolle enthalten Informationen über das Gerät und die App. Vergewissern Sie sich, dass Hardwaremodell und Plattformversion unterstützt werden. Stellen Sie sicher, dass die verwendeten Versionen von Secure Mail und MDX Toolkit die aktuellen Versionen und kompatibel sind. Weitere Informationen finden Sie unter Systemanforderungen für Secure Mail und Endpoint Management-Kompatibilität.

- CtxLog_VPNConfig.xml (iOS) und VpnConfig.xml (Android)

Die VPN-Konfigurationsprotokolle sind nur für Secure Hub verfügbar. Überprüfen Sie, ob die aktuelle Citrix ADC-Version (`ServerBuildVersion`) verwendet wird. Überprüfen Sie die Einstellungen von `SplitDNS` und `SplitTunnel` wie folgt:

- Wenn “Split DNS” auf **Remote**, **Local** oder **Both** eingestellt ist, stellen Sie sicher, dass der FQDN des Mailservers über DNS aufgelöst wird. (Split DNS ist für Secure Hub auf Android verfügbar).
- Wenn “Split Tunnel” auf **On** eingestellt ist, stellen Sie sicher, dass der Mailserver als eine der auf dem Back-End zugänglichen Internet-Apps aufgelistet ist.
- CtxLog_AppPolicies.xml (iOS), Policy.xml (Android und Windows Phone)

Die Richtlinienprotokolle enthalten die Werte aller für Secure Mail festgelegten MDX-Richtlinien zum Zeitpunkt des Protokollabrufs. Überprüfen Sie bei Verbindungsproblemen die Werte für die Richtlinien <`BackgroundServices`> und <`BackgroundServicesGateway`>.

- Diagnoseprotokolle (im Diagnoseordner)

Bei Erstkonfigurationen von Secure Mail ist das häufigste Problem “Ihr Firmennetzwerk ist zurzeit nicht verfügbar”. Mit den Diagnoseprotokollen können Sie Verbindungsprobleme wie folgt beheben.

Die wichtigsten Spalten in den Diagnoseprotokollen sind Timestamp, Message Class und Message. Wenn eine Fehlermeldung in Secure Mail angezeigt wird, notieren Sie die Zeit, damit Sie entsprechende Protokolleinträge schnell in der Spalte **Zeitstempel** finden können.

Um zu ermitteln, ob die Verbindung zwischen Gerät und Citrix Gateway funktioniert, überprüfen Sie die Einträge für AG Tunneler. Die folgenden Meldungen geben an, dass die Verbindung funktioniert:

- AG policy Intercepting FQDN:443 for STA tunneling
- New TCP proxy connection to (null):443 established

Um zu ermitteln, ob die Verbindung zwischen Citrix Gateway und Endpoint Management funktioniert (und das STA-Ticket validiert wird), gehen Sie wie fogt vor: Überprüfen Sie im Secure Hub-Diagnoseprotokoll die INFO (4)-Einträge unter “Message Class” für den Registrierungszeitpunkt des Geräts. Die folgenden Meldungen geben an, dass Secure Hub ein STA-Ticket von Endpoint Management erhalten hat:

- Getting STA Ticket.
- Got STA Ticket response.
- STA Ticket – Success obtaining STA ticket for App – Secure Mail.

> Hinweis:
>
> Bei der Registrierung fordert Secure Hub ein STA-Ticket von Endpoint Management an. Endpoint Management sendet das STA-Ticket an das Gerät, wo es gespeichert und der STA-Ticketliste von Endpoint Management hinzugefügt wird.

Wenn Sie wissen möchten, ob Endpoint Management ein STA-Ticket für einen Benutzer ausgestellt hat, überprüfen Sie das im Supportpaket enthaltene Protokoll UserAuditLogFile.log. Dort sind für alle Tickets Ausstellungszeit, Benutzername, Benutzergerät und Ergebnis aufgelistet. Zum Beispiel:

Time: 2015-06-30T 12:26:34.771-0700

User: user2

Device: Mozilla/5.0 (iPad; CPU OS 8_1_2 like macOS)

Result: Successfully generated STA ticket for user ‘user2’ for app ‘Secure Mail’

Überprüfen Sie die Kommunikation zwischen Citrix Gateway und dem E-Mail-Server und ob die DNS- und Netzwerkeinstellungen richtig konfiguriert sind. Greifen Sie dazu mit Secure Web auf Outlook Web Access (OWA) zu. Wie Secure Mail kann Secure Web über einen Micro VPN-Tunnel eine Verbindung mit Citrix Gateway herstellen. Secure Web fungiert als Proxy für die interne oder externe Ressource, auf die die App zugreift. In den meisten Fällen und besonders in einer Exchange-Umgebung wird OWA auf dem Mailserver gehostet.

Öffnen Sie zum Testen der Konfiguration Secure Web und geben Sie den FQDN der OWA-Seite ein. Diese Anforderung wird mit der gleichen DNS-Auflösung und Route übermittelt wie die Kommunika-

tion zwischen Citrix Gateway und dem Mailserver. Wenn die OWA-Seite geöffnet wird, wissen Sie, dass Citrix Gateway mit dem Mailserver kommuniziert.

Wenn die vorherigen Prüfungen ergaben, dass die Kommunikation erfolgreich ist, wissen Sie, dass die Ursache des Problems nicht der Citrix-Setup ist. Stattdessen liegt das Problem am Exchange- oder Traveler-Server.

Sie können Informationen für Ihre Exchange- oder Traveler-Serveradministratoren sammeln. Ermitteln Sie zunächst, ob HTTP-Probleme auf dem Exchange- oder Traveler-Server vorliegen, indem Sie im Secure Mail-Diagnoseprotokoll nach dem Wort "Error" suchen. Wenn die Fehler HTTP-Codes enthalten und Sie mehrere Exchange- oder Traveler-Server haben, untersuchen Sie jeden Server. Exchange und Traveler verfügen über HTTP-Protokolle, die HTTP-Anfragen und Antworten von Clientgeräten aufführen. Das Protokoll für Exchange ist C:\inetpub\LogFiles\W3SVC1\U_EX.log. Das Protokoll für Traveler ist IBM_TECHNICAL_SUPPORT>HTTHR.log.

Aufrufen von Absturzprotokollen zu Secure Mail für iOS

1. Gehen Sie auf dem iOS-Gerät zu **Settings** > **Privacy** > **Analytics** > **Analytics Data**.
2. Klicken Sie in der Liste **Data** auf den Namen der App und den entsprechenden Zeitstempel. Die Protokolle werden angezeigt.

Beheben von Problemen mit E-Mail, Kontakten oder Kalender

Wenn Sie beispielsweise keine E-Mails senden können oder E-Mails im Entwurfsordner hängenbleiben, Kontakte fehlen oder Kalendereinträge nicht synchronisiert sind, können Sie diese Probleme in Secure Mail beheben. In solchen Fällen verwenden Sie die Exchange ActiveSync-Postfachprotokolle für die Problembehandlung. Die Protokolle führen eingehende Anfragen von den Benutzergeräten und ausgehende Antworten vom Mailserver auf.

Weitere Informationen finden Sie in dem TechNet-Blogbeitrag Under the Hood: Exchange ActiveSync Mailbox Log Analysis.

Bewährte Methoden für die unbegrenzte Synchronisierung

Wenn Benutzer den E-Mail-Synchronisierungszeitraum auf **Alles** festlegen, erfolgt eine unbegrenzte Synchronisierung. Für die unbegrenzte Synchronisierung wird angenommen, dass die Benutzer ihre Postfachgröße, d. h. den Posteingang und alle synchronisierten Ordner, verwalten. Zur Gewährleistung der optimalen Leistung sind einige Punkte zu berücksichtigen:

1. Wenn die Postfachgröße insgesamt 18.000 Nachrichten oder 600 MB überschreitet, kann dies die E-Mail-Synchronisierung verlangsamen.

2. Die Aktivierung von **Anlagen mit Wi-Fi laden** bei Verwendung der unbegrenzten Synchronisierung wird nicht empfohlen. Diese Option kann innerhalb kurzer Zeit zu einer großen E-Mail-Datenmenge auf dem Gerät führen.
3. Wenn Sie die Aktivierung der unbegrenzten Synchronisierung durch die Benutzer verhindern möchten, legen Sie die Richtlinie **Max. Synchronisierungsintervall** auf einen anderen Wert als **Alle** fest.
4. Es wird nicht empfohlen, **Alle** für **Standardsynchronisierungsintervall** festzulegen.

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