Secure Mail

Contents

Überblick über Secure Mail

June 6, 2024

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

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

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

Secure Mail ist mit folgender Software kompatibel:

- Exchange Server 2019 Cumulative Update 14
- Exchange Server 2019 Cumulative Update 13
- Exchange Server 2019 Cumulative Update 12
- Exchange Server 2019 Cumulative Update 11
- Exchange Server 2019 Cumulative Update 10
- Exchange Server 2019 Cumulative Update 9
- Exchange Server 2019 Cumulative Update 8
- Exchange Server 2019 Cumulative Update 7
- Exchange Server 2019 Cumulative Update 6
- Exchange Server 2016 Cumulative Update 23
- Exchange Server 2016 Cumulative Update 22
- Exchange Server 2016 Cumulative Update 21
- Exchange Server 2016 Cumulative Update 20
- Exchange Server 2016 Cumulative Update 19
- Exchange Server 2016 Cumulative Update 18
- Exchange Server 2016 Cumulative Update 17
- Exchange Server 2013 Cumulative Update 23
- Exchange Server 2013 Cumulative Update 22
- Exchange Server 2013 Cumulative Update 21
- HCL Domino Version 12.0.2 FP2
- HCL Traveler Version 12.0.2.1 Build 202302010413_30

- HCL Domino 11 (früher Lotus Notes)
- HCL Domino 10.0.1 (früher Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197 (früher Lotus Notes)
- HCL Domino 10.0.1.0 Build 201811191126_20 (früher Lotus Notes)
- HCL Domino 9.0.1.21 (früher Lotus Notes)
- Microsoft Office 365 (Exchange Online)

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

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

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

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

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

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

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

Was ist neu in Secure Mail

June 6, 2024

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

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

> **Hinweis:**
>
> Secure Mail bietet ab September 2023 keine Unterstützung mehr für Android 7.x und iOS 12.x.

Was ist neu in der aktuellen Version

Secure Mail für iOS 24.3.0

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

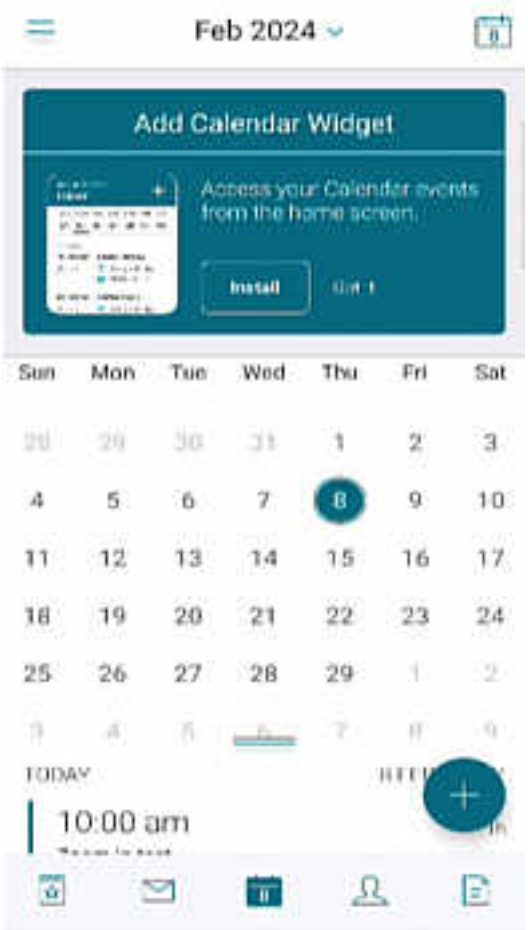
Was ist neu in früheren Releases

Secure Mail für iOS 24.2.0

In diesem Release wurde die allgemeine Leistung und Stabilität verbessert.

Secure Mail für Android 24.1.0

Unterstützt das Zoom-In-Feature für Kalenderereignisse Ab Version 24.1.0 unterstützt Secure Mail für Android das Zoom-In-Feature für Kalenderereignisse. Dieses Feature ist standardmäßig aktiviert. Jetzt gilt das Zoom-In-Feature sowohl für Nachrichten als auch für Kalenderereignisse. Das erweiterte Zoom-In-Feature bietet eine bessere Benutzererfahrung.



Secure Mail für iOS 23.9.0

Unterstützung für iOS 17 Ab diesem Release wird Secure Mail auf Geräten mit iOS 17 unterstützt. Ein Upgrade auf die Secure Mail-Version auf 23.9.0 gewährleistet, dass Geräte, die auf iOS 17 aktualisiert werden, weiter unterstützt werden.

Unterstützung für HCL Domino 12 Ab diesem Release bietet Secure Mail für Android und iOS Unterstützung für HCL Domino Version 12.0.2 FP2 und HCL Traveler Version 12.0.2.1 Build 202302010413_30.

> **Hinweis:**
>
> Wenn Sie ein Upgrade von HCL Domino 11 auf HCL Domino 12 durchführen, stellen Sie sicher, dass Sie den folgenden Benutzer-Agent in der Datei **notes.ini** auf dem Domino-Server aktualisieren. Damit wird sichergestellt, dass alle ActiveSync 16.1-Funktionen, wie Entwurfssynchronisierung und Kalenderanhänge, in Secure Mail weiterhin ordnungsgemäß funktionieren. Weitere Informationen finden Sie unter How to enable Citrix Secure Mail clients for HCL Traveler Exchange ActiveSync 16.1 Support.
>
> `NTS_DEVICE_TYPE_USER_AGENT_APPLE=(^Apple-(iPhone|iPod|iPad|Touchdown))|(^Mozilla.(iPhone|iPod|iPad))|(^WorxMail.(iPhone|iPod|iPad))`

Secure Mail für Android 23.8.2

E-Mail-Anhänge ohne Wasserzeichen anzeigen Wenn Sie Secure Mail für Android Version 23.8.1 oder früher verwenden, sehen Sie beim Anzeigen von E-Mail-Anhängen ein Wasserzeichen. Um E-Mail-Anhänge ohne Wasserzeichen anzuzeigen, aktualisieren Sie auf Secure Mail für Android Version 23.8.2 oder höher.

> **Hinweis:**
>
> Nach dem 31. Oktober 2023 behebt ein Upgrade auf die Version 23.8.1 das Wasserzeichenproblem in E-Mail-Anhängen nicht. Daher wird empfohlen, auf die Version 23.8.2 zu aktualisieren.

Secure Mail für Android 23.8.1

E-Mail-Anhänge ohne Wasserzeichen anzeigen Wenn Sie Secure Mail für Android Version 23.8.0 oder früher verwenden, sehen Sie möglicherweise ein Wasserzeichen, wenn Sie E-Mail-Anhänge anzeigen. Um E-Mail-Anhänge ohne Wasserzeichen anzuzeigen, aktualisieren Sie auf Secure Mail für Android Version 23.8.1 oder höher.

Unterstützung für HCL Domino 12 Ab diesem Release bietet Secure Mail für Android und iOS Unterstützung für HCL Domino Version 12.0.2 FP2 und HCL Traveler Version 12.0.2.1 Build 202302010413_30.

> **Hinweis:**
>
> Wenn Sie ein Upgrade von HCL Domino 11 auf HCL Domino 12 durchführen, stellen Sie sicher,

> dass Sie den folgenden Benutzer-Agent in der Datei **notes.ini** auf dem Domino-Server aktualisieren. Damit wird sichergestellt, dass alle ActiveSync 16.1-Funktionen, wie Entwurfssynchronisierung und Kalenderanhänge, in Secure Mail weiterhin ordnungsgemäß funktionieren. Weitere Informationen finden Sie unter How to enable Citrix Secure Mail clients for HCL Traveler Exchange ActiveSync 16.1 Support.
>
> `NTS_DEVICE_TYPE_USER_AGENT_APPLE=(^Apple-(iPhone|iPod|iPad|Touchdown))|(^Mozilla.(iPhone|iPod|iPad))|(^WorxMail.(iPhone|iPod|iPad))`

Secure Mail für Android 23.8.0

Unterstützung für Android 14 Ab diesem Release wird Secure Mail auf Geräten mit Android 14 unterstützt. Ein Upgrade auf die Secure Mail-Version auf 23.8.0 gewährleistet, dass Geräte, die auf Android 14 aktualisiert werden, weiter unterstützt werden.

Secure Mail für Android 23.7.0

Unterstützung für Microsoft Exchange Cumulative Update 13 Ab Version 23.7.0 unterstützt Secure Mail das Cumulative Update 13 für Microsoft Exchange Server 2019.

Unterstützung für hybride moderne Authentifizierung mit on-premises Exchange Secure Mail unterstützt jetzt hybride moderne Authentifizierung (HMA) mit dem Cumulative Update 8 für Exchange Server 2016 und dem Cumulative Update 19 für Exchange Server 2013.

Secure Mail für iOS 23.7.0

Unterstützung für hybride moderne Authentifizierung mit on-premises Exchange Secure Mail unterstützt jetzt hybride moderne Authentifizierung (HMA) mit dem Cumulative Update 8 für Exchange Server 2016 und dem Cumulative Update 19 für Exchange Server 2013.

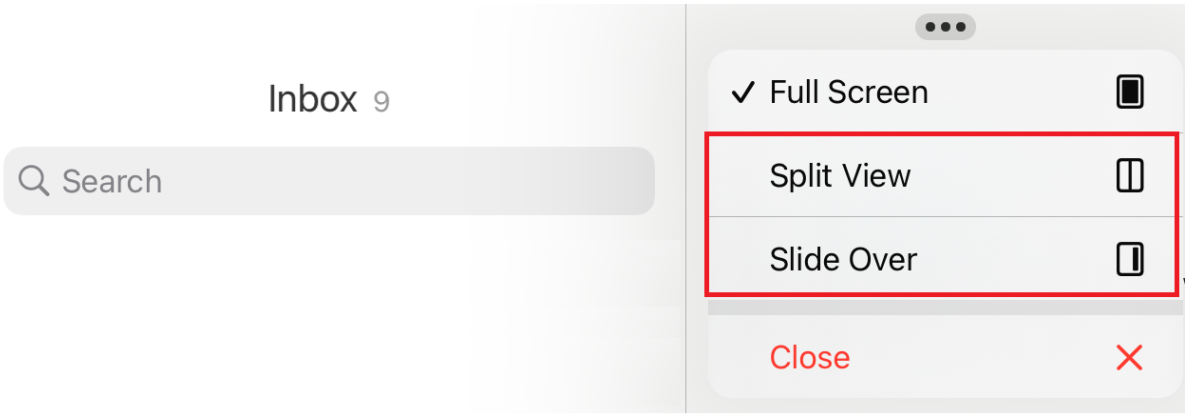
Dunkler Modus Ab Version 23.7.0 unterstützt Secure Mail den dunklen Modus. Um E-Mails im dunklen Modus anzuzeigen, gehen Sie in der App zu **Einstellungen** > **App-Design** > und wählen Sie **Dunkler Modus**.

Secure Mail für Android 23.6.0

Dunkler Modus Ab Version 23.6.0 unterstützt Secure Mail den dunklen Modus. Um E-Mails im dunklen Modus anzuzeigen, gehen Sie in der App zu **Einstellungen** > **App-Design** > und wählen Sie **Dunkler Modus**.

Secure Mail für iOS 23.5.0

Multitasking in den Modi "Split View"und "Slide Over" Ab Release 23.5.0 unterstützt Secure Mail Multitasking auf iPad-Geräten. Öffnen Sie Secure Mail und tippen Sie auf die Auslassungspunkte, um die Option **Split View** oder **Slide Over** für Multitasking auszuwählen. Diese Funktion fördert die Produktivität der Benutzer.



Im Modus **Split View** wird die zweite App neben der aktuellen App angezeigt. Im Modus **Slide Over** wird die zweite App im Vollbildmodus geöffnet und das Fenster der aktuellen App verkleinert. Sie können dieses nach rechts oder links verschieben.

Secure Mail 23.3.5

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 23.2.0

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail 22.11.0

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 22.9.0

Secure Mail für iOS Secure Mail unterstützt jetzt iOS 16.

Secure Mail für Android Secure Mail unterstützt jetzt Android 13.

Secure Mail 22.6.2

Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail 22.6.0

Ab dieser Version enthält Secure Mail Unterstützung für Exchange Server 2016 Cumulative Update 23.

Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 22.3.0

Secure Mail für iOS **Unterstützung für HCL Domino 11**. Ab dieser Version unterstützt Secure Mail für iOS HCL Domino 11 (ehemals Lotus Notes).

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

Secure Mail für Android **Unterstützung für HCL Domino 11**. Ab dieser Version unterstützt Secure Mail für Android HCL Domino 11 (ehemals Lotus Notes).

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

Secure Mail 22.2.0

Secure Mail für iOS Die Option zum Verwalten Ihrer Feeds war in Version 21.5.0 veraltet. In dieser Version werden nur die folgenden Standardfeedkarten in Secure Mail für iOS angezeigt:

- Ungelesen
- Besprechungseinladungen
- Anstehende Besprechungen
- Von Ihrem Manager

Wenn Sie diese Funktion derzeit aktiviert und konfiguriert haben, werden die Einstellungen mit den Standardkarten überschrieben.

Secure Mail für Android Die Option zum Verwalten Ihrer Feeds war in Version 21.5.0 veraltet. In dieser Version werden nur die folgenden Standardfeedkarten in Secure Mail für iOS angezeigt:

- Ungelesen
- Besprechungseinladungen
- Anstehende Besprechungen
- Von Ihrem Manager

Wenn Sie diese Funktion derzeit aktiviert und konfiguriert haben, werden die Einstellungen mit den Standardkarten überschrieben.

Secure Mail 21.12.0

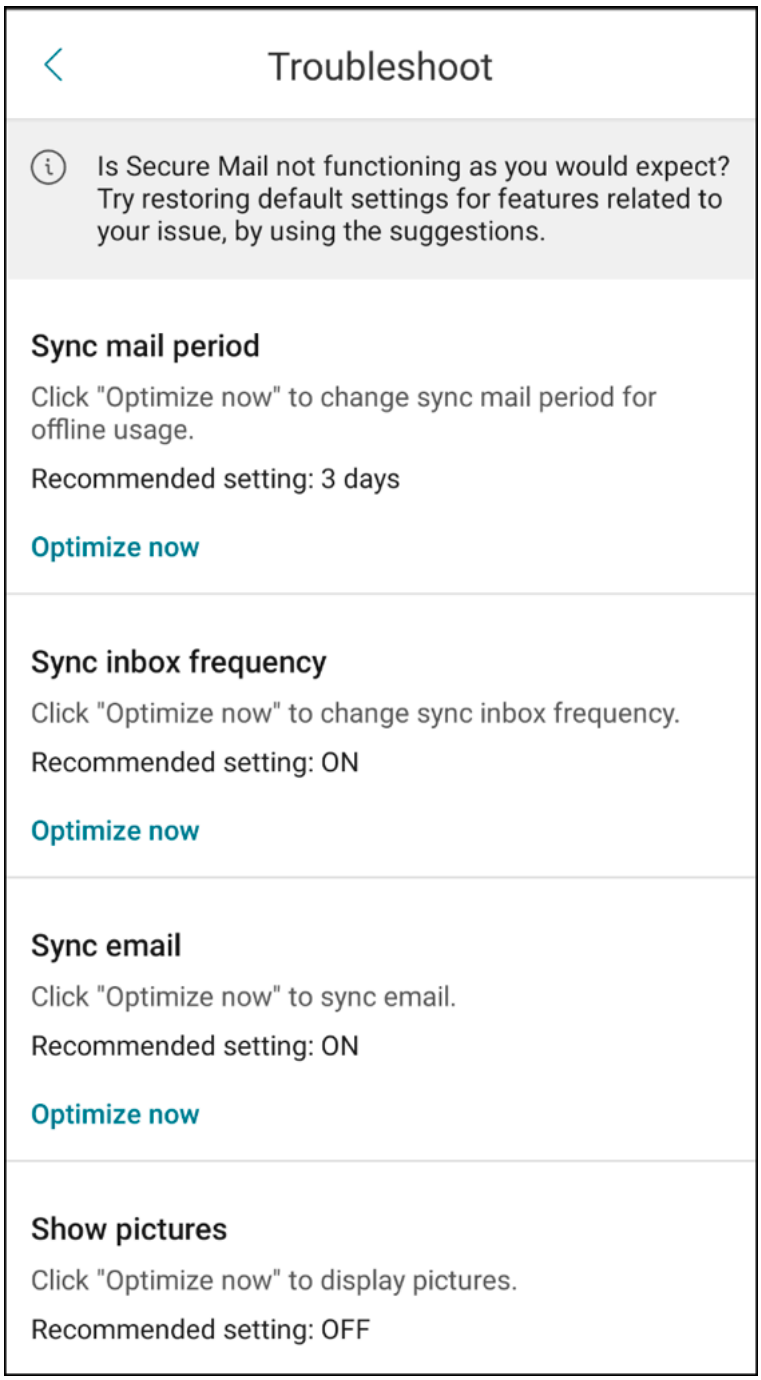
Secure Mail für iOS Unterstützung für benutzerdefinierten Benutzeragent. Ab diesem Release können Sie für Active Directory-Verbunddienste (AD FS) oder Identitätsanbieter (IdP) benutzerdefinierte Benutzeragents für die Authentifizierung mit Microsoft Office 365 verwenden. Um diese Funktion verwenden zu können, müssen Sie die Richtlinie **Benutzerdefinierter Benutzeragent für moderne Authentifizierung** in der Citrix Endpoint Management-Konsole aktivieren und konfigurieren.

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 21.11.0

Secure Mail für Android

Selbstdiagnosetool Sie können jetzt eine Problembehandlung für Fehler durchführen, die in Secure Mail für Android auftreten könnten. Verwenden Sie die Schaltfläche **Problembehandlung** unter der Menüoption **Support** in den App-Einstellungen. Zum Beheben von Problemen öffnen Sie Secure Mail und navigieren Sie zu **Einstellungen** > **Problembehandlung**.



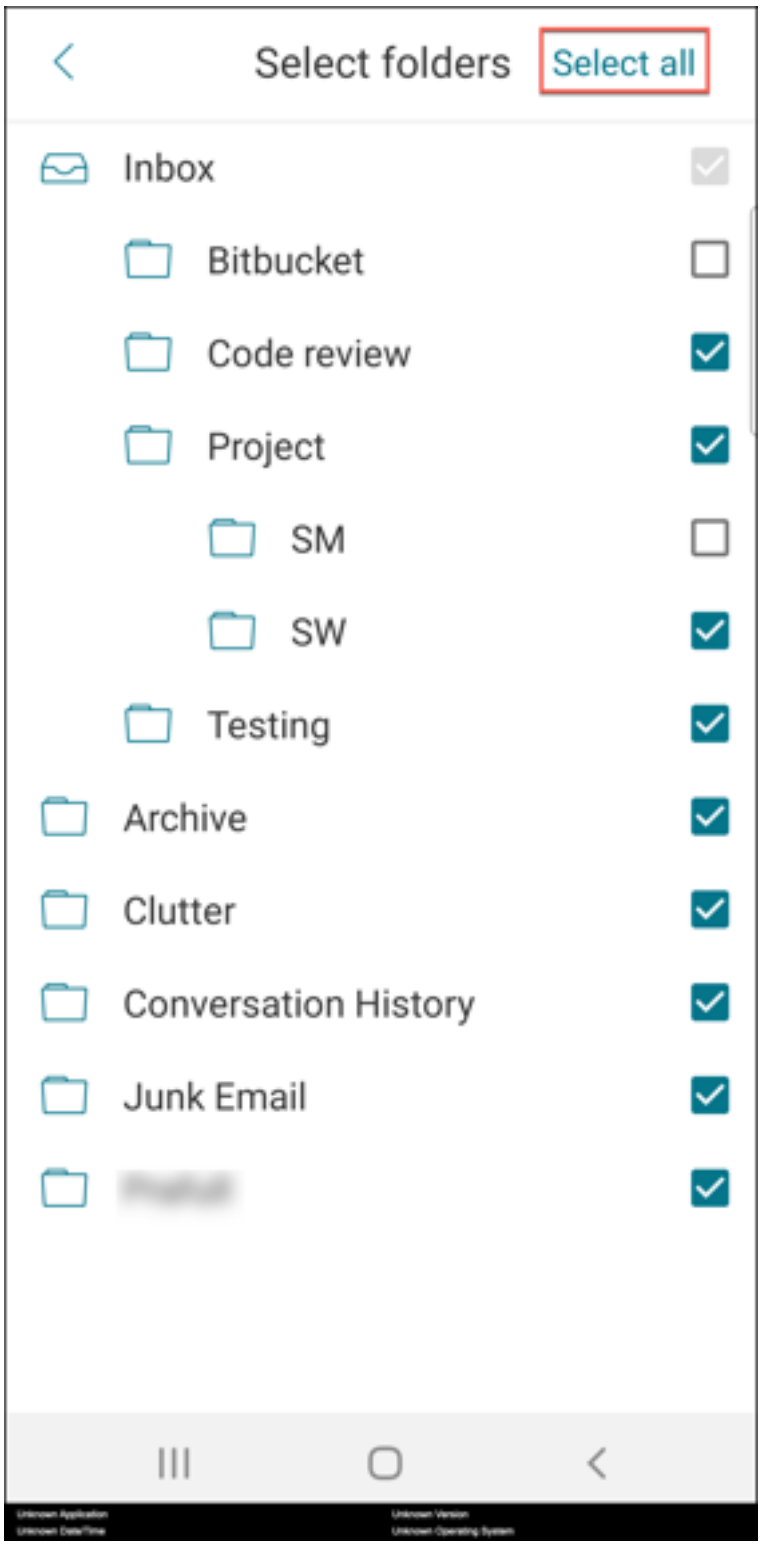
Die folgenden Menüelemente werden zur Problembehandlung angezeigt:

- Standard-App-Einstellungen löschen
- Standard-Erinnerungszeit
- Akkuoptimierungen ignorieren
- Kalenderbenachrichtigungen verwalten
- E-Mail-Benachrichtigungen verwalten
- Fotos anzeigen

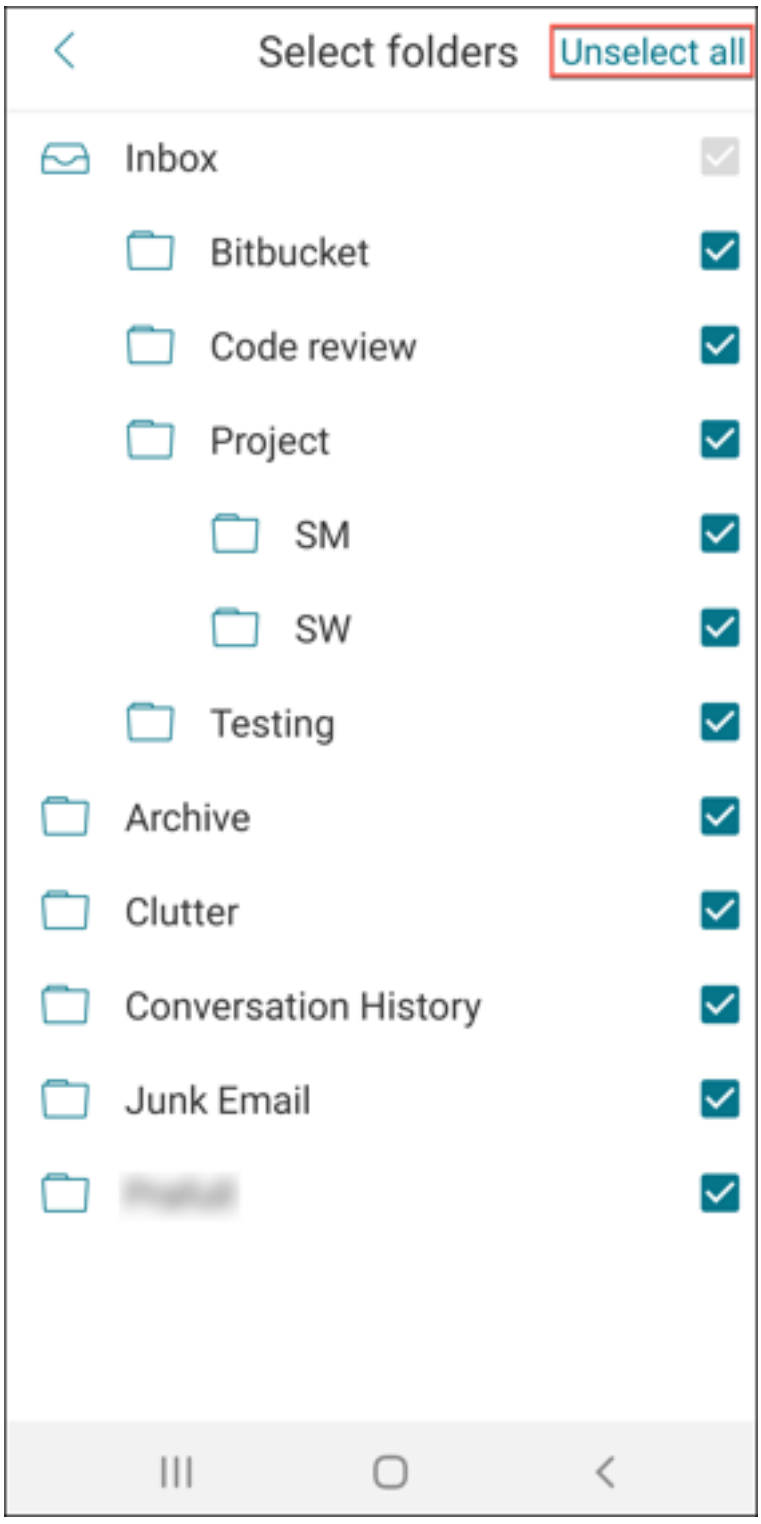
- Kalender synchronisieren
- Kontakte synchronisieren
- E-Mails synchronisieren
- Synchronisierungshäufigkeit - Posteingang
- Mail-Sync-Zeitraum

Wenn diese Einstellungen alle auf die Standardwerte zurückgesetzt wurden und Sie immer noch Probleme mit der Secure Mail haben, wenden Sie sich an Ihren Administrator.

Verbesserungen bei Benachrichtigungen zu Unterordnern Sie können jetzt Benachrichtigungen für alle Unterordner erhalten, indem Sie zu **Einstellungen** > **Benachrichtigungen** > **E-Mail-Ordner** navigieren und im Bildschirm **Ordner auswählen** auf die Option **Alle auswählen** klicken.



Klicken Sie auf **Gesamte Auswahl aufheben**, um Benachrichtigungen für alle Unterordner zu deaktivieren.



Secure Mail 21.10.5

Ab dieser Version bietet Secure Mail Unterstützung für Exchange Server 2019 Cumulative Update 11 und für Exchange Server 2016 Cumulative Update 22.

Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail für Android Dieses Release enthält Bugfixes.

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

Secure Mail 21.10.0

Secure Mail für Android

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

Secure Mail 21.9.1

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 21.9.0

Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 21.8.5

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

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

Secure Mail 21.8.0

Secure Mail für iOS

E-Mail-basierte Autodiscovery von Exchange Server in Hybridumgebungen In Secure Mail für iOS können Sie Ihr Microsoft 365 Exchange-Konto mit Ihrer E-Mail-Adresse konfigurieren und dadurch ein reibungsloses Anmeldeerlebnis für Exchange-Hybridumgebungen gewährleisten. Dieses Feature steht auch für On-Premises-Exchange Server zur Verfügung.

> **Hinweis:**
>
> Stellen Sie sicher, dass Sie Autodiscovery für den Exchange Server aktivieren.

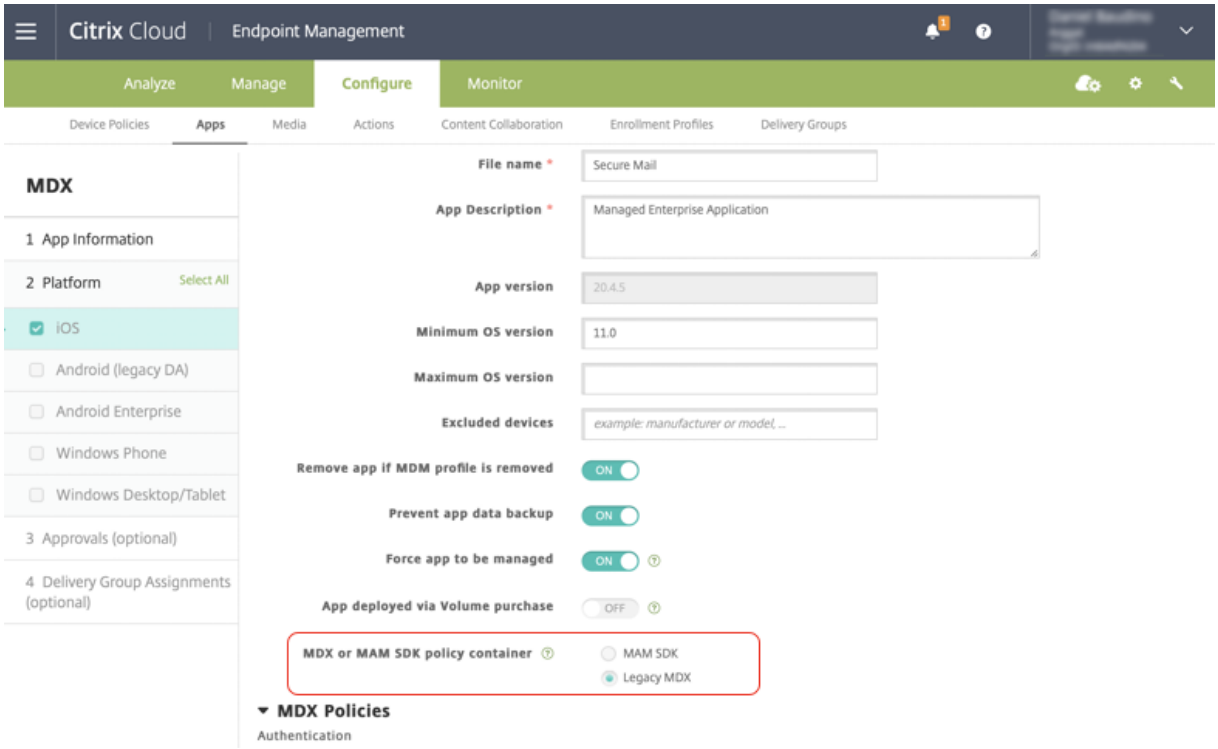
Pushbenachrichtigungen mit Rich-Media-Inhalt in Bereitstellungen mit moderner Authentifizierung mit Microsoft Office 365 Ab diesem Release unterstützt Secure Mail Pushbenachrichtigungen, wenn die Netzwerkzugriffsrichtlinie auf **Tunnel - Web-SSO** festgelegt ist und der Exchange Web Services (EWS)-Hostname in der **Ausschlussliste** enthalten ist. Sind EWS- und ActiveSync-Host identisch, müssen Sie sicherstellen, dass der ActiveSync-Host in der Richtlinie **Ausschlussliste** enthalten ist.

Dualmodus für Secure Mail Das MAM-SDK zur Mobilanwendungsverwaltung ersetzt Bereiche der MDX-Funktionalität, die von der iOS-Plattform nicht bereitgestellt werden. Die MDX-Technologie erreicht das Ende des Lebenszyklus (EOL) im Juli 2023.

Citrix Secure Mail wird mit dem MDX- und dem MAM-SDK-Framework veröffentlicht, um auf das für Juli 2023 geplante MDX-EOL vorzubereiten. Um die Verwaltung Ihrer Unternehmensanwendungen fortzusetzen, müssen Sie das MAM-SDK integrieren. Citrix empfiehlt den Wechsel zum **MAM-SDK**. Der Dualmodus soll den Übergang der Secure Mail-App zum neuen MAM-SDK-Modell ermöglichen.

Mit der Dualmodus-Funktion können Sie Apps entweder wie bisher mit MDX (jetzt **Legacy-MDX**) verwalten oder zum neuen **MAM-SDK** wechseln. Sie erhalten die folgenden Optionen für Richtlinieneinstellungen im **Richtliniencontainer für MDX oder MAM SDK**:

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



In der Richtlinie **Richtliniencontainer für MDX oder MAM SDK** können Sie Ihre Option von **Legacy-MDX** in **MAM-SDK** ändern.
Es wird empfohlen, nicht von **MAM-SDK** zu **Legacy-MDX** zu wechseln, da Sie beim Umstellen die App dann neu installieren müssen. Der Standardwert ist **Legacy-MDX**. Stellen Sie sicher, dass Sie für Secure Mail und Secure Web auf einem Gerät denselben Richtlinienmodus festlegen. Sie können nicht zwei verschiedene Modi auf demselben Gerät ausführen.

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

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

Voraussetzungen

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

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

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

Einschränkungen

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

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

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

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

Hinweis:

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

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

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

Secure Mail für Android

Dieses Release enthält Bugfixes.

Secure Mail 21.7.0

Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 21.6.0

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

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

Wenn Sie die Richtlinien für **Tunnel - Vollständiges VPN** oder **Tunnel - Vollständiges VPN und Web-SSO** verwenden, müssen Sie zur Richtlinie **Tunnel - Web-SSO** wechseln. Ihre E-Mails werden nicht synchronisiert, wenn Sie die veralteten Richtlinien weiterverwenden.

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

Secure Mail für Android Unterstützung für Selbstdiagnose mit der Option **Problembehandlung**. Mit diesem Feature können Sie überprüfen, ob die Grundeinstellungen, die für das korrekte Funktionieren der App entscheidend sind, als Standard festgelegt wurden oder nicht. Wenn Fehler in Bezug auf bestimmte Secure Mail-Einstellungen auftreten, verwenden Sie dieses Feature, um App-Probleme zu beheben.

Um auf dieses Feature zuzugreifen, öffnen Sie die App-Einstellungen und tippen Sie unter **Support** auf **Problembehandlung**. Die folgenden Menüoptionen werden angezeigt, die Sie überprüfen und bearbeiten können:

- Mail-Sync-Zeitraum
- Synchronisierungshäufigkeit - Posteingang
- E-Mails synchronisieren
- Fotos anzeigen
- Standard-Erinnerungszeit
- Kalender synchronisieren
- Kontakte synchronisieren

Um den Standardwert für eine Einstellung wiederherzustellen, tippen Sie auf **ÄNDERUNG ANWENDEN**. Um alle Einstellungen auf ihre Standardwerte zurückzusetzen, tippen Sie auf **ÄNDERUNGEN AUF ALLE ANWENDEN**.

Secure Mail 21.5.0

Ab dieser Version bietet Secure Mail Unterstützung für Exchange Server 2019 Kumulatives Update 9 und für Exchange Server 2016 Kumulatives Update 20.

Secure Mail für iOS

- **Erstellen von Microsoft Teams-Besprechungen in Secure Mail-Kalenderereignissen.** In Secure Mail für iOS können Sie Einladungen für Microsoft Teams-Besprechungen erstellen, während Sie Kalenderereignisse erstellen. Um eine Microsoft Teams-Besprechung zu erstellen, aktivieren Sie die Umschaltfläche **Microsoft Teams-Besprechung**. Der Link zur Besprechungseinladung und die Details werden automatisch mit den Ereignisdetails gesendet. Weitere Informationen finden Sie unter Erstellen von Microsoft Teams-Besprechungen in Secure Mail-Kalenderereignissen.

- Ab diesem Release sind die folgenden Richtlinienoptionen für die Richtlinie **Netzwerkzugriff** veraltet und werden ab Version 21.6.0 nicht mehr unterstützt:

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

  Wenn Sie die Richtlinien für **Tunnel - Vollständiges VPN** oder **Tunnel - Vollständiges VPN und Web-SSO** verwenden, müssen Sie zur Richtlinie **Tunnel - Web-SSO** wechseln. Ihre E-Mails werden nicht synchronisiert, wenn Sie die veralteten Richtlinien weiterverwenden.

  > **Hinweis:**
  >
  > Wenn Sie **Tunnel - Vollständiges VPN** verwenden und Secure Ticket Authority konfiguriert ist, wird die Anzeige für die moderne Authentifizierung nicht geladen.

Secure Mail für Android

- Ab diesem Release ist die Richtlinie **Erforderliches Upgrade deaktivieren** in der Citrix Endpoint Management-Konsole nicht mehr verfügbar. Ihre App wird automatisch auf die neueste im Play Store verfügbare Version aktualisiert.
- In Secure Mail für Android ist die Option **Feeds verwalten** ab diesem Release veraltet. Wenn dieses Feature derzeit aktiviert und konfiguriert ist, werden Feeds weiterhin basierend auf Ihren Einstellungen im Fenster **Feeds** angezeigt. Wenn Sie ein neuer Benutzer sind oder zuvor alle Feedkarten entfernt haben, sind die folgenden Standardfeedkarten verfügbar:

  - Ungelesen
  - Besprechungseinladungen
  - Anstehende Besprechungen
  - Von Ihrem Manager

Secure Mail 21.4.5

Secure Mail für Android **Autodiscovery auf E-Mail-Basis** In Secure Mail für Android können Sie Ihr Microsoft O365 Exchange-Konto mit Ihrer E-Mail-Adresse konfigurieren, wodurch ein reibungsloses Anmeldeerlebnis gewährleistet wird. Das Feature ist auch für On-Premises-Benutzer verfügbar, wenn Autodiscovery in der Hybridumgebung aktiviert ist

> **Hinweis:**
>
> Das Feature wird nur ab Exchange Server 2016 Cumulative Update 3 unterstützt.

Secure Mail 21.4.0

Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail 21.3.5

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 21.3.0

Secure Mail für iOS Das Bereitstellungsziel für Secure Mail iOS wurde in iOS 12.2 geändert. Das Microsoft Intune App SDK für iOS Version 14.1.3 erfordert, dass Ziel-Apps eine iOS-Bereitstellungsversion von mindestens iOS 12.2 haben. Das Bereitstellungsziel für Secure Mail wird auf iOS 12.2 aktualisiert, um diese Anforderung zu erfüllen.

Secure Mail für Android Erstellen von Microsoft Teams-Besprechungen in Secure Mail-Kalenderereignissen. In Secure Mail für Android können Sie Einladungen für Microsoft Teams-Besprechungen erstellen, während Sie Kalenderereignisse erstellen.
Um eine Microsoft Teams-Besprechung zu erstellen, aktivieren Sie die Umschaltfläche **Microsoft Teams-Besprechung**. Der Link zur Besprechungseinladung und die Details werden automatisch mit den Ereignisdetails gesendet. Weitere Informationen finden Sie unter Erstellen von Microsoft Teams-Besprechungen in Secure Mail-Kalenderereignissen.

Secure Mail 21.2.0

Ab dieser Version bietet Secure Mail Unterstützung für Exchange Server 2019 Kumulatives Update 8 und für Exchange Server 2016 Kumulatives Update 19.

Secure Mail für iOS

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

Secure Mail für Android

- **Überarbeitung der Farben für Secure Mail.** Secure Mail ist konform mit Citrix Branding-Farbaktualisierungen.
- **Unterstützung für Microsoft Intune** Secure Mail für Android unterstützt die neueste Version von Microsoft Intune 7.2.2.

- **Stabile Funktionsfähigkeit auf faltbaren Geräten.** Secure Mail für Android enthält Fixes, um ein stabiles Funktionieren auf faltbaren Geräten zu gewährleisten.

Secure Mail 21.1.5

Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail 21.1.0

Dieses Release enthält Bugfixes.

Secure Mail 20.12.0

Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail 20.11.0

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

Secure Mail 20.10.5

Secure Mail für iOS Dieses Release enthält Bugfixes.

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

Secure Mail 20.10.0

Ab dieser Version bietet Secure Mail Unterstützung für Exchange Server 2019 Kumulatives Update 7 und für Exchange Server 2016 Kumulatives Update 18.

Secure Mail für iOS **Teilnahme an Microsoft Teams-Besprechungen über Secure Mail.** In Secure Mail für iOS können Sie Microsoft Teams-Besprechungen direkt über eine Einladung im Kalender beitreten. Ist die Microsoft Teams-App installiert, wird die App geöffnet und Sie nehmen an der Besprechung teil. Ist die App nicht installiert, wird eine Option zum Download von Microsoft Teams aus dem App Store angezeigt. Bei Besprechungen im Format `https://teams.microsoft.com/l/meetup-join/meetinglink` wird die App geöffnet und Sie nehmen direkt an der Besprechung teil.

> **Hinweis:**
>
> Ihr Administrator muss hierfür in die Richtlinie "Zulässige URLs"`+^msteams:` einfügen. Weitere Informationen finden Sie unter App-Interaktion (ausgehende URL).

Secure Mail für Android

- **Teilnahme an Microsoft Teams-Besprechungen über Secure Mail.** In Secure Mail für Android können Sie Microsoft Teams-Besprechungen direkt über eine Einladung im Kalender beitreten. Ist die Microsoft Teams-App installiert, wird die App geöffnet und Sie nehmen an der Besprechung teil. Ist die App nicht installiert, wird eine Option zum Download von Microsoft Teams aus Google Play angezeigt. Bei Besprechungen im Format `https://teams.microsoft.com/l/meetup-join/>meetinglink` wird die App geöffnet und Sie nehmen direkt an der Besprechung teil.

  > **Hinweis:**
  >
  > Ihr Administrator muss hierfür in die Richtlinie "Ausnahmeliste für eingeschränktes Öffnen"`{ action=android.intent.action.VIEW scheme=msteams package=com.microsoft.teams }` einfügen. Weitere Informationen finden Sie unter Interaktion von Apps.

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

Secure Mail 20.9.5

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 20.9.0

Unterstützung für Azure Government Cloud Computing Secure Mail für iOS und Android unterstützt Government Cloud Computing (GCC) High, das moderne Authentifizierung (OAuth) auf dem Azure Active Directory-Mandanten bietet. Secure Mail ist als Endpunkt auf dem GCC High registriert,

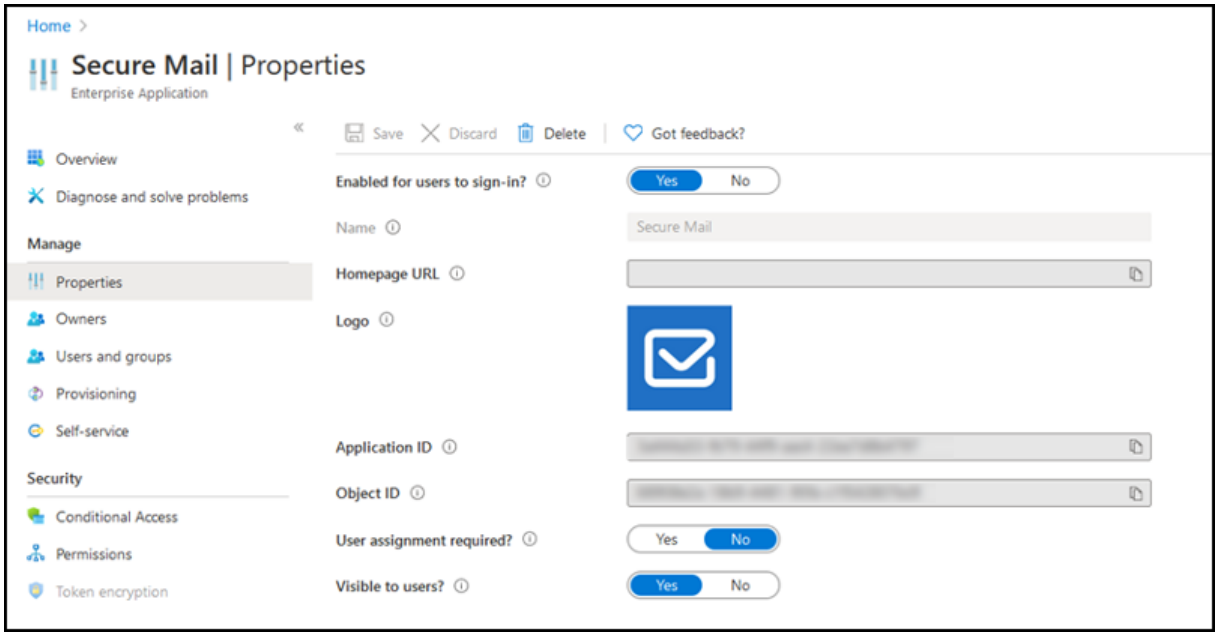
um die obligatorische Anforderung von Microsoft für den gesamten GCC High Service zu erfüllen. Weitere Informationen finden Sie unter Neuerungen bei Azure Active Directory in Microsoft 365 Government.

Sie werden nun zur Authentifizierung an GCC High auf dem Azure Active Directory-Mandanten weitergeleitet. Der Administrator muss Berechtigungen für Secure Mail auf dem Azure Active Directory-Mandanten zulassen.

Voraussetzungen Stellen Sie sicher, dass der globale Administrator von Azure Active Directory folgende Schritte ausführt:

- Download der aktuellen Version von Secure Mail auf Ihr Gerät.
- Konfigurieren Ihres Exchange-Kontos in der Secure Mail-App und Zulassen der App-Berechtigung in Azure Active Directory für alle Benutzer, die sich anmelden. Sie sehen den folgenden Bildschirm.

> **Hinweis:**
>
> Diese Schritte sind von globalen Administratoren auszuführen und nur einmal erforderlich. Sobald der App der Zugriff gewährt wurde, können Sie einfach ein Upgrade über den App Store ausführen.



Nach dem Upgrade Nach einem Upgrade erhalten Sie ein Aufforderung zur Neuautorisierung nachdem der Aktualisierungstoken abgelaufen ist und werden zu GCC High in Azure Active Directory umgeleitet. Überprüfen Sie den vorherigen Workflow, um sicherzustellen, dass die Autorisierungsanforderung an GCC High in Azure Active Directory gesendet wird.

Es gibt zwei Möglichkeiten zur Überprüfung des Workflows:

- Secure Mail mit dem App-Namen **Secure Mail-GCC High** wird auf der Anmeldeseite im Azure Active Directory-Mandanten angezeigt.
- Überprüfen Sie in den Secure Mail-Protokollen, ob die Weiterleitungen nach der Neuauthentifizierung über https://login.microsoftonline.us erfolgen.

Secure Mail 20.8.5

Secure Mail für Android Secure Mail für Android unterstützt Android 11.

Secure Mail 20.8.0

Ab dieser Version bietet Secure Mail Unterstützung für Exchange Server 2019 Kumulatives Update 6 und für Exchange Server 2016 Kumulatives Update 17.

Secure Mail für Android **Dualmodus für Secure Mail.** Das MAM-SDK zur Mobilanwendungsverwaltung ersetzt Bereiche der MDX-Funktionalität, die von den iOS- und Android-Plattformen nicht bereitgestellt werden. Die MDX-Technologie erreicht das Ende des Lebenszyklus (EOL) im März 2022. Um die Verwaltung Ihrer Unternehmensanwendungen fortzusetzen, müssen Sie das MAM-SDK integrieren.

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

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

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

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

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

- Aktualisieren Sie Citrix Endpoint Management auf die Versionen 10.12 RP2 und höher oder 10.11 RP5 und höher.
- Aktualisieren Sie Ihre mobilen Apps auf die Version 20.8.0 oder höher.

- Aktualisieren Sie die Richtliniendatei auf Version 20.8.0 oder höher.
- Wenn Ihre Organisation Drittanbieter-Apps verwendet, müssen Sie das MAM-SDK in diese Drittanbieter-Apps integrieren, bevor Sie zum MAM-SDK für Ihre mobilen Produktivitätsapps von Citrix wechseln. Alle verwalteten Apps müssen gleichzeitig in das MAM-SDK verschoben werden.

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

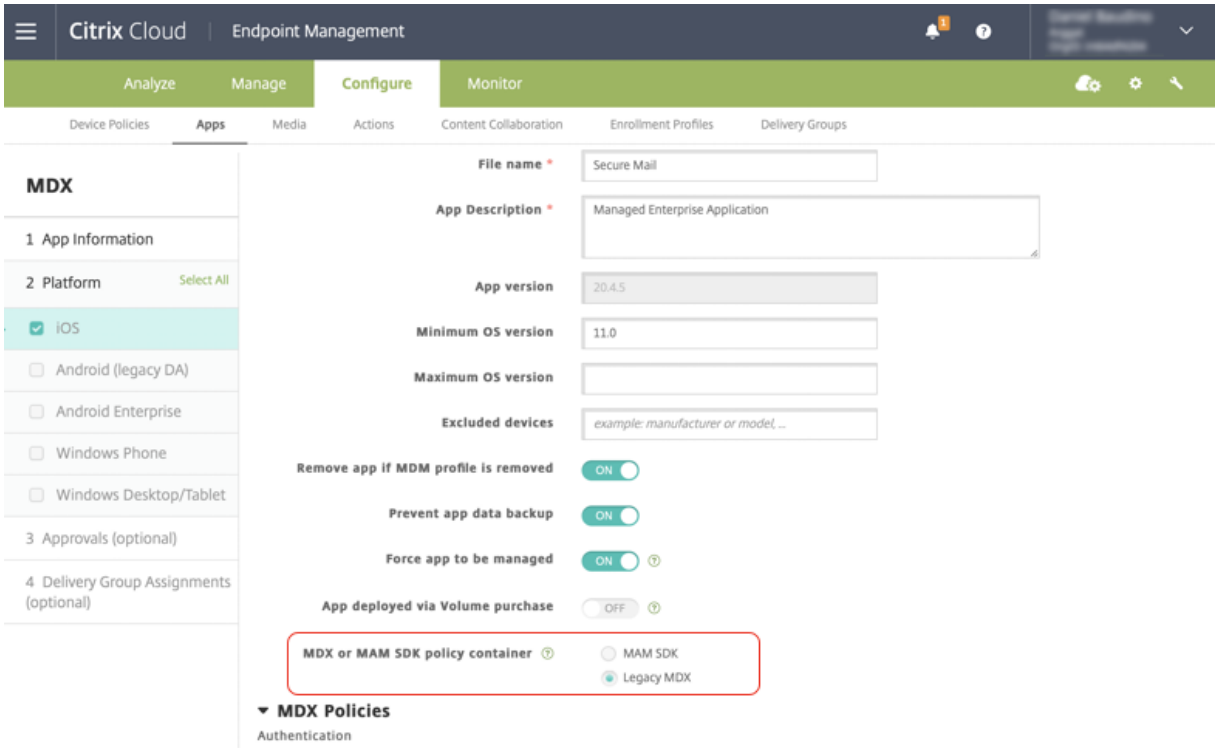
Einschränkungen

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

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

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

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



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

Secure Mail für iOS Synchronisierungsoptimierung für Postfach. In Secure Mail für iOS wurde die **Postfachsynchronisierung** optimiert, um die Benutzererfahrung zu verbessern. Der **Kalender** und die **Kontakte** werden schneller synchronisiert. E-Mails, die älter als 3 Wochen sind, werden abgeschnitten, um die Synchronisierungszeit zu verkürzen. Sie können die vollständige E-Mail anzeigen, wenn Sie sie öffnen.

Secure Mail 20.7.5

> **Hinweis:**
>
> Die Unterstützung für Android 6.x wurde am 30. Juni 2020 eingestellt.

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

Secure Mail 20.7.0

Dieses Release enthält Bugfixes.

Secure Mail 20.6.5

Dieses Release enthält Bugfixes.

Secure Mail 20.6.0

Dieses Release enthält Bugfixes.

Secure Mail 20.5.0

Dieses Release enthält Bugfixes.

Secure Mail 20.4.5

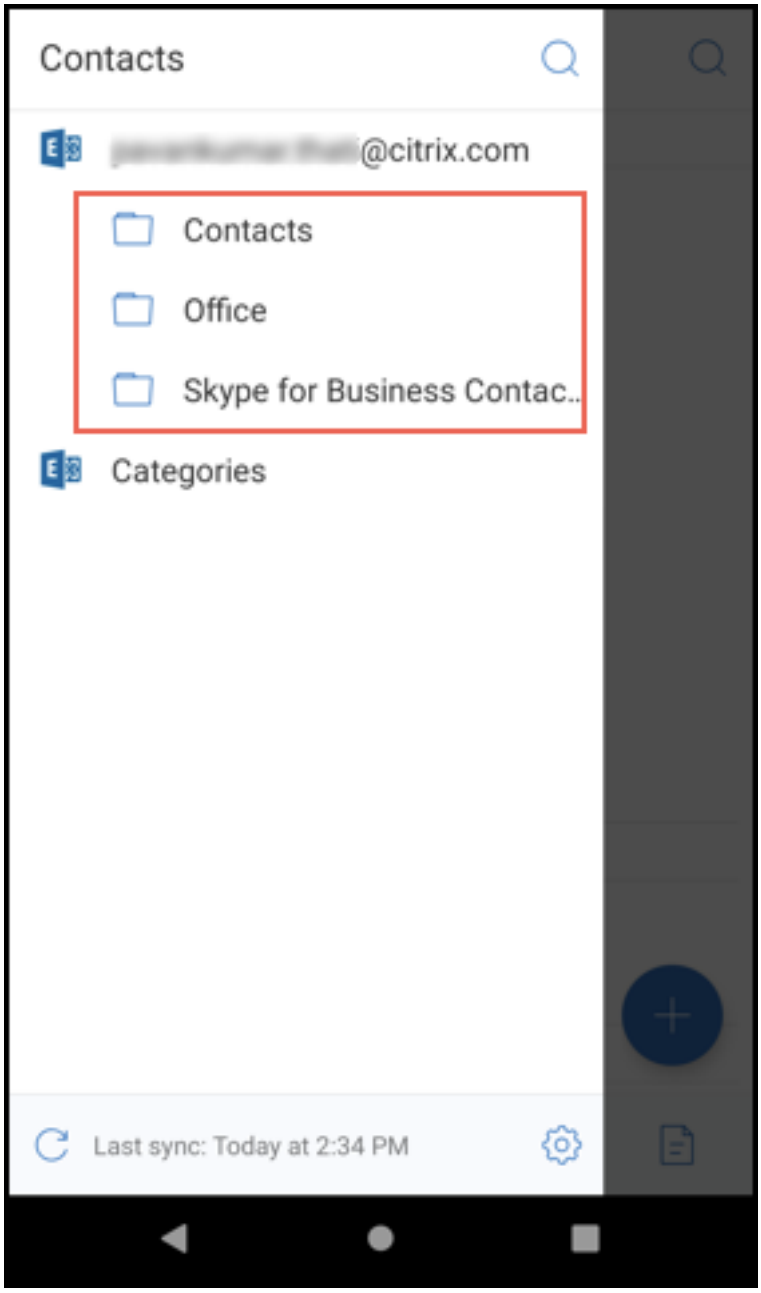
Secure Mail für Android Ab dieser Version bietet Secure Mail Unterstützung für Exchange Server 2019 Kumulatives Update 5 und für Exchange Server 2016 Kumulatives Update 16.

Secure Mail 20.4.0

Ab dieser Version bietet Secure Mail Unterstützung für Exchange Server 2016 Kumulatives Update 15 und für Exchange Server 2013 Kumulatives Update 23.

Secure Mail 20.3.0

Secure Mail für Android **Ordner unter "Kontakte"erstellen.** In Secure Mail für Android können Sie Ordner unter **Kontakte** für Ihr E-Mail-Konto hinzufügen, bearbeiten und löschen.



Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail 20.2.0

Secure Mail für Android

Entwürfe minimieren

In Secure Mail für Android können Sie einen Entwurf minimieren, während Sie eine E-Mail erstellen und innerhalb der App navigieren. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter E-Mail-Entwurf minimieren.

Secure Mail 20.1.5

Secure Mail für iOS Ab dieser Version enthält Secure Mail Unterstützung für Exchange Server 2019 Cumulative Update 4.

Secure Mail für Android

- **2-Wege-Kontaktsynchronisierung** In Secure Mail für Android können Sie Secure Mail-Kontakte aus Ihrer lokalen Kontaktliste erstellen, bearbeiten und löschen.
- **Unterstützung für ICS-Dateien.** In Secure Mail für Android können Sie angehängte ICS-Dateien anzeigen und als Ereignis in Ihren Kalender importieren.
- Ab dieser Version enthält Secure Mail Unterstützung für Exchange Server 2019 Cumulative Update 4.

Secure Mail 20.1.0

Ab dieser Version enthält Secure Mail Unterstützung für Exchange Server 2016 Cumulative Update 14.

Secure Mail 19.12.5

Secure Mail für iOS Dieses Release enthält Bugfixes.

Secure Mail für Android **Senden von E-Mails rückgängig machen.** In Secure Mail für Android können Sie das Senden von E-Mail rückgängig machen. Sobald Sie auf die Schaltfläche **Senden** tippen, erhalten Sie eine Popupmeldung, mit der Sie das Senden rückgängig machen können. Tippen Sie auf **Rückgängig**, um das Senden rückgängig zu machen, die E-Mail oder die E-Mail-Empfänger zu bearbeiten, Anlagen anzuhängen oder zu entfernen oder die E-Mail zu verwerfen.

Anlagen im Ordner "Entwürfe"werden synchronisiert. Wenn der Ordner **Entwürfe** in Secure Mail für Android synchronisiert wird, werden die Anlagen auch synchronisiert und sind auf allen Geräten verfügbar. Dieses Feature ist für Geräte verfügbar, in denen Exchange ActiveSync Version 16 oder höher ausgeführt wird.

Secure Mail 19.11.5

Secure Mail für iOS **Kontaktbild in Secure Mail.** Zeigen Sie in Secure Mail für iOS ein Bild des Kontakts an, wenn Sie Empfänger in E-Mails oder Besprechungseinladungen hinzufügen. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Bilder Ihrer Kontakte anzeigen.

Secure Mail für Android **In-App-Ansicht von PDF-Dateien.** In Secure Mail für Android können Sie PDF-Dateien in der App anzeigen, auch Lesezeichen und Anmerkungen. Ebenfalls verfügbar ist die erweiterte Ansicht anderer Microsoft Office-Anlagen.

Secure Mail für iOS 19.10.6

Dieses Release enthält Bugfixes.

Secure Mail 19.10.5

Secure Mail für iOS **Entwürfe minimieren.** In Secure Mail für iOS können Sie einen Entwurf minimieren, während Sie eine E-Mail erstellen, und innerhalb der App navigieren. Diese Funktion ist auf Geräten mit iOS 13 und höher verfügbar. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter E-Mail-Entwurf minimieren.

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 19.10.0

Verwenden Sie die Richtlinie für Office 365 Exchange Server, um die Office 365-Serveradresse zu definieren. In Secure Mail iOS und Android wurde im Abschnitt **OAuth-Unterstützung für Office 365** die Richtlinie **Office 365 Exchange Server** hinzugefügt. Mit dieser Richtlinie können Sie in Cloud den Hostnamen für das Office 365-Postfach definieren. Die Richtlinie unterstützt auch Office 365 für Behörden. Der Hostname ist ein einzelner Wert, z. B. *outlook.office365.com*. Der Standardwert ist *outlook.office365.com*.

Secure Mail iOS und Android unterstützen die Verschlüsselungsverwaltung. Mit der Verschlüsselungsverwaltung können Sie moderne Geräteplattformsicherheit nutzen und gleichzeitig sicherstellen, dass das Gerät in einem ausreichenden Zustand bleibt, um die Plattformsicherheit effektiv zu nutzen. Durch die Verschlüsselungsverwaltung eliminieren Sie die Redundanz der lokalen Datenverschlüsselung, da die Dateisystemverschlüsselung von der iOS- oder Android-Plattform bereitgestellt wird. Um dieses Feature zu aktivieren, müssen Administratoren in der Citrix Endpoint

Management-Konsole die MDX-Richtlinie **Verschlüsselungstyp** auf **Plattformverschlüsselung mit Durchsetzen der Compliance** festlegen.

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

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

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

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

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

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

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

- iOS 10: Die Betriebssystemversion der App ist größer oder gleich der angegebenen Version.
- Debuggerzugriff: Debugging ist für die App nicht aktiviert.
- Gerät mit Jailbreak: Auf Geräten mit Jailbreak wird die App nicht ausgeführt.
- Gerätepasscode: Der Gerätepasscode ist **aktiviert**.
- Datenfreigabe: Die Datenfreigabe ist für die App nicht aktiviert.

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

- Android SDK 24 (Android 7 Nougat) - Die App führt eine Betriebssystemversion aus, die größer oder gleich der angegebenen Version ist.

- Debuggerzugriff: Debugging ist für die App nicht aktiviert.
- Gerät mit Rooting: Auf Geräten mit Rooting wird die App nicht ausgeführt.
- Gerätesperre: Der Gerätepasscode ist **aktiviert**.
- Gerät verschlüsselt: App wird auf einem verschlüsselten Gerät ausgeführt.

Secure Mail 19.9.5

Secure Mail für iOS **Unterstützung für ICS-Dateien.** In Secure Mail für iOS können Sie angehängte ICS-Dateien als Ereignis in Ihren Kalender importieren.

Secure Mail für Android Dieses Release enthält Bugfixes.

Secure Mail 19.9.0

Ab diesem Release unterstützt Secure Mail die folgenden Server:

- Exchange Server 2016 Kumulatives Update 13
- IBM Lotus Notes Traveler Version 10.0.1.0 Build 201811191126_20
- IBM Domino Mail Server Version 10.0.1

Secure Mail für iOS

- Secure Mail für iOS unterstützt iOS 13.
- **Melden von Phishing-E-Mail mit MIME-Kopfzeile:** Wenn ein Benutzer in Secure Mail für iOS eine Phishing-E-Mail meldet, wird zu der E-Mail eine EML-Datei als Anlange erstellt. Der Empfänger der E-Mail kann die MIME-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. Weitere Informationen finden Sie unter Melden von Phishing-E-Mail (als Anlage).
- **Unterstützung für dynamische E-Mails.** Secure Mail für iOS wurde optimiert, um dynamische E-Mails zu liefern. Bisher wurden E-Mail-Inhalte mit großen Tabellen oder Bildern falsch gerendert. Dieses Feature biete E-Mail-Inhalte, die auf allen unterstützten Geräten unabhängig von E-Mail-Format und Größe besser lesbar sind.
- **Drag & Drop für Kalendereereignisse** In Secure Mail für iOS können Sie die Zeit eines vorhandenen Kalendereereignisses durch Drag & Drop ändern. Ziehen Sie das Ereignis auf die gewünschte Zeit am Tag der Besprechung oder an einem anderen Tag.
- **Autom. weiterleiten** Wenn Sie in Secure Mail für iOS eine Nachricht in den **Unterhaltungen** löschen, können Sie auswählen, zu welcher Nachricht Sie zurückkehren. Um diese Funktion

zu verwenden, navigieren Sie zu **Einstellungen > Autom. weiterleiten**. Wählen Sie dann die gewünschte Option aus. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter E-Mail in Unterhaltung löschen und automatisch andere E-Mail anzeigen.

- **Unterstützung für WkWebView.** Secure Mail für iOS unterstützt WkWebView. Dieses Feature verbessert die Art und Weise, wie Secure Mail-Emails und Kalenderereignisse auf Ihrem Gerät gerendert werden.

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

Secure Mail für Android 19.8.5

Dieses Release enthält Bugfixes.

Secure Mail 19.8.0

Secure Mail für iOS Dieses Release enthält Leistungsverbesserungen und Bugfixes.

Secure Mail für Android

- Unterstützung für Android Q.
- **Unterstützung für 64-Bit-Apps für Google Play.** Secure Mail für Android unterstützt 64-Bit-Architekturen.
- **Verbesserungen an der UI für das Aktualisieren durch Ziehen in Secure Mail für Android. In Übereinstimmung mit den Material Design-Richtlinien haben wir kleinere Verbesserungen am Aktualisieren durch Ziehen gemacht.** Der Synchronisierungszeitstempel ist unten auf dem Bildschirm verfügbar, wenn Sie auf das Hamburgersymbol tippen.

Secure Mail 19.7.5

Secure Mail für iOS

- **Automatische Synchronisierung des Ordners "Entwürfe"**. In Secure Mail für iOS wird der Ordner "Entwürfe"automatisch synchronisiert, sodass Ihre Entwürfe auf allen Geräten verfügbar sind. Dieses Feature ist für Bereitstellungen verfügbar, in denen Exchange ActiveSync v16 oder höher ausgeführt wird. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Automatische Synchronisierung des Ordners "Entwürfe".

- **Secure Mail für iOS unterstützt Single Sign-On, wenn Sie Microsoft Intune im MDM + MAM-Modus verwenden.** Um diese Feature zu verwenden, muss die Microsoft Authenticator-App auf Ihrem Gerät installiert sein. Weitere Informationen zum Installieren der Microsoft Authenticator-App finden Sie unter **Download and install the Microsoft Authenticator app** in *docs.microsoft.com*.

Secure Mail für Android

> Hinweis:
>
> Citrix empfiehlt ein Upgrade auf Secure Mail Version 19.7.5, bevor Sie Ihr Betriebssystem auf Android Q aktualisieren.

- **Web SSO für Tunneling-Richtlinie für Umgebungen verwenden, die moderne Authentifizierung mit Microsoft Office 365 ausführen.** In Secure Mail für Android wird eine neue Richtlinie **Web-SSO zum Tunneln verwenden** eingeführt. Mit dieser Richtlinie können Sie OAuth-Datenverkehr über Web-SSO tunneln. Vorgehensweise:
  - Legen Sie Richtlinie **Web-SSO zum Tunneln verwenden** auf **Ein** fest.
  - Wählen Sie die Option **Tunnel - Web-SSO** für die Netzwerkzugriffsrichtlinie.
  - Schließen Sie alle Hostnamen, die mit OAuth in Verbindung stehen, von der Richtlinie für **Hintergrunddienste** aus.
- **Secure Mail für Android unterstützt Single Sign-On, wenn Sie Microsoft Intune im MDM + MAM-Modus verwenden.** Um diese Feature zu verwenden, muss das Intune-Unternehmensportal auf Ihrem Gerät installiert sein. Sobald Sie sich am Intune-Unternehmensportal angemeldet haben, können Sie SSO im MDM + MAM-Modus verwenden, ohne sich mit Ihren Anmeldeinformationen in Secure Mail neu authentifizieren zu müssen.

Secure Mail 19.6.5

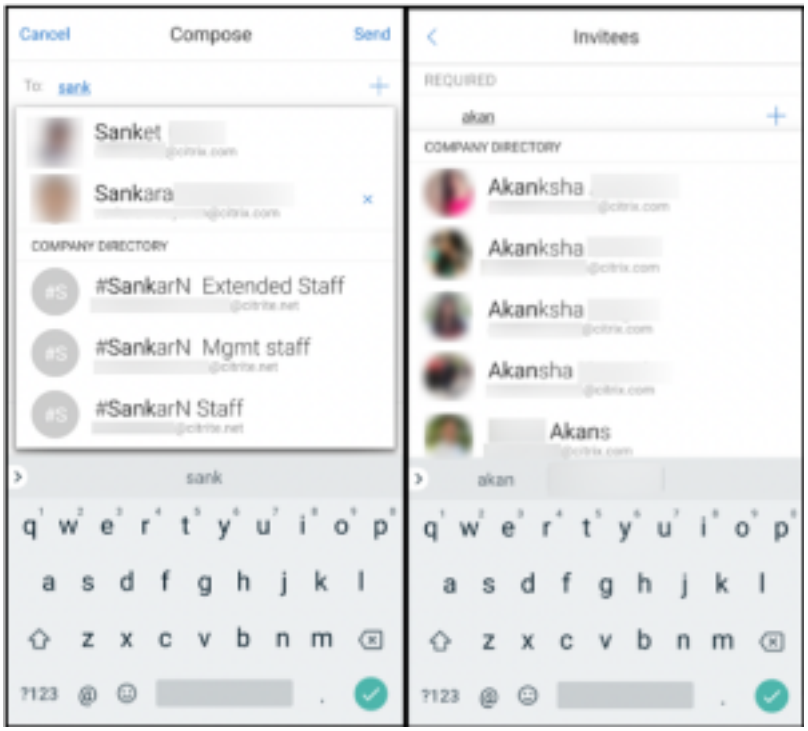
Secure Mail für iOS Secure Mail für iOS Version 19.6.5 enthält Leistungsverbesserungen und Fehlerbehebungen. Informationen zu behobenen und bekannten Probleme finden Sie unter Bekannte und behobene Probleme.

Secure Mail für Android

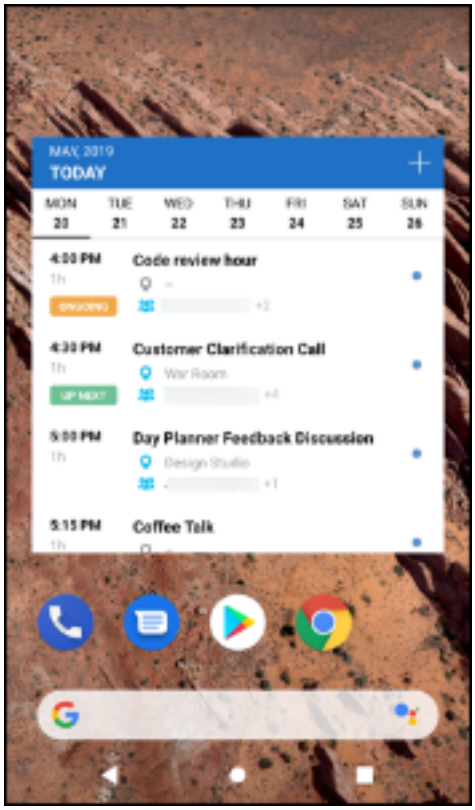
- **Drag & Drop für Kalendererereignisse** In Secure Mail für Android können Sie die Zeit eines vorhandenen Kalendererereignisses durch Drag & Drop ändern. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Kalendererereigniszeit ändern.
- **Unterstützung für dynamische E-Mails.** Secure Mail für Android wurde optimiert, um dynamische E-Mails zu liefern. Bisher wurden E-Mail-Inhalte mit großen Tabellen oder

Bildern falsch gerendert. Dieses Feature biete E-Mail-Inhalte, die besser lesbar sind, auf allen unterstützten Geräten unabhängig von dem E-Mail-Format und der Größe.

- **Kontaktbild in Secure Mail.** Zeigen Sie in Secure Mail für Android das Bild des Kontakts an, wenn Sie Empfänger in E-Mails oder Besprechungseinladungen hinzufügen. Das Bild des Kontakts wird neben dem Namen angezeigt. Bei mehreren Personen mit demselben Namen hilft das Bild, den korrekten Empfänger zu identifizieren, wenn Sie Empfänger E-Mails oder Besprechungseinladungen hinzufügen. Um nach Kontakten zu suchen, die nicht lokal gespeichert sind, geben Sie mindestens vier Zeichen des Empfängernamens ein, um das Bild anzuzeigen.



- **Widget für Kalenderagenda.** In Secure Mail für Android ist die **Kalenderagenda** als Widget verfügbar. Von diesem Widget können Sie die bevorstehenden Ereignisse im **Kalender** für eine Woche anzeigen. Mit diesem Feature können Sie ein **Kalendererereignis** erstellen, ein vorhandenes Ereignis anzeigen und die Details bearbeiten. Die Richtlinie **Screenshot blockieren** gilt nicht für das auf dem Startbildschirm platzierte Widget. Sie können das Widget jedoch mit der Richtlinie **Kalenderwidget zulassen** deaktivieren.



Secure Mail 19.5.5

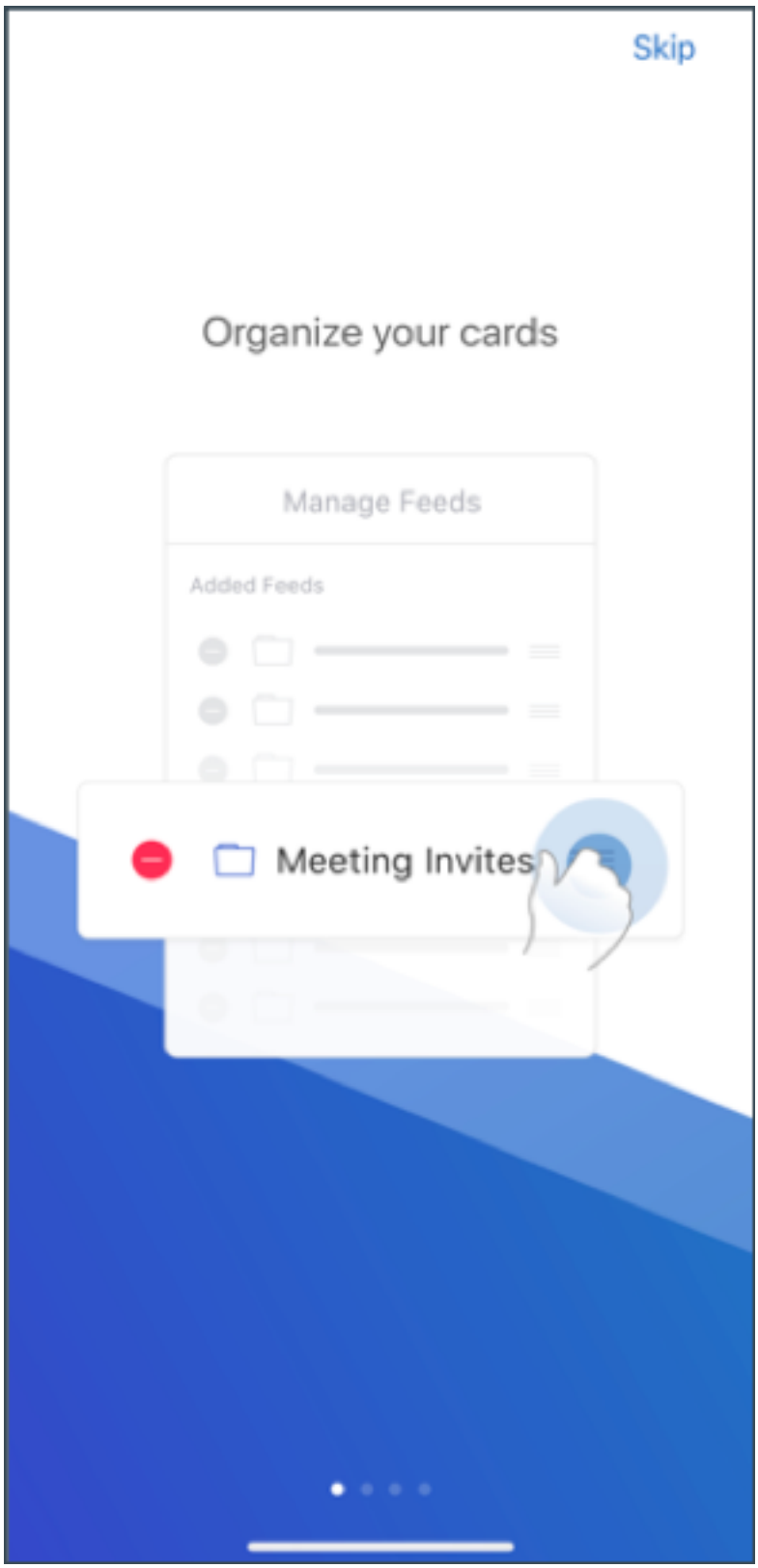
Secure Mail für Android Secure Mail für Android Version 19.5.5 enthält Leistungsverbesserungen und Fehlerbehebungen. Informationen zu behobenen und bekannten Probleme finden Sie unter Bekannte und behobene Probleme.

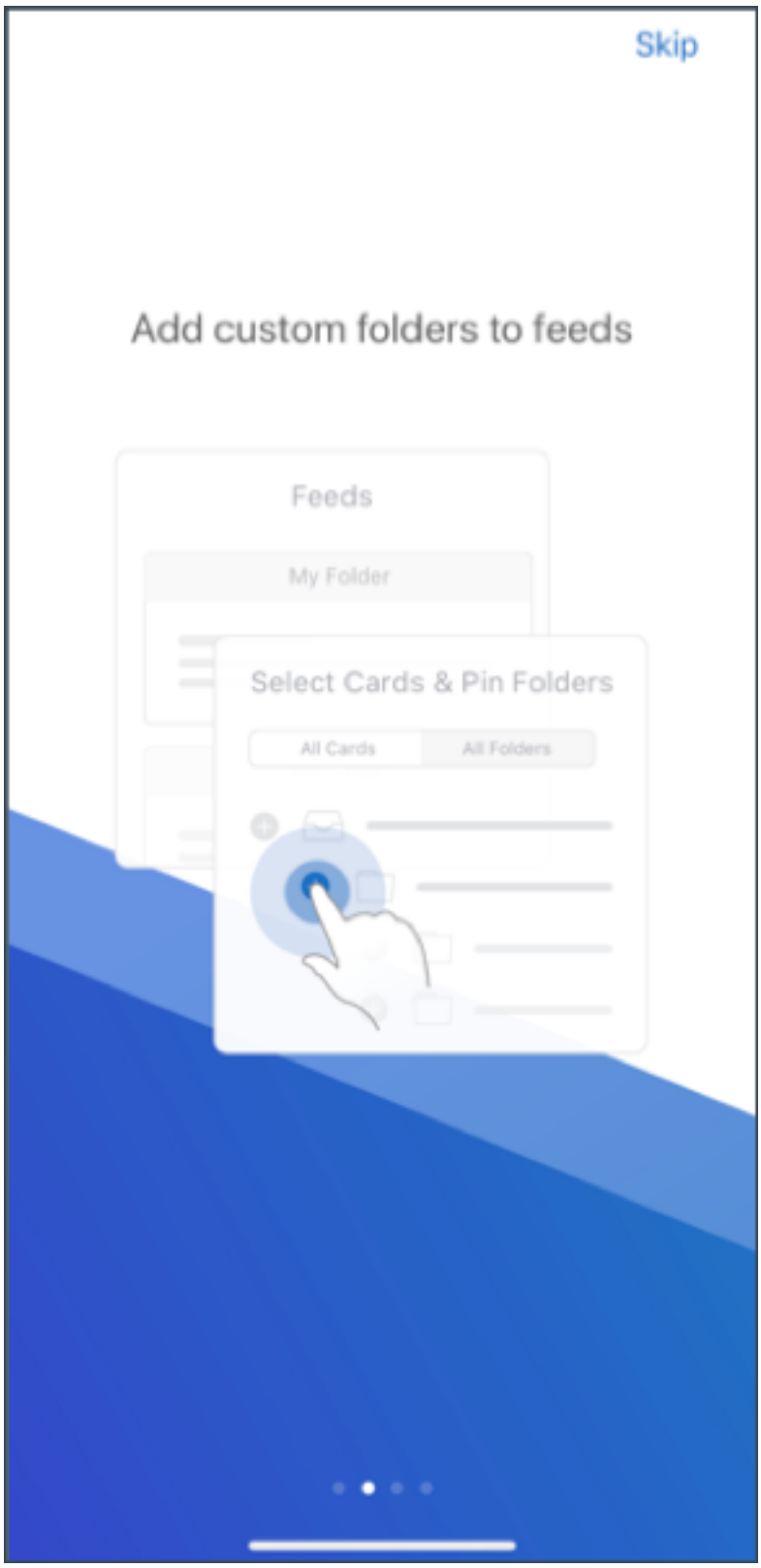
Secure Mail für iOS

- Secure Mail für iOS unterstützt Single Sign-On, wenn Sie Microsoft Intune im MDM + MAM-Modus verwenden. Um diese Feature zu verwenden, muss die Microsoft Authenticator-App auf Ihrem Gerät installiert sein. Die Microsoft Authenticator-App ist in App-Stores verfügbar.
- **Support für Slack EMM:** Slack EMM ist für Slack-Kunden mit aktiviertem Enterprise Mobility Management (EMM). Secure Mail für iOS unterstützt die Anwendung **Slack EMM**, mit der Administratoren die Integration von Secure Mail in die **Slack-App** oder die **Slack EMM-App** wählen können.

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 Feeds verwalten.

Automatische Synchronisierung des Ordners "Entwürfe". In Secure Mail für Android wird der Ordner "Entwürfe" automatisch synchronisiert, sodass Ihre Entwürfe auf allen Geräten verfügbar sind. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Automatische Synchronisierung des Ordners "Entwürfe".

Secure Mail für Android 19.4.6, 19.4.5 und 19.3.5

Diese Releases enthalten Leistungsverbesserungen und Bugfixes.

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

Secure Mail 19.3.0

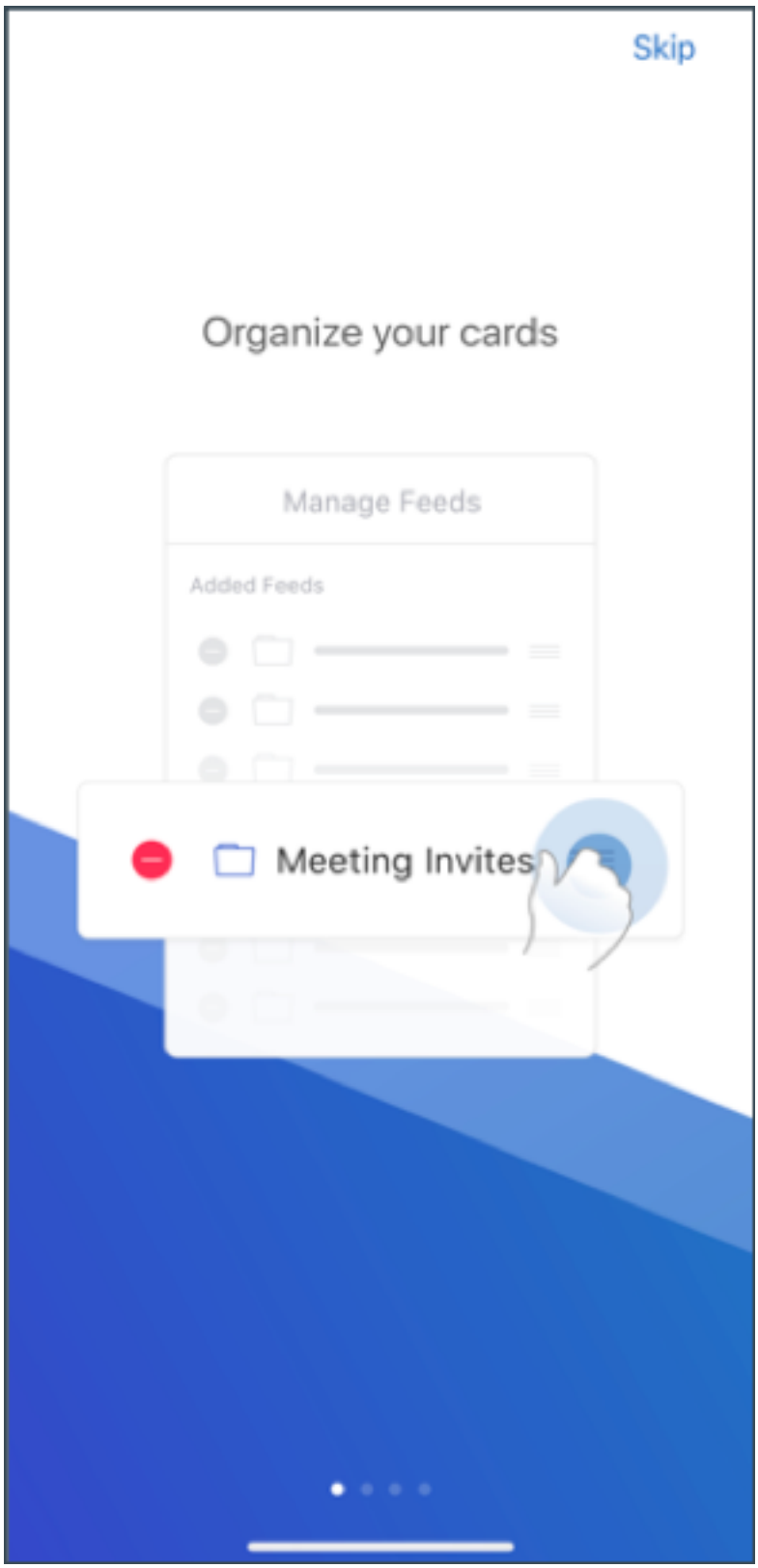
Ab diesem Release unterstützt Secure Mail die folgenden Server:

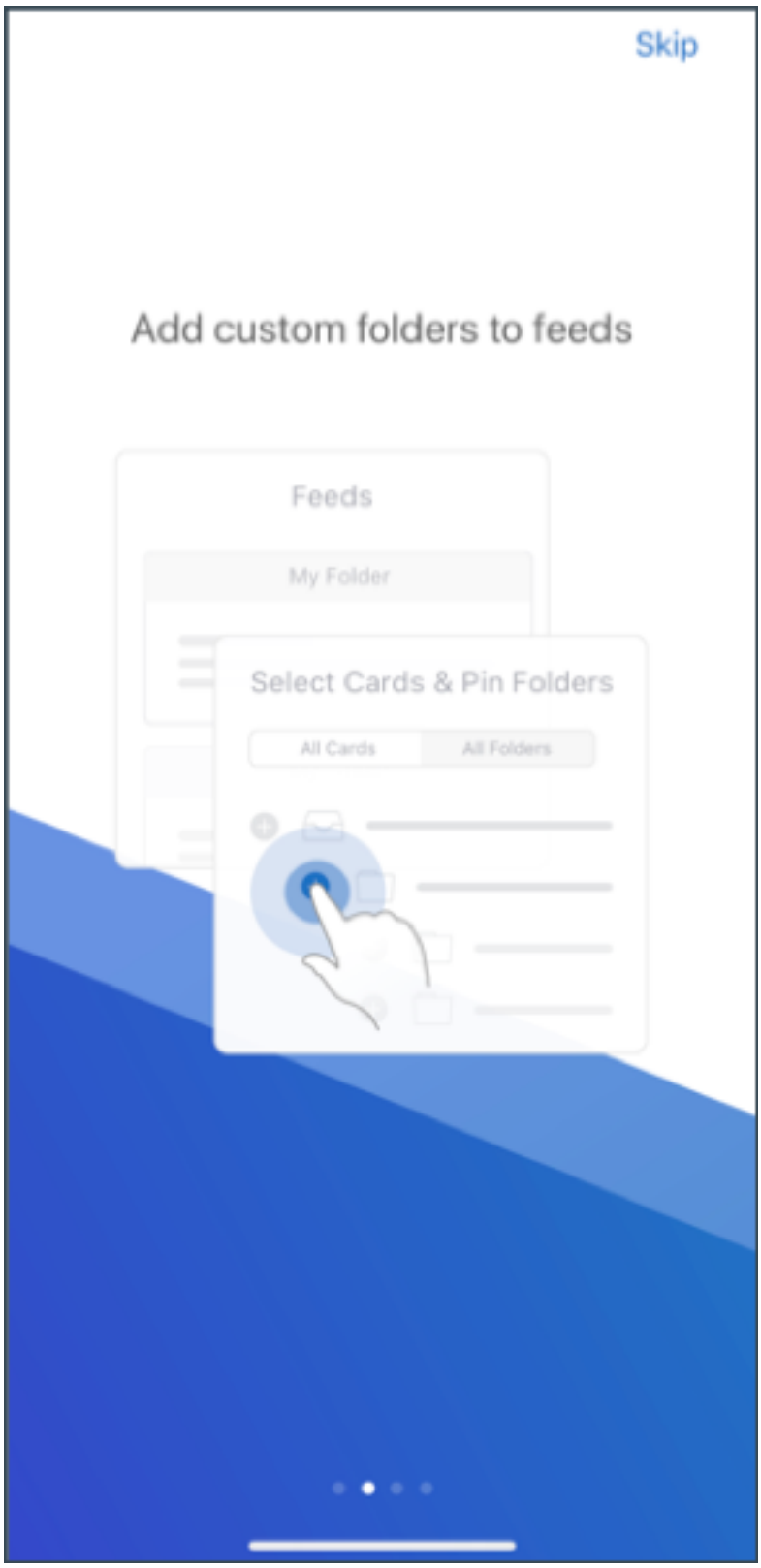
- Exchange Server 2019 Cumulative Update 1
- Exchange Server 2016 Cumulative Update 12
- Exchange Server 2013 Cumulative Update 22
- Exchange Server 2010 SP3 Update Rollup 26

Weitere Informationen und die vollständige Liste der kompatiblen Server 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.

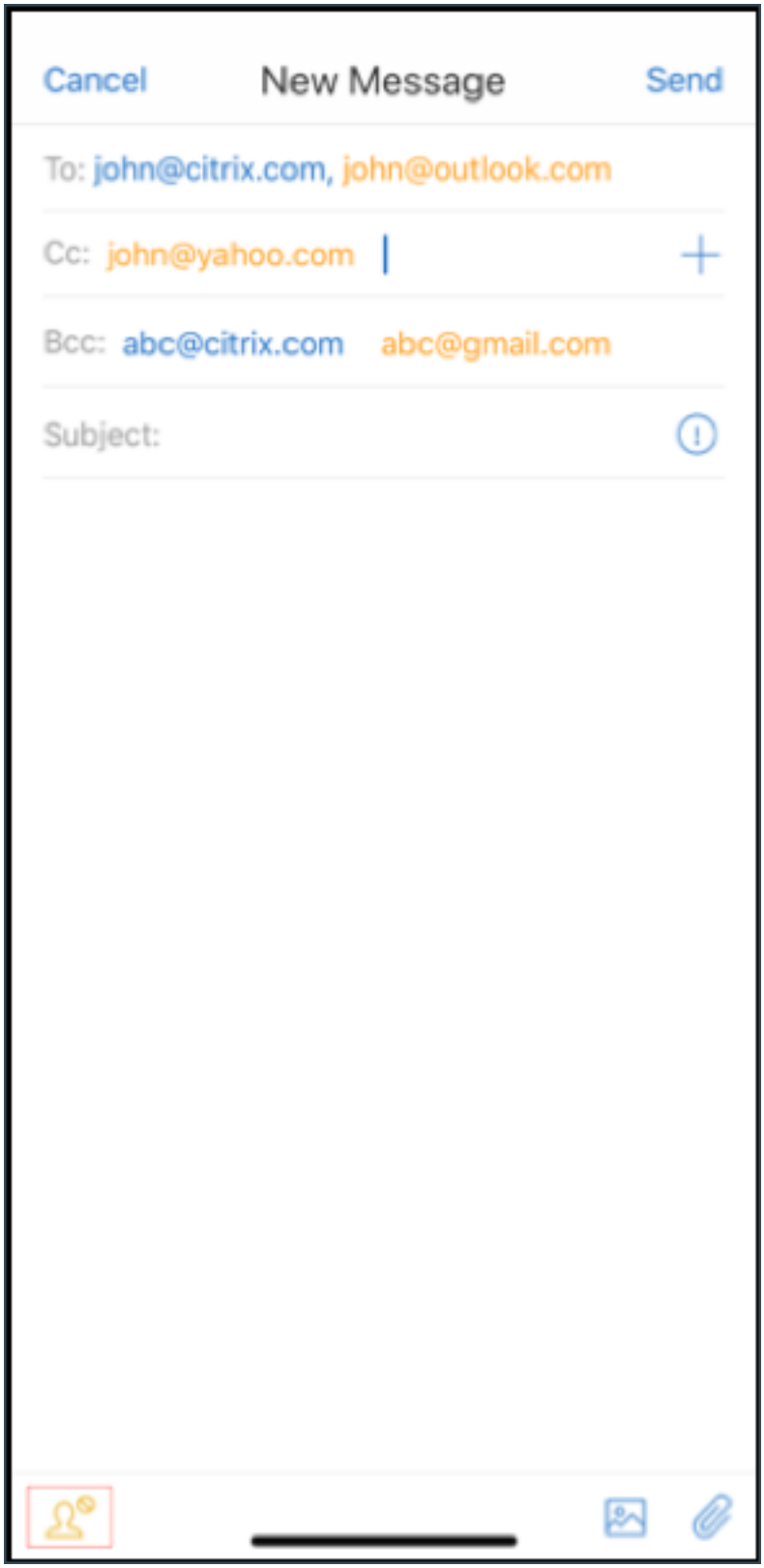




Weitere Informationen zum Verwalten Ihrer Feeds finden Sie unter Feeds verwalten.

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.

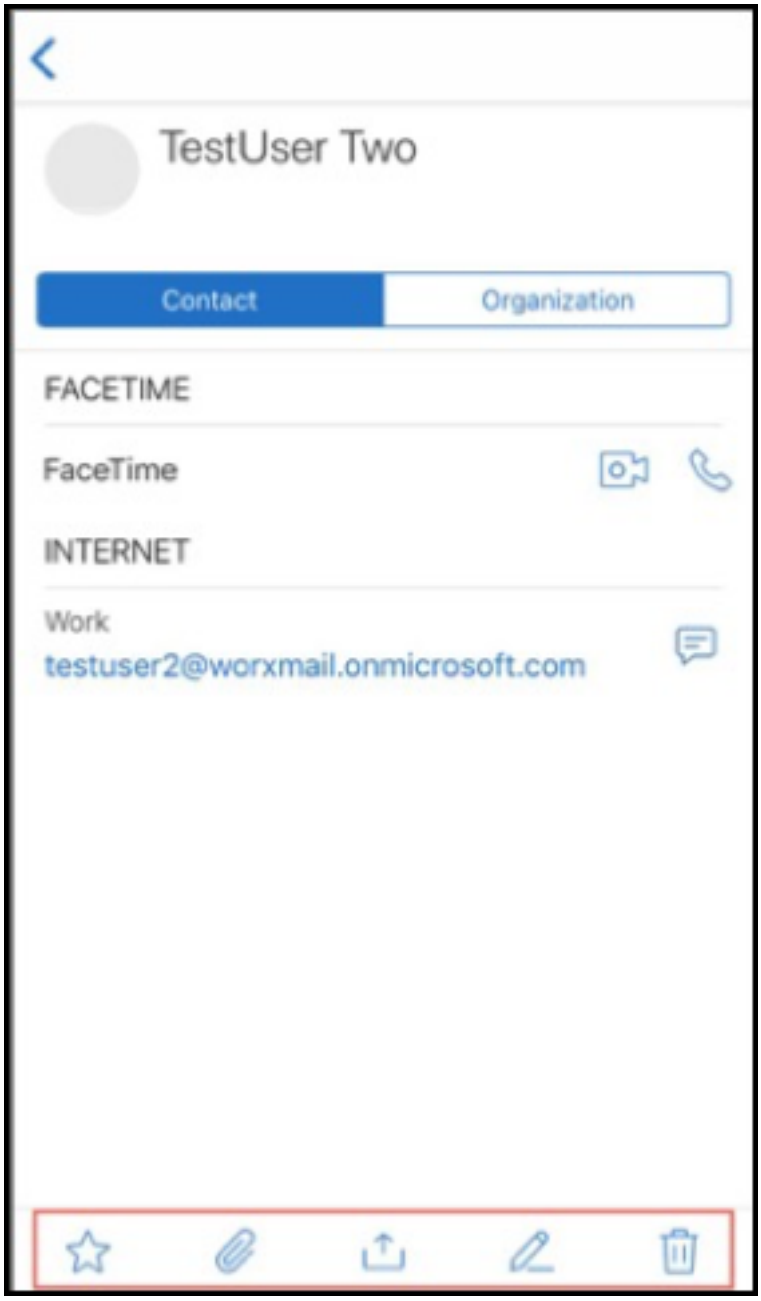
Wenn Sie eine E-Mail erstellen, beantworten oder weiterleiten, werden externe Empfänger in der Adressenliste markiert. Ein **Kontakte**-Warnsymbol wird links unten auf dem Bildschirm angezeigt. Tippen Sie auf das Symbol **Kontakte**, um die Adressenliste zu ändern.



Weitere Informationen 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 Dieses Release enthält Leistungsverbesserungen und Bugfixes.

Informationen zu behobenen und bekannten Probleme 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**
  - **Share**
  - **Löschen**

  Tippen Sie auf der Registerkarte **Organisation** rechts neben **Vorgesetzte(r)**, **Direkte Mitarbeiter** oder **Kollegen** auf das Symbol "Mehr". Erstellen Sie dann entweder eine E-Mail- oder Kalendereinladung. 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 parallel über "Tunnel - Web-SSO"und die Secure Ticket Authority (STA) tunneln. Sie können auch Verbindungen mit "Tunnel - Web-SSO"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 unter Hinzufügen einer MDX-App.
2. Klicken Sie für die Netzwerkzugriffsrichtlinie auf die Option **Tunnel - Web-SSO**. Weitere Informationen finden Sie unter App-Netzwerkzugriff

Secure Mail für iOS 19.1.6

Dieses Release enthält Leistungsverbesserungen und Bugfixes.

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 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:**
>
> Dieses 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-Media-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** muss auf **Zulassen** oder **E-Mail-Absender oder Ereignistitel** festgelegt sein.
  - 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. Wenn die Anlage nicht mit Secure Mail angezeigt werden kann, wird eine Liste der Apps angezeigt. Sie können dann die erforderliche App zur Anzeige der Anlage auswählen. Weitere Informationen 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 Android enthält die MDX-Richtlinie **Kalender exportieren** den 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

Dieses Release enthält Leistungsverbesserungen und Bugfixes.

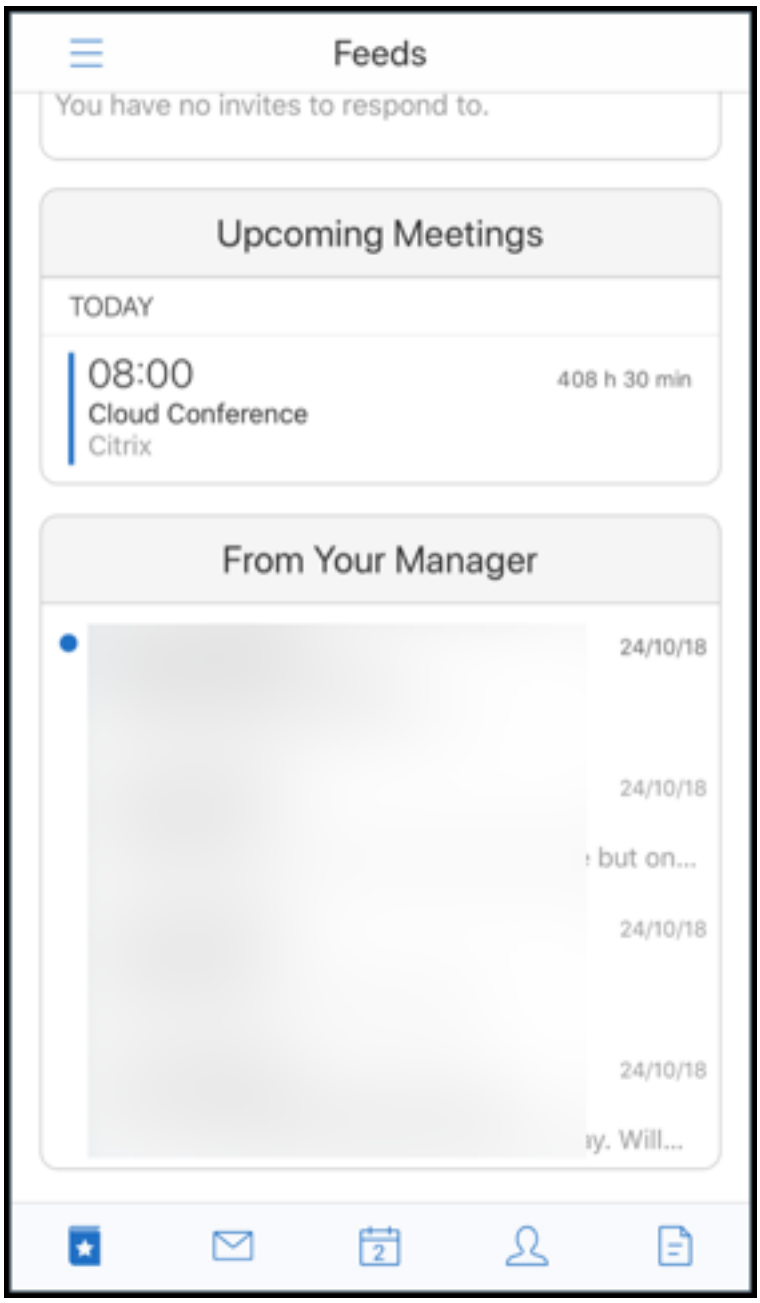
Informationen zu behobenen und bekannten Probleme finden Sie unter Bekannte und behobene Probleme.

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** als **Als Anlage melden** festlegen. Der Administrator konfiguriert diese Einstellungen in der Citrix Endpoint Management-Konsole. Weitere Informationen zum Konfigurieren von MDX-Richtlinien für Secure Mail finden Sie unter MDX-Richtlinien für mobile Produktivitätsapps.
- **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. Weitere Informationen finden Sie unter Drucken von E-Mails und Kalenderereignissen.
- **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:**
>
> Dieses 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. Weitere Informationen 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-Level 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.

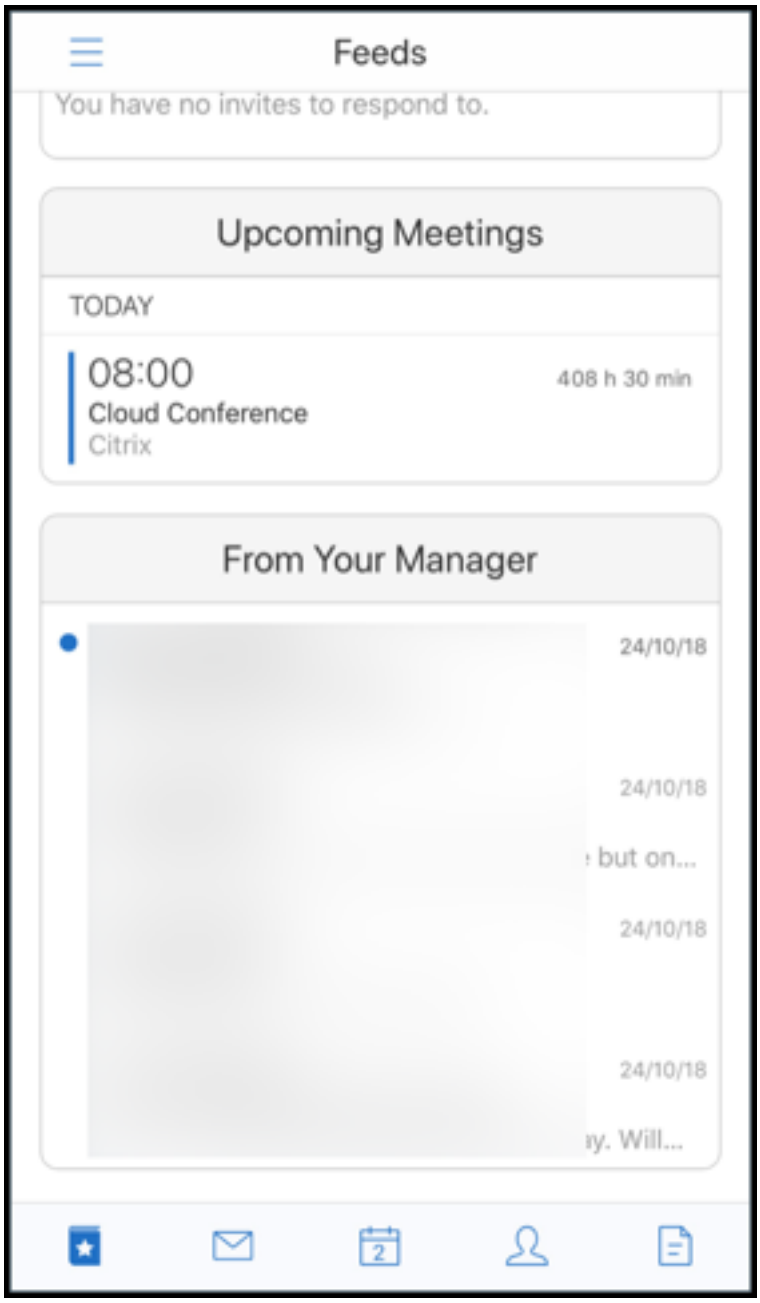
Einschränkungen:

- Wenn Sie keine FCM-basierten Push-Benachrichtigungen aktiviert haben, erfolgt die Hintergrundsynchronisierung alle 15 Minuten. Das Intervall variiert, 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-Media-Inhalt:** In Secure Mail für iOS werden je nach Benachrichtigungsfehler Fehlermeldungen zu Pushbenachrichtigungen in der Mitteilungszentrale auf Geräten angezeigt. Informationen zu den Fehlermeldungen zu Pushbenachrichtigungen in Secure Mail für iOS finden Sie unter 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:**
>
> Dieses 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. Weitere Informationen 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. Weitere Informationen finden Sie unter Benachrichtigungskanäle.
- **Phishing-E-Mails melden (durch Weiterleiten):** In Secure Mail für iOS können Sie das Feature "Als Phishing melden"verwenden, um eine E-Mail (durch Weiterleiten) 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 **Phishingberichtmethode** auf **Durch Weiterleiten melden** festlegen. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Phishing-E-Mail melden.

Secure Mail 18.9.0

- Neues Versionsnummerierungsschema im Format "yy.mm.version". Beispiel: Version **18.9.0**
- **Phishing-E-Mails melden (durch Weiterleiten):** In Secure Mail für Android können Sie das Feature "Als Phishing melden"verwenden, um eine E-Mail (durch Weiterleiten) 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 melden"konfigurieren und "Phishingberichtmethode"auf **Durch Weiterleiten melden** festlegen. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Phishing-E-Mail melden.
- **Verbesserungen an den Feedkarten:** 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. Weitere Informationen 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: Identifizieren Sie eingehende Anrufe von Ihren Kontakten, indem Sie in den **Einstellungen** des Geräts die Secure Mail-Anrufer-ID 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”. Weitere Informationen finden Sie unter Secure Mail-Anrufer-ID.

Secure Mail 10.8.60

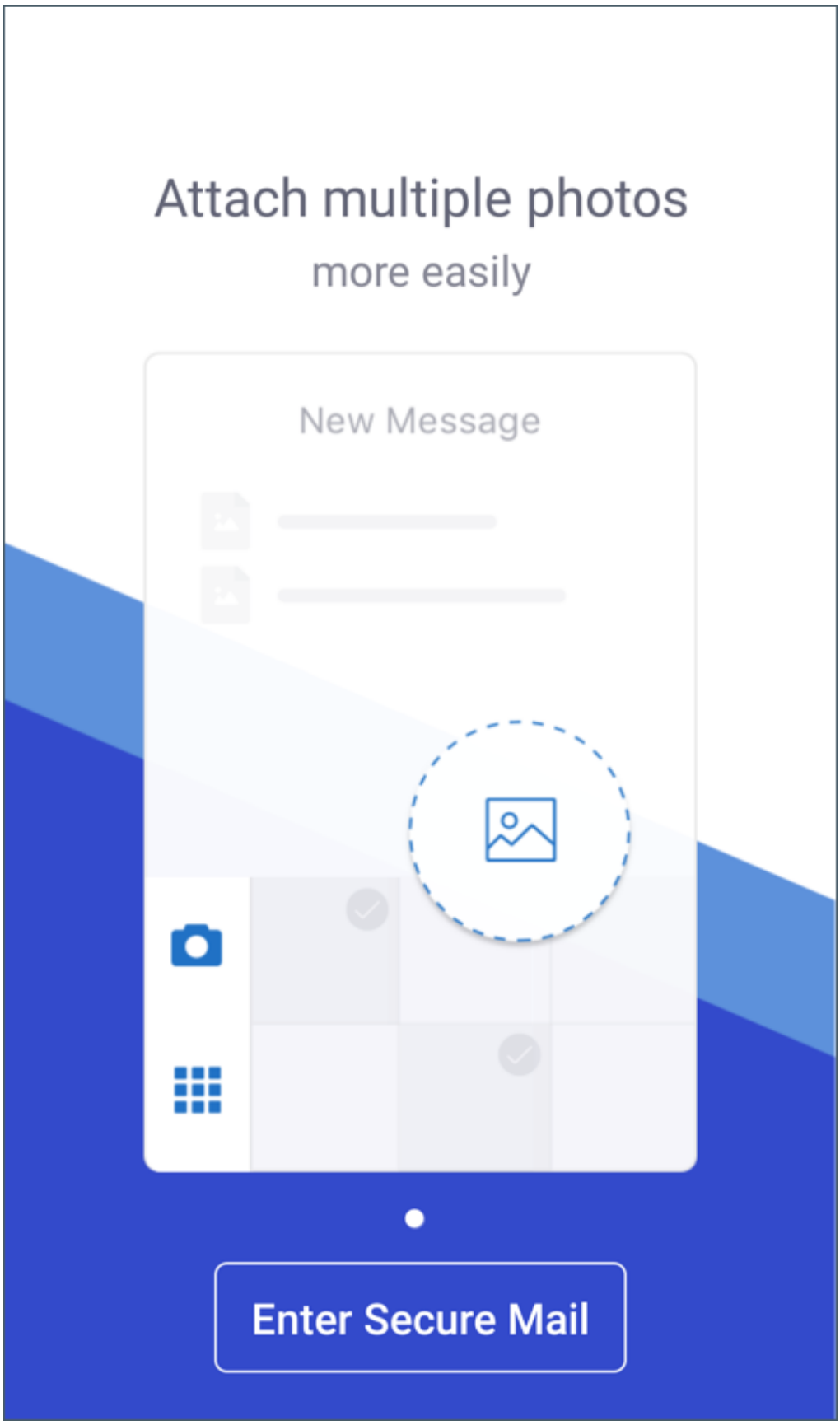
- Secure Mail unterstützt Android P.
- Secure Mail ist jetzt auch auf Polnisch verfügbar.
- In Secure Mail für iOS können Sie Dateien an Ihre E-Mail von der iOS nativen Dateianwendung anhängen. Weitere Informationen finden Sie unter iOS-Features.

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.

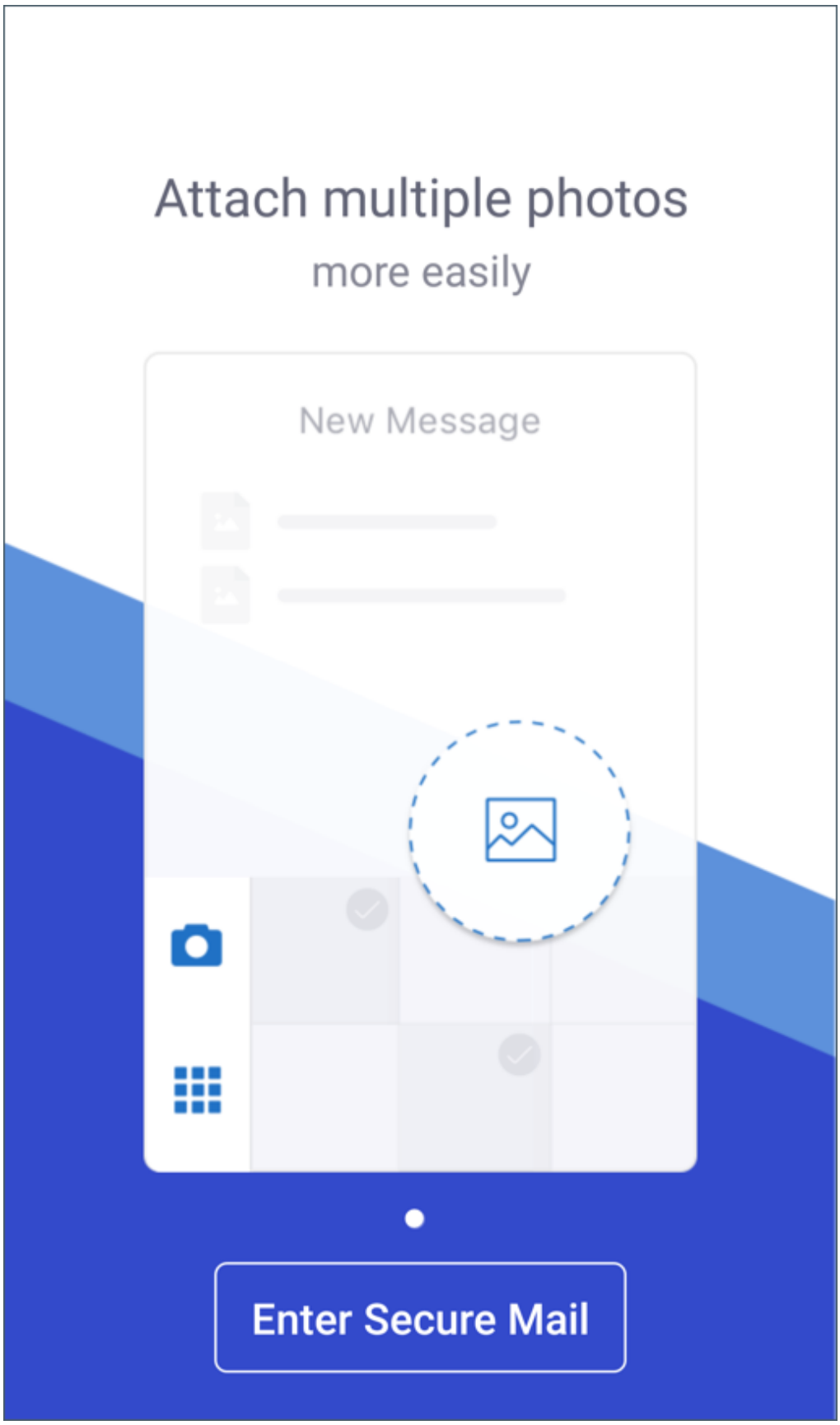


Feeds-Bildschirm in Secure Mail. Der Bildschirm **Feeds** von Secure Mail für iOS und Android enthält alle ungelesenen E-Mails und Besprechungseinladungen sowie anstehende Besprechungen.

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.



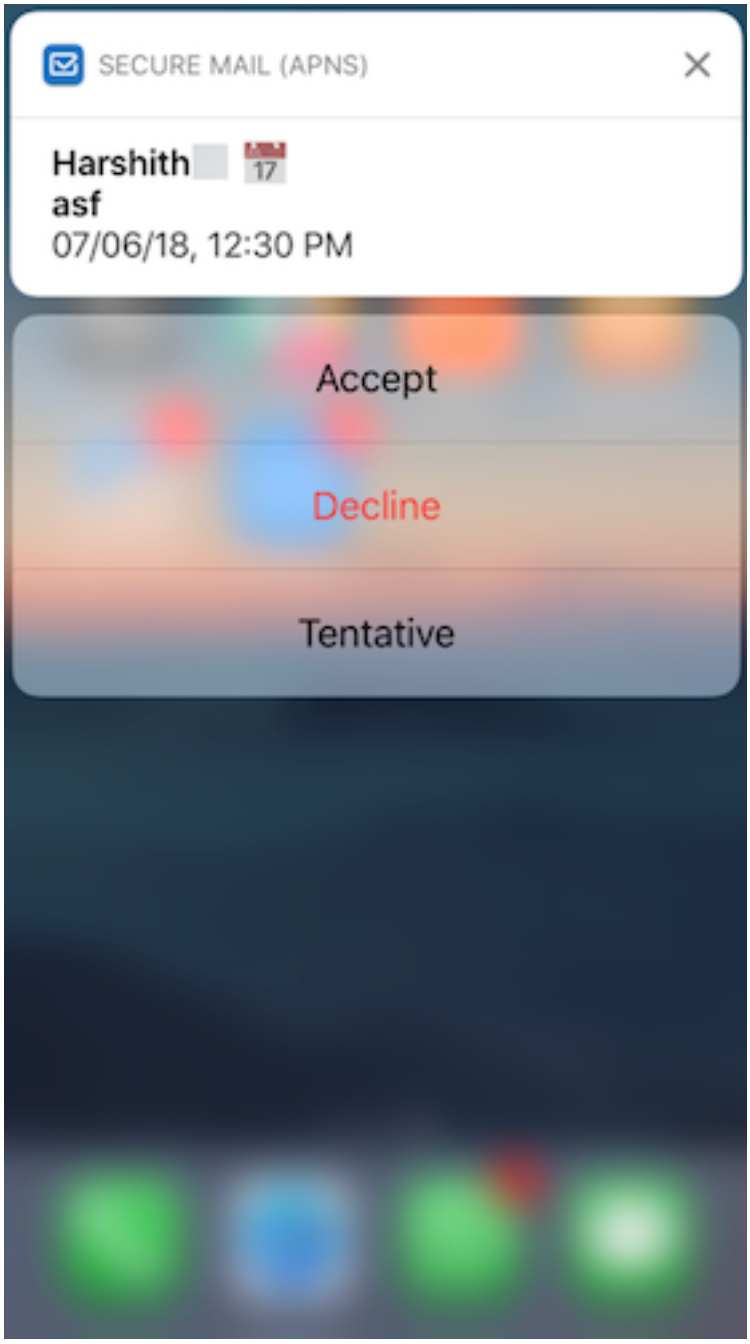
Secure Mail 10.8.40

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

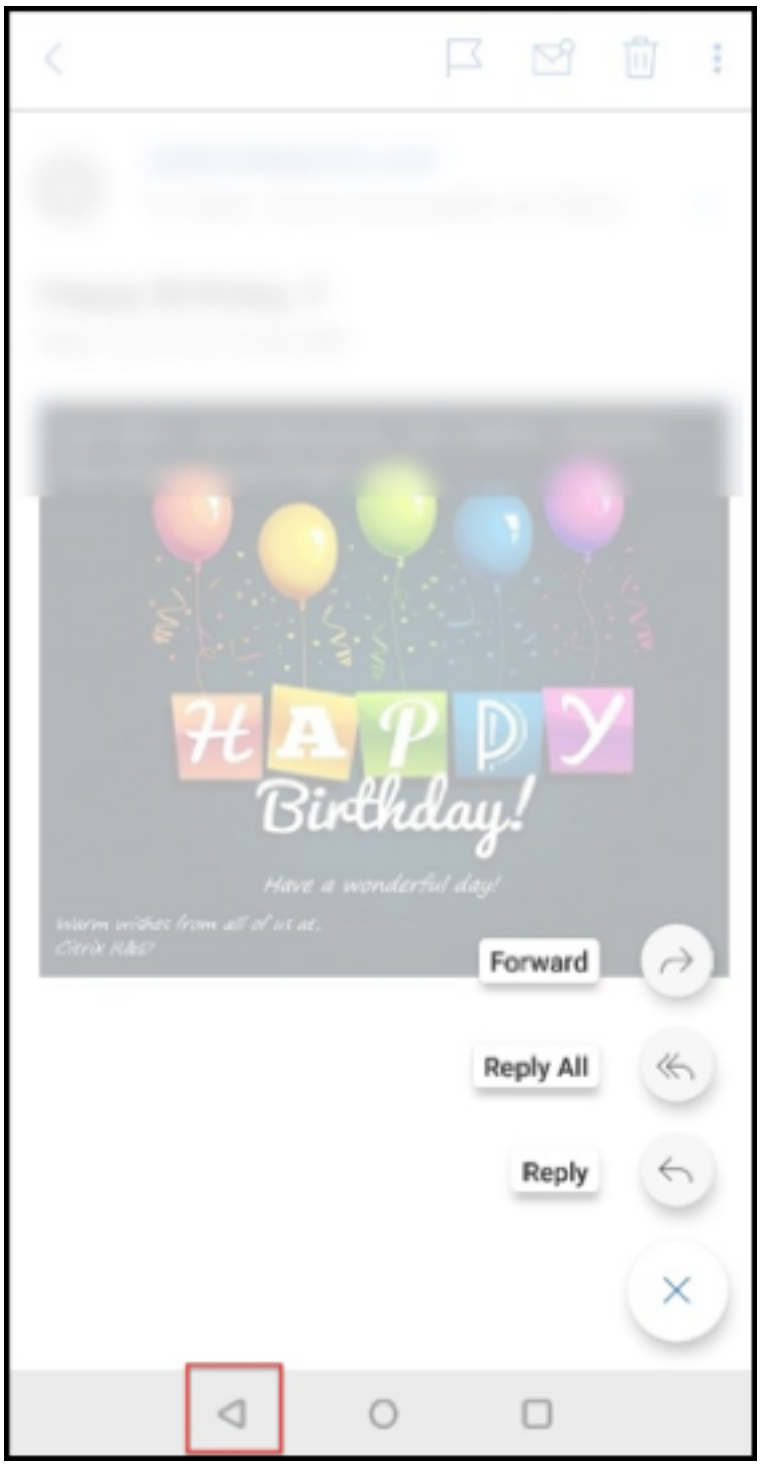
Secure Mail 10.8.35

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.

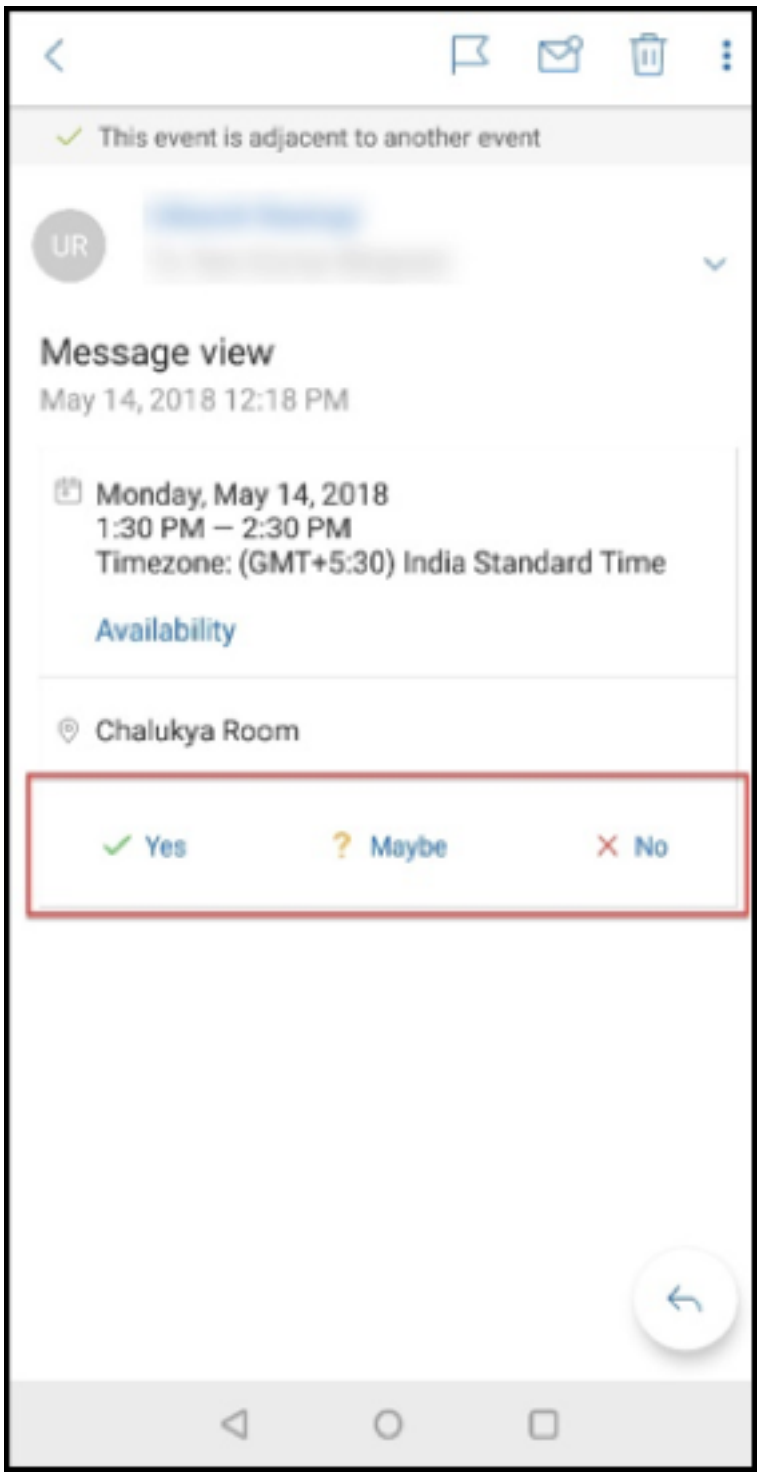


- **Erweiterungen für die Taste “Zurück”in Secure Mail für Android.** In Secure Mail für Android können Sie auf Ihrem Gerät auf die Taste “Zurück”tippen, um die erweiterten Optionen der unverankerten Aktionstaste zu schließen. Wenn die unverankerte Aktionstaste im erweiterten Zustand ist, werden durch 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

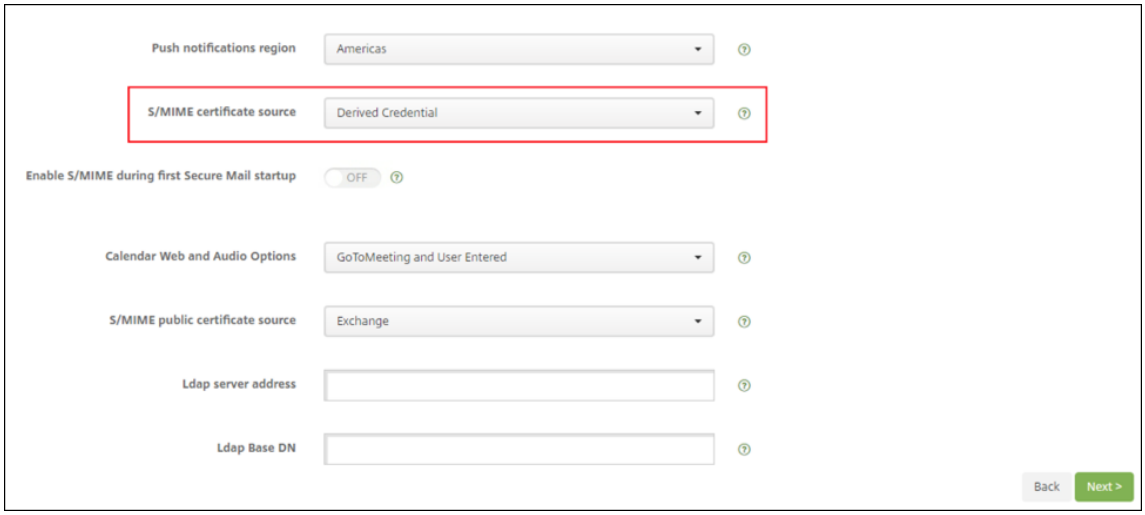
Secure Mail für iOS unterstützt jetzt S/MIME für abgeleitete Anmeldeinformationen: Damit dieses Feature funktioniert, führen Sie folgende Schritte aus:

- Wählen Sie "Abgeleitete Anmeldeinformationen"als Quelle des S/MIME-Zertifikats aus. Weitere Informationen finden Sie unter Abgeleitete Anmeldeinformationen für iOS.
- 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).

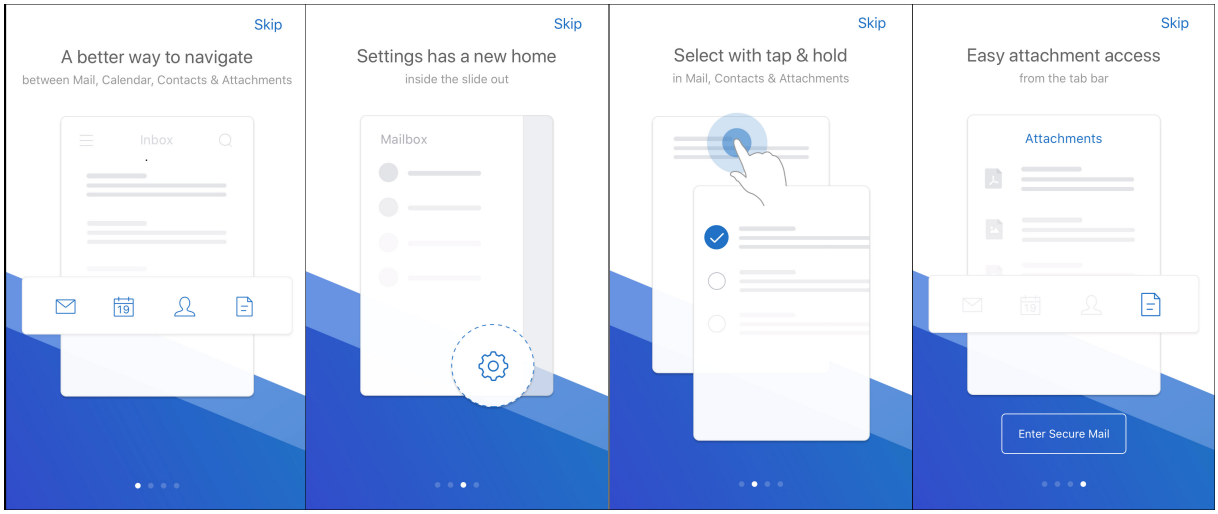
Weitere Informationen zum Registrieren von Geräten mit abgeleiteten Anmeldeinformationen finden Sie unter Registrieren von Geräten mit abgeleiteten Anmeldeinformationen.

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.

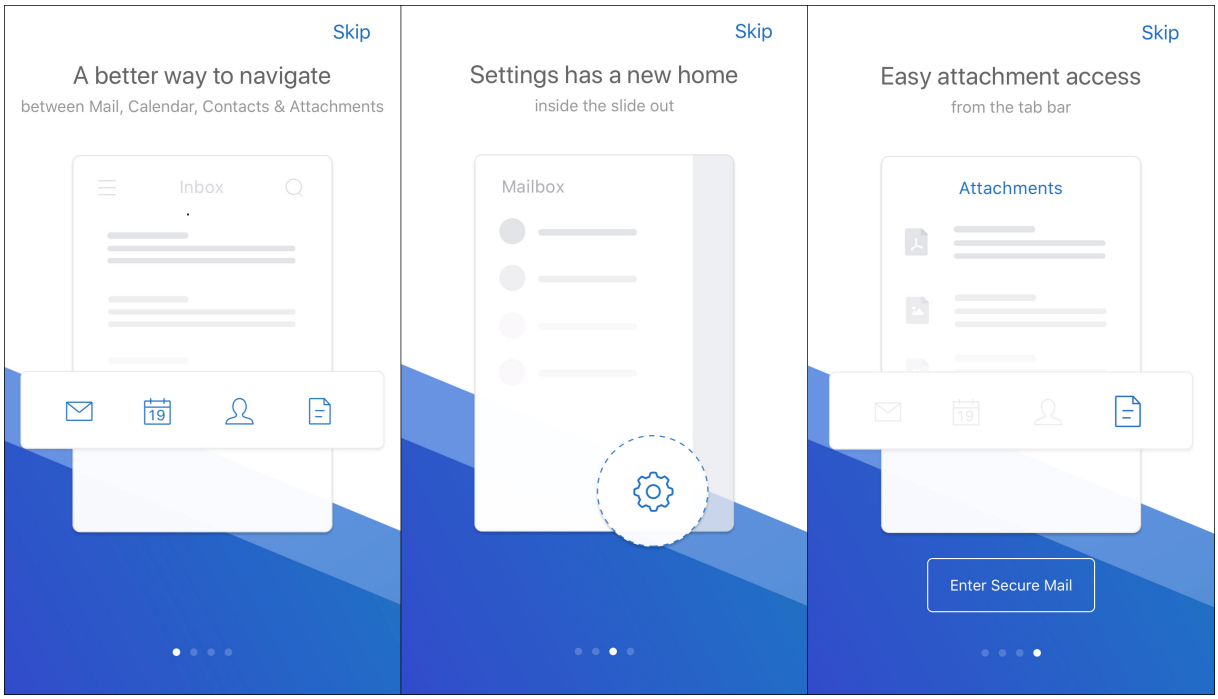


Secure Mail für iOS und Android wurden umfassend überarbeitet: Wir haben die Navigation für Benutzer einfacher und effizienter gemacht. Wir haben das Menü und die Aktionstasten in Form einer Navigationsleiste neu ausgerichtet.

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

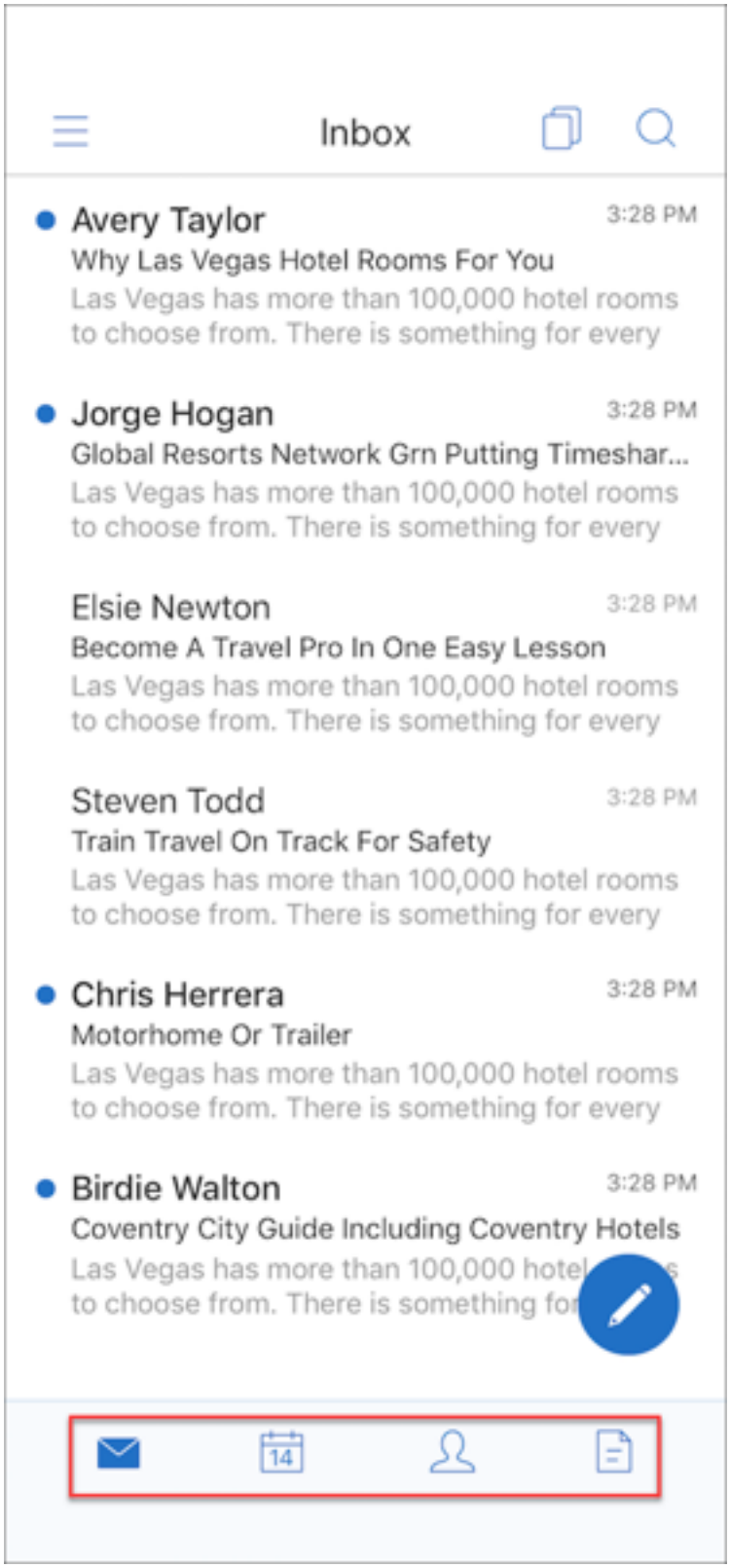


Die folgende Abbildung zeigt die neue Navigationsleiste auf Android-Geräten.

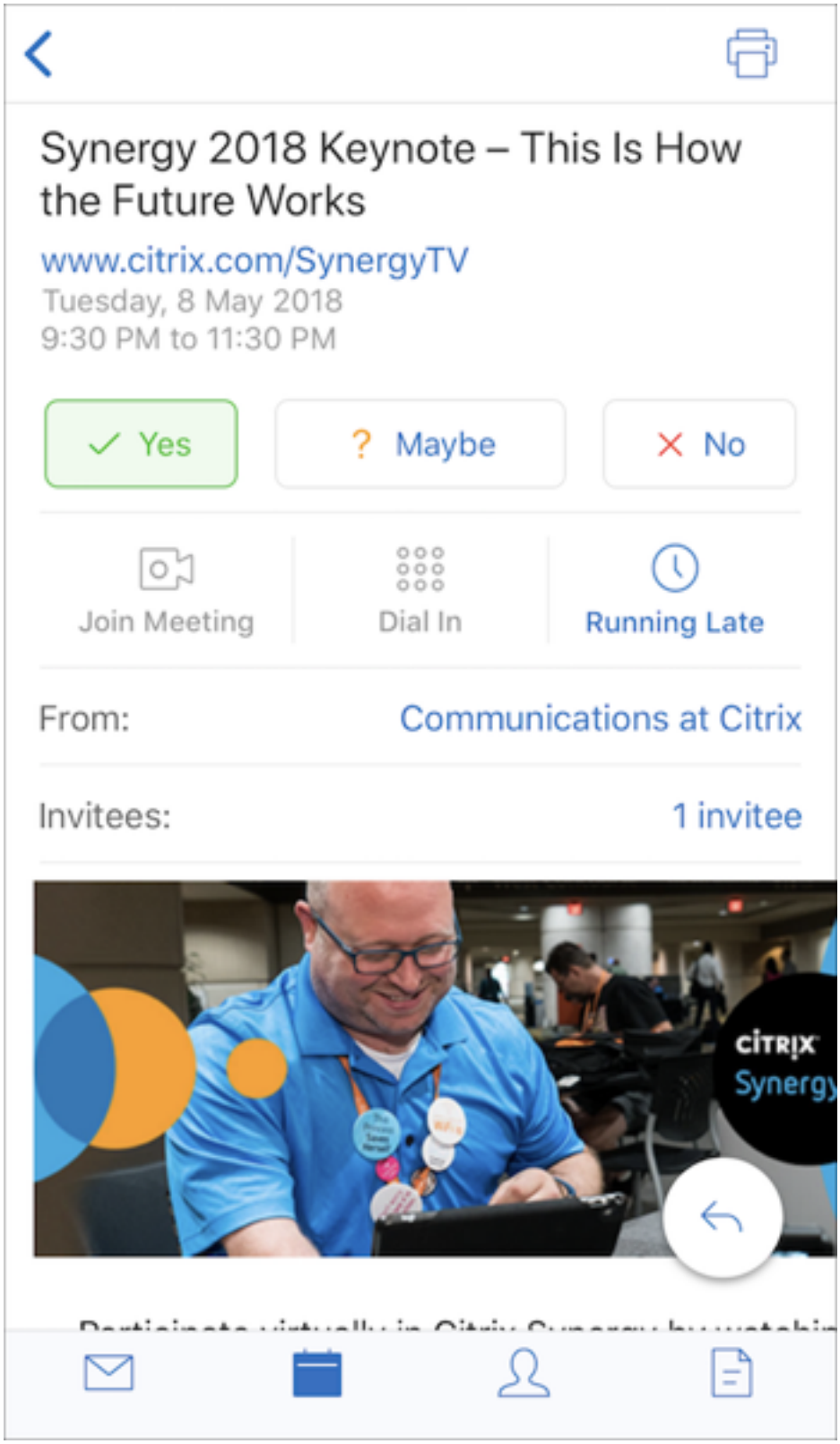


Folgendes hat sich geändert:

- 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.

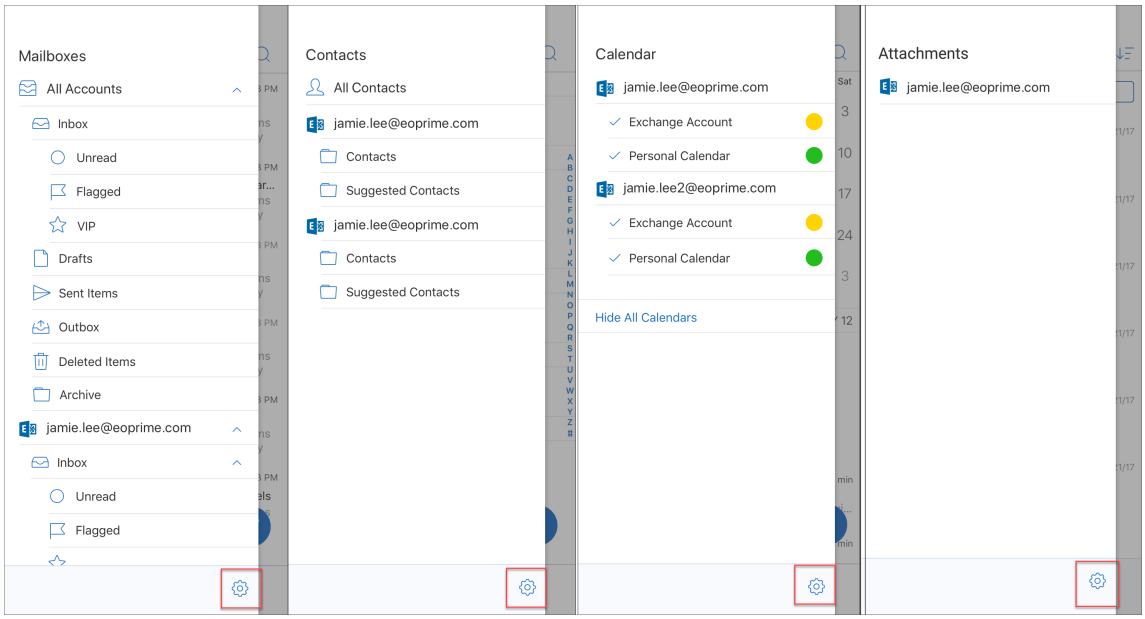


> **Hinweis:**
>
> Auf Android-Geräten ist die Tastenleiste nach dem Öffnen einer E-Mail-Nachricht nicht verfügbar. Wenn Sie beispielsweise eine E-Mail oder ein Kalenderereignis öffnen, ist die Tastenleiste nicht verfügbar, (siehe unten).

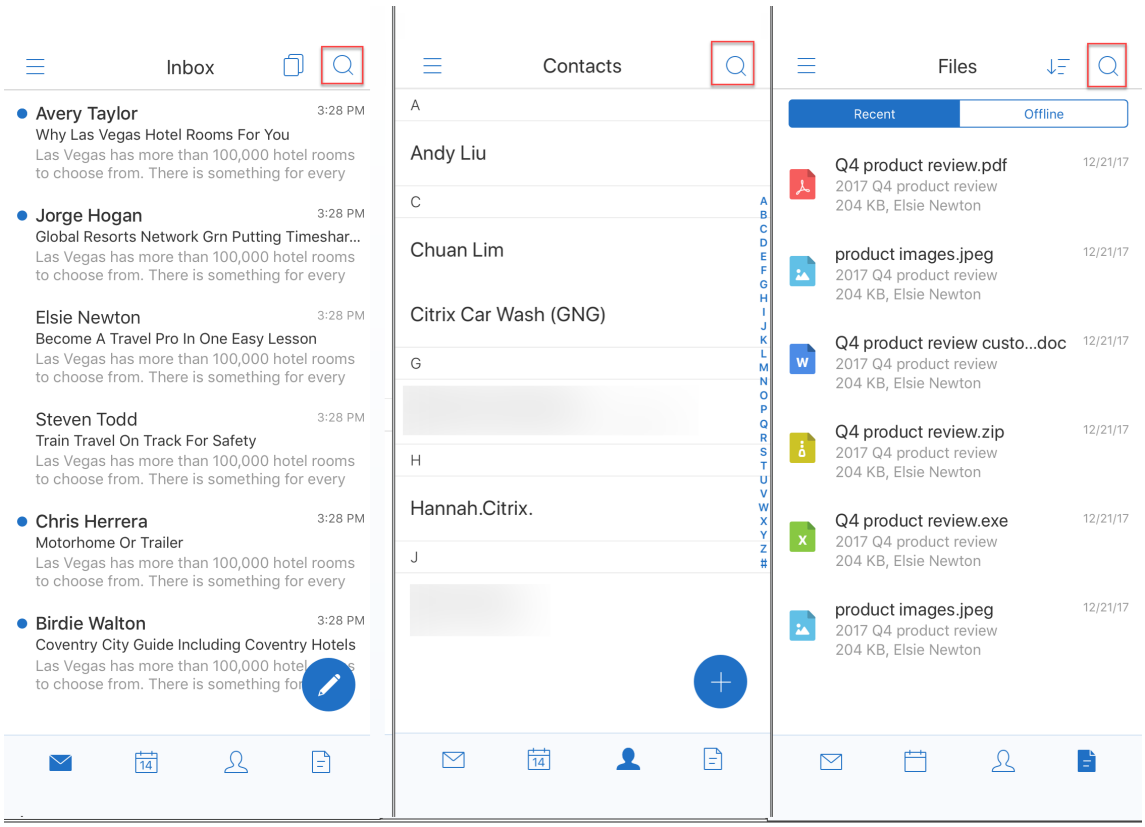


- Das Menü **Einstellungen** ist in allen Menüs, wie E-Mail, Kalender, Kontakte und Anlagen, verfügbar. Um zu den Einstellungen zu gelangen, tippen Sie auf das Hamburgersymbol und dann auf

die Taste **Einstellungen** unten rechts, wie in der folgenden Abbildung dargestellt.

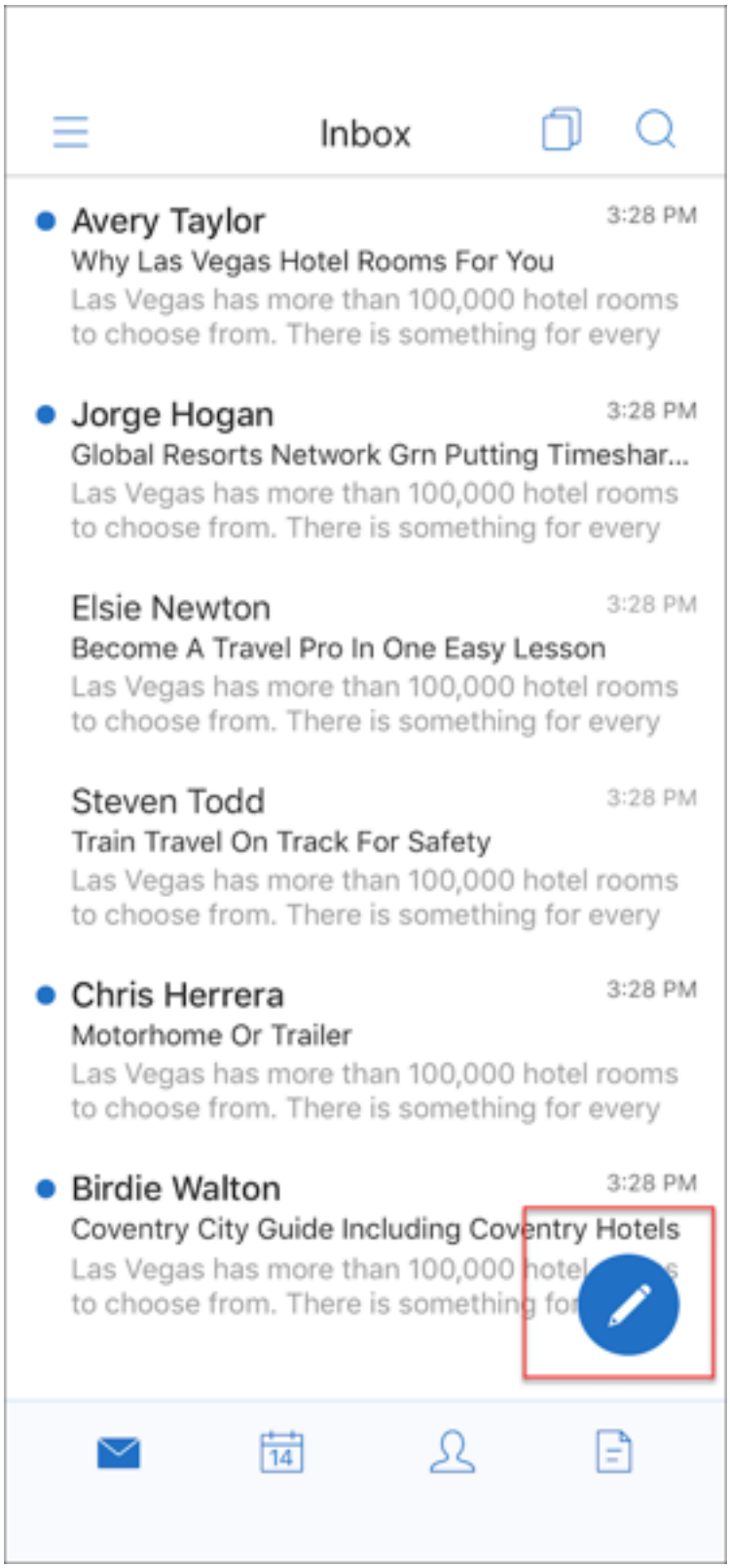


- Das Symbol **Suchen** ersetzt die Suchleiste und ist in den Ansichten “Posteingang”, “Kontakte” und “Anlagen”verfügbar.



- 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).



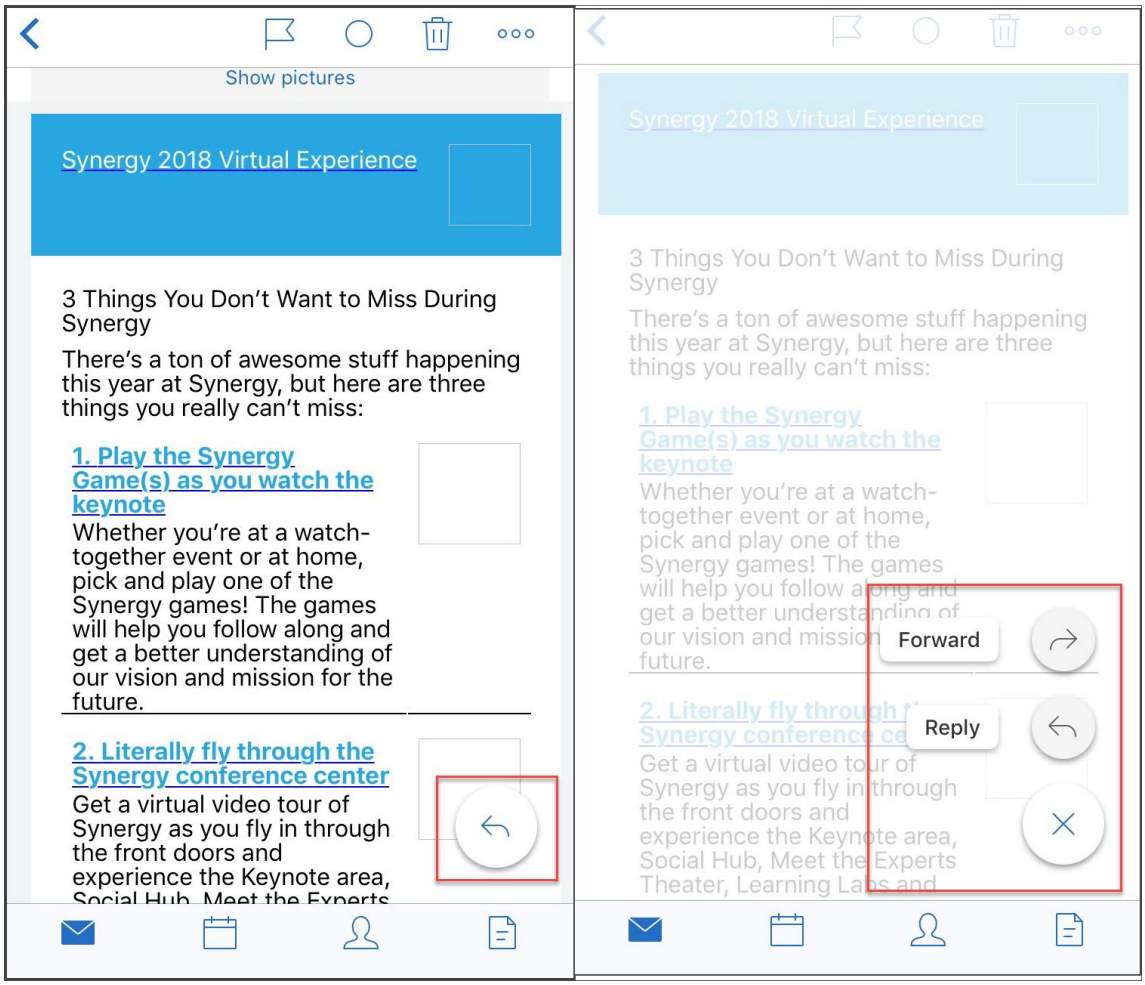
- Die folgenden Menüoptionen sind jetzt oben rechts auf Ihrem Bildschirm verfügbar:

  - **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.



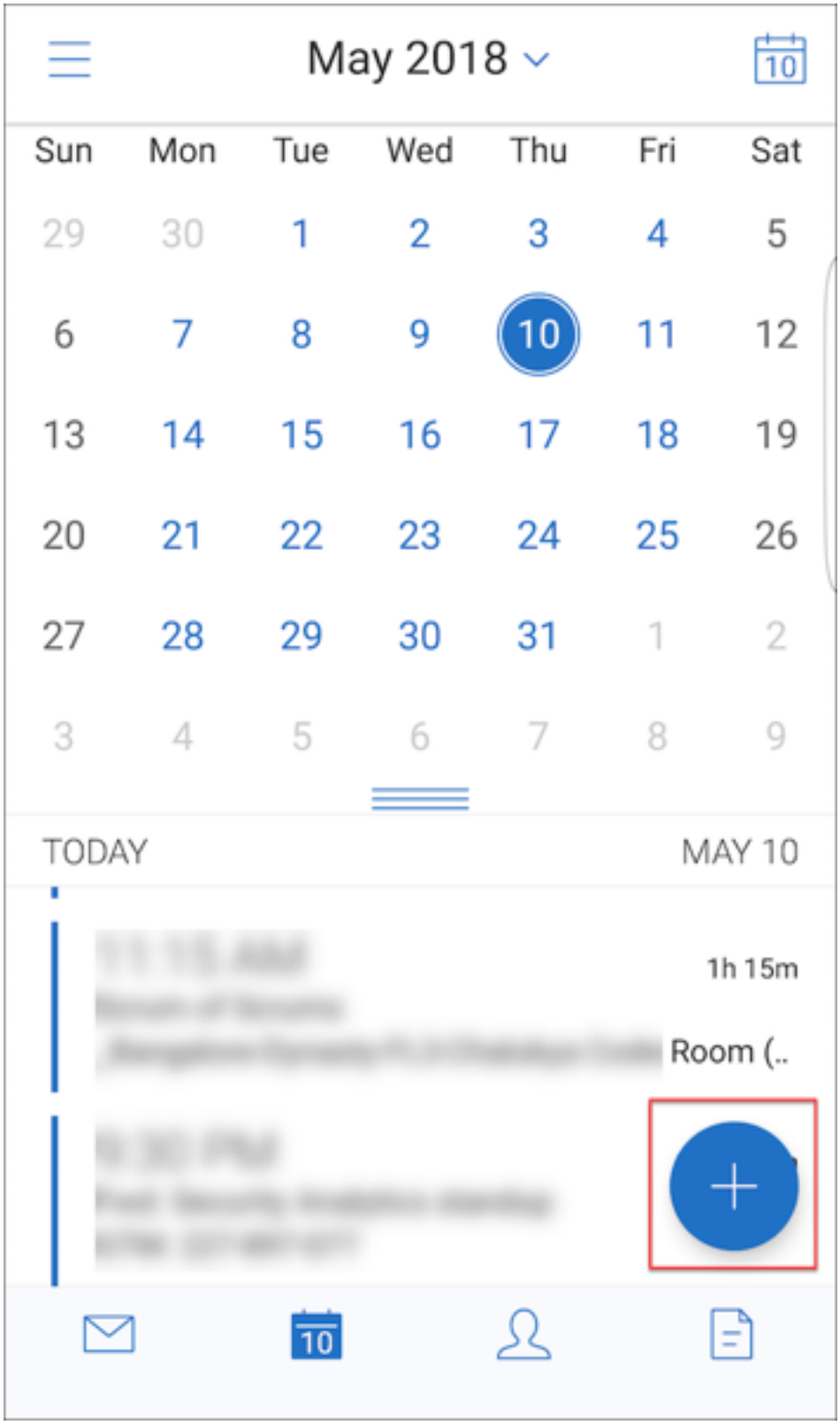
- Beim Anzeigen einer E-Mail stehen die folgenden Menüoptionen oben rechts auf dem Bildschirm zur Verfügung:

  - **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”.

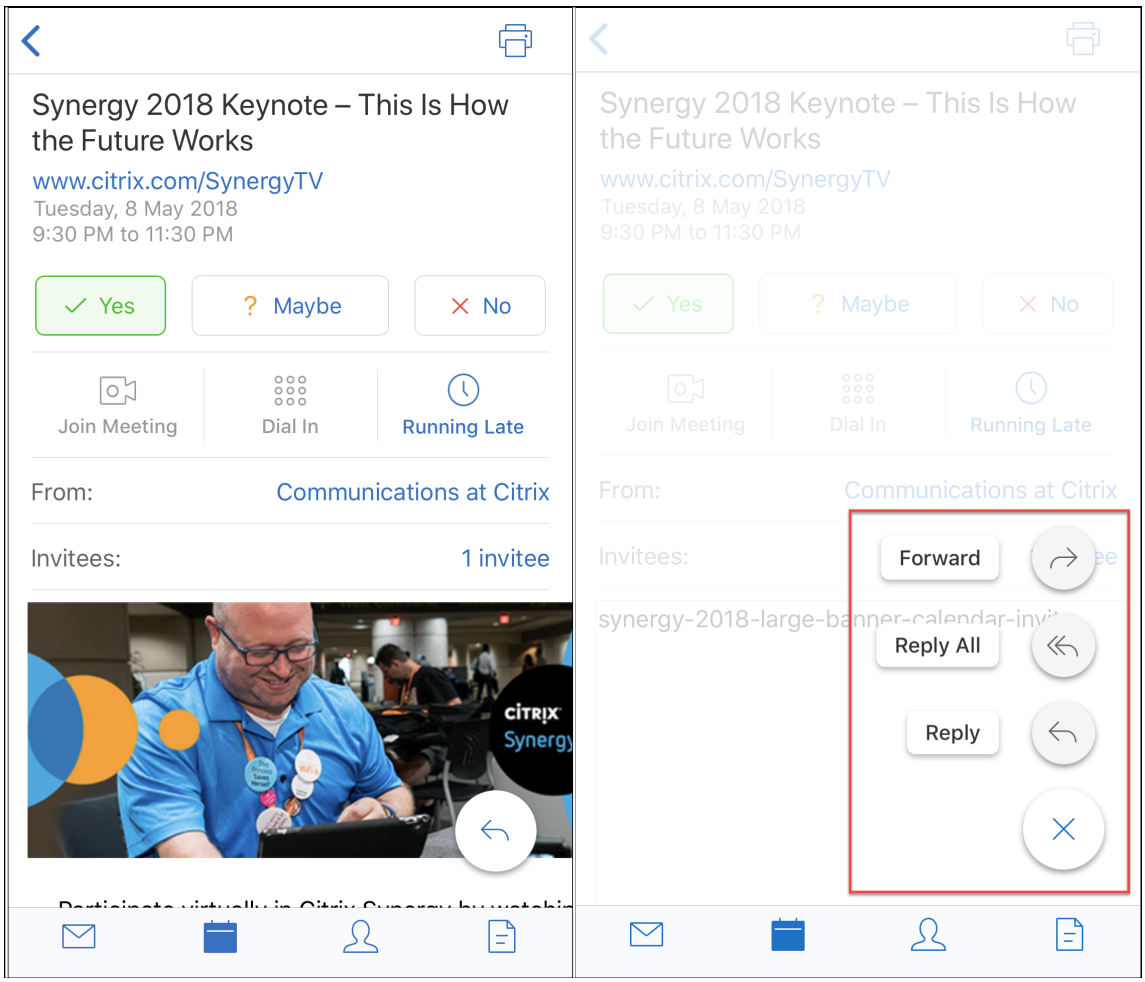
Kalender - Änderungen

- 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:

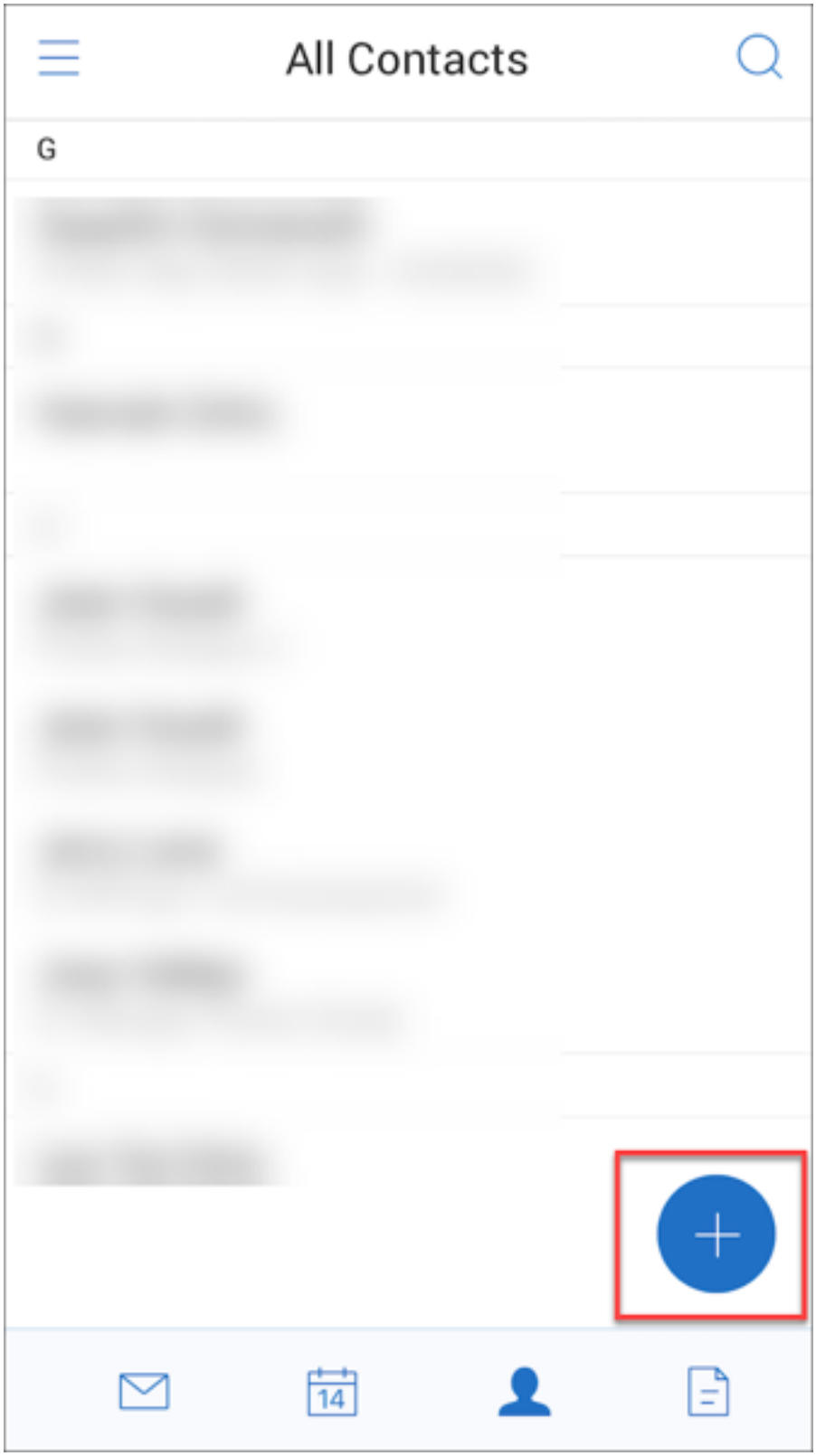
- **Heute:** Antippen, um die heutigen Ereignisse anzuzeigen.
- **Suchen:** Antippen, um nach einem Ereignis zu suchen.
- **Unverankerte Aktionstaste zum Antworten:** Tippen Sie während der Anzeige eines Ereignisses auf “Weiterleiten”, “Allen antworten”oder “Antworten”.



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.

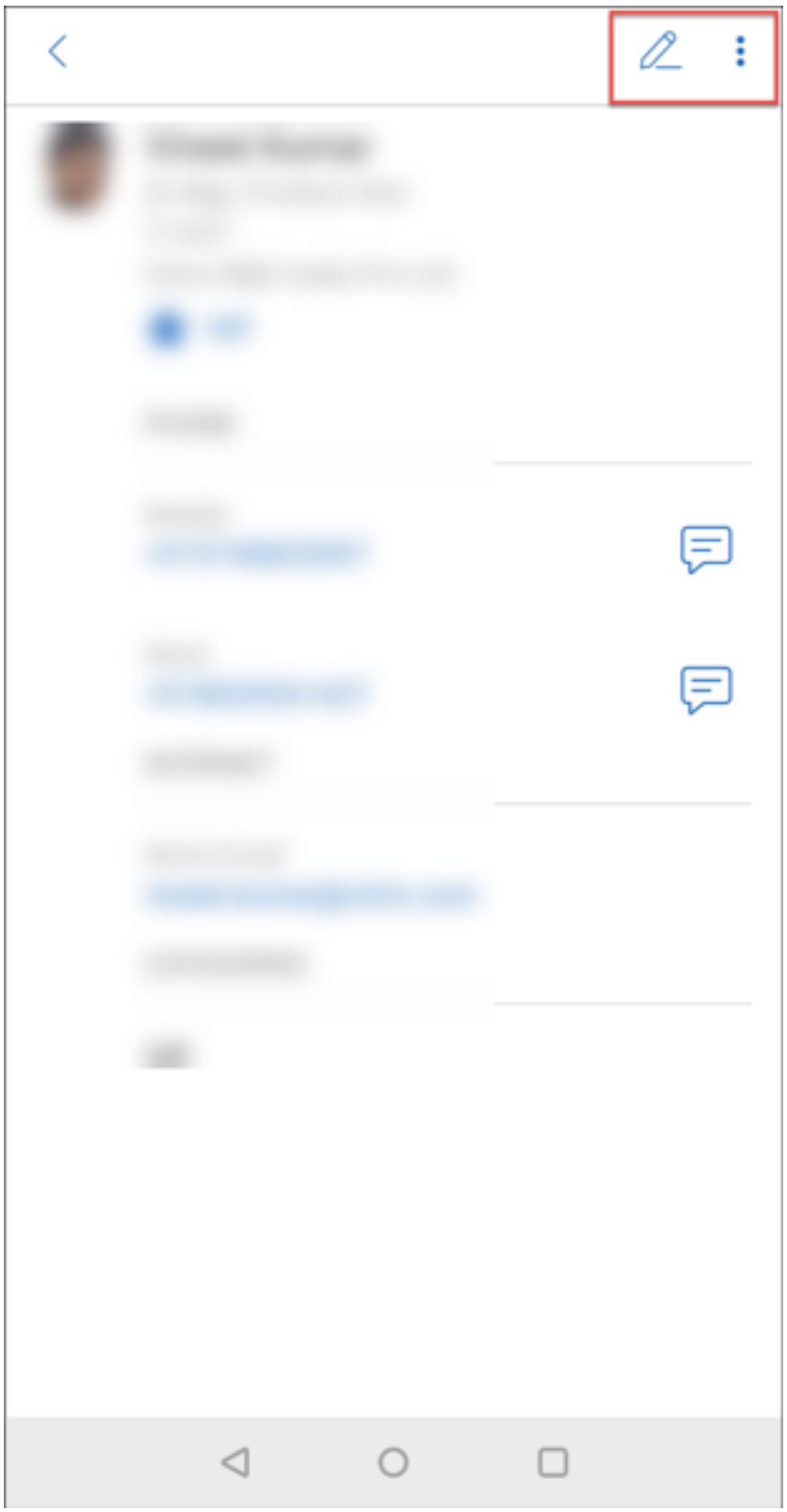


- Die Menüoption **Suchen** ist jetzt oben rechts auf dem Bildschirm verfügbar. Tippen Sie auf die Option, um nach einem Kontakt zu suchen.

- Beim Anzeigen eines Kontakts stehen die folgenden Menüoptionen oben rechts auf dem Bildschirm zur Verfügung:

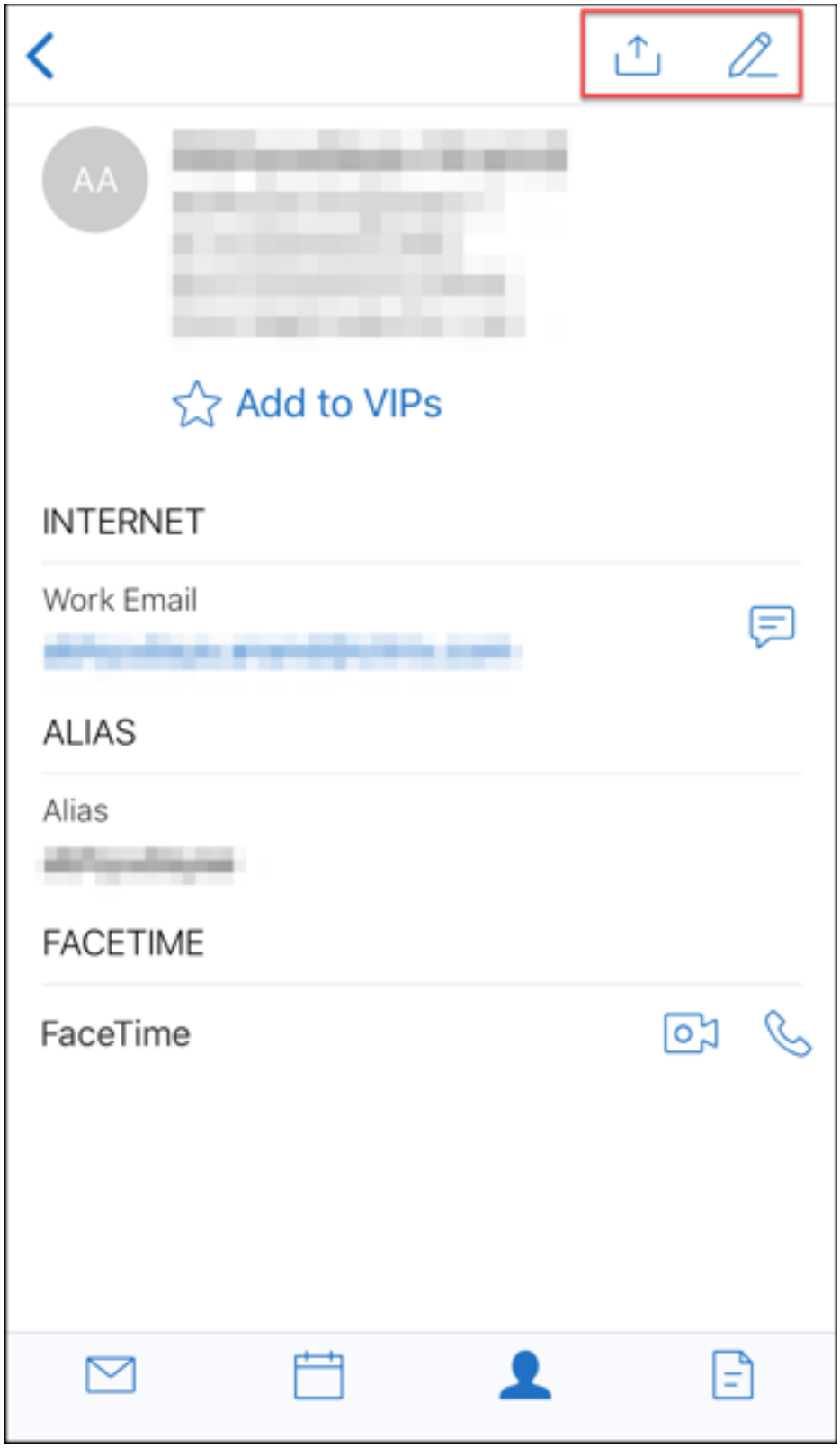
  Auf Android-Geräten:

  - **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”.

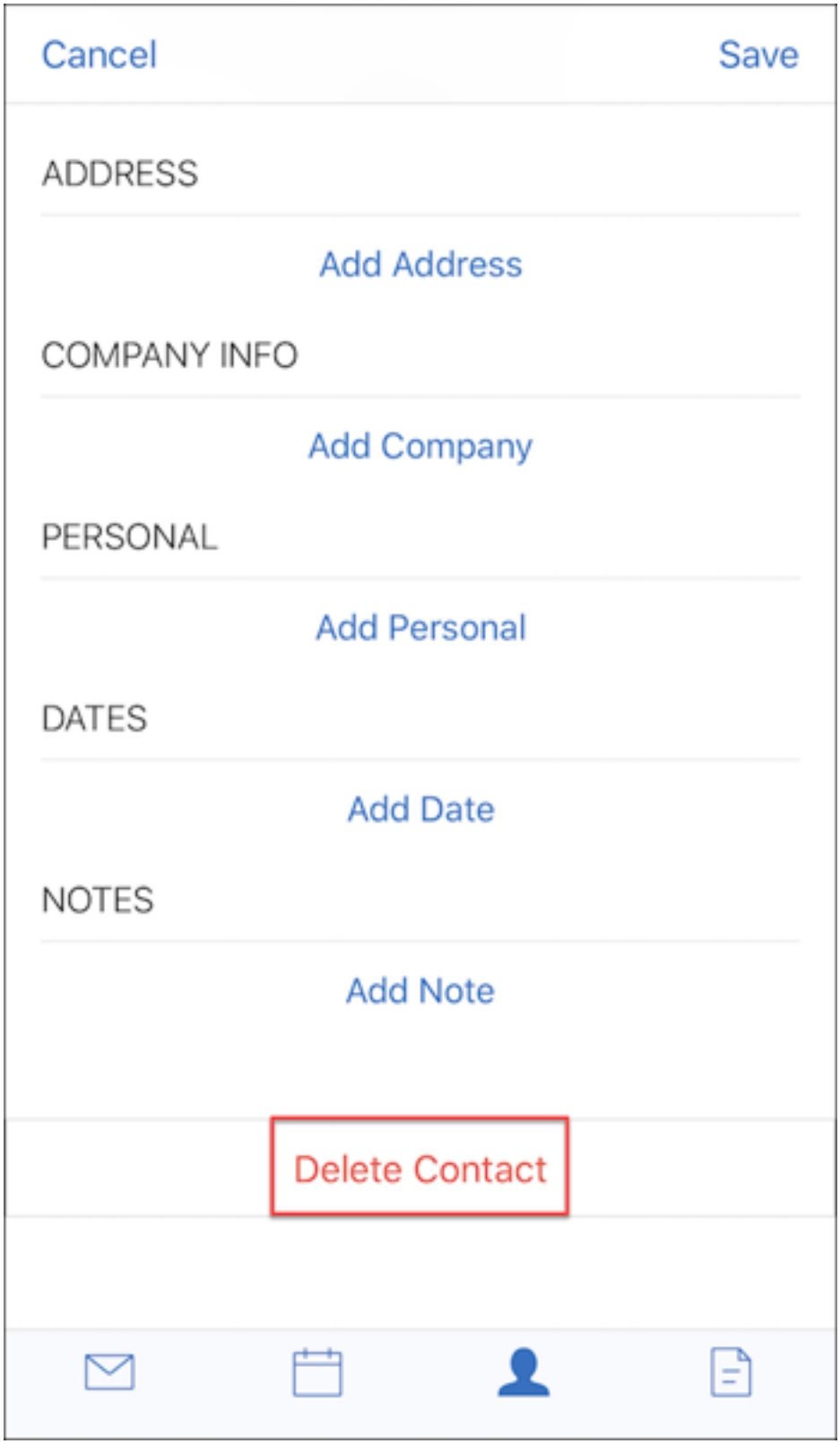


Auf iOS-Geräten:

- **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 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 iOS.
- Secure Mail für iOS unterstützt Pushbenachrichtigungen mit Rich-Media-Inhalt. Benachrichtigungen mit Rich-Media-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. Weitere Informationen finden Sie unter Pushbenachrichtigungen mit Rich-Media-Inhalt.

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

- Secure Mail für iOS unterstützt jetzt Rich-Text-Signaturen. Sie können Bilder oder Links in Ihrer E-Mail-Signatur verwenden. Weitere Informationen 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. Weitere Informationen finden Sie unter Rich-Text-Signaturen.
- **Secure Mail unterstützt Android Enterprise (zuvor "Android for Work").** Sie können ein separates Arbeitsprofil erstellen, indem Sie Android Enterprise-Apps in Secure Mail verwenden. Weitere Informationen finden Sie unter Android Enterprise in Secure Mail.
- **Secure 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). Weitere Informationen finden Sie unter Moderne Authentifizierung mit Microsoft Office 365.

> **Hinweis:**
>
> 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.

Bekannte und behobene Probleme

June 6, 2024

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

Secure Mail für iOS 24.3.0

Behobene Probleme

- Trotz der erfolgreichen Installation und Registrierung von Secure Mail erhalten Endbenutzer bei der Konfiguration der App möglicherweise die folgende Fehlermeldung:

  "Bei der Verbindung zum Server ist ein Timeout aufgetreten. Versuchen Sie es in einigen Minuten erneut."

  [XMHELP-4538]

- Nach dem Upgrade auf Secure Mail für iOS Version 24.2.0 können bestehende Endbenutzer möglicherweise nicht auf Secure Mail zugreifen und es wird die folgende Fehlermeldung angezeigt:

  "Secure Mail konnte den Server nicht erreichen. Versuchen Sie erneut, die Serveradresse einzugeben. Wenn Sie immer noch Probleme haben, wenden Sie sich an Ihren IT-Administrator"

  [XMHELP-4539]

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

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Mail für iOS 24.2.0

Behobene Probleme

- In Secure Mail für iOS wird die Schaltfläche "Hinzufügen (+)"auf der Kalenderseite möglicherweise nicht angezeigt, sodass Sie keine neuen Kalendereereignisse erstellen können. [XMHELP-4460]
- Secure Mail kann aufgrund eines Netzwerkverbindungsproblems keine E-Mails auf iPhone- und iPad-Geräten synchronisieren. [XMHELP-4473]
- Wenn Sie den dunklen Modus in Secure Mail für iOS verwenden, können Sie Ihre E-Mail-Nachrichten möglicherweise nicht lesen. [XMHELP-4499]

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Mail für Android 24.1.0

Behobene Probleme

- Wenn Sie versuchen, E-Mail-Anhänge zu öffnen, die größer als 10 MB sind, reagiert Secure Mail für Android nicht mehr. [XMHELP-4399]

- Wenn Sie versuchen, einen E-Mail-Anhang im DOCX-Format zu öffnen, der arabische Zeichen oder Hyperlinks enthält, reagiert Secure Mail für Android nicht mehr. Das Problem tritt auf, wenn das Polaris-SDK nicht aktualisiert ist. [XMHELP-4491]

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Mail für Android 23.10.0

Behobene Probleme

- Wenn Sie einen Anhang aus Secure Mail öffnen, finden Sie möglicherweise die Option **Nach Citrix Files hochladen** unter der Option **Mehr (⊠)** > **Öffnen mit**, auch wenn die App **Citrix Files** nicht auf Ihrem Gerät installiert ist. [XMHELP-4437]
- Wenn Sie die Vorschau einer ICS-Datei anzeigen, die an eine in Secure Mail erhaltene Besprechungseinladung angehängt ist, stellen Sie möglicherweise fest, dass die in der Vorschau der ICS-Datei angezeigte Besprechungszeit eine Stunde hinter der ursprünglichen Uhrzeit liegt. Dieses Problem tritt in Sommerzeitregionen auf. [XMHELP-4429]
- Wenn Sie Secure Mail auf Version 23.8.2 aktualisieren und den dunklen Modus aktivieren, tritt möglicherweise ein Problem bei der Vorschau eines E-Mail-Anhangs auf. Möglicherweise können Sie die Menüliste nicht sehen, wenn Sie auf das Dreipunktsymbol **(...)** klicken. [CXM-112699]

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Mail für Android 23.8.2

Behobene Probleme

In diesem Release wurden keine Probleme behoben.

Bekannte Probleme

Wenn Sie Secure Mail auf Version 23.8.2 aktualisieren und den dunklen Modus aktivieren, tritt möglicherweise ein Problem bei der Vorschau eines E-Mail-Anhangs auf. Möglicherweise können Sie

die Menüliste nicht sehen, wenn Sie auf das Dreipunktsymbol **(...)** klicken. Um dieses Problem zu umgehen, aktivieren Sie den hellen Modus für Secure Mail. [CXM-112699]

Secure Mail für Android und iOS 23.7.0

Behobene Probleme

In diesem Release wurden keine Probleme behoben.

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Mail für Android 23.8.1

Behobene Probleme

In diesem Release wurden keine Probleme behoben.

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Mail für iOS 23.9.0

Behobene Probleme

- Bei Verwendung der Version 23.2.0 von Secure Mail für iOS mit dem HCL Domino 11-Server können Sie zuvor gespeicherte E-Mail-Entwürfe möglicherweise nicht senden. In Secure Mail wird angezeigt, dass die E-Mails erfolgreich gesendet wurden, die Empfänger erhalten sie jedoch nicht. [XMHELP-4306]

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Mail für Android 23.8.0

Behobene Probleme

In diesem Release wurden keine Probleme behoben.

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Mail für Android 23.7.0

Behobene Probleme

- Möglicherweise erhalten Sie keine Erinnerungsbenachrichtigungen für Kalenderereignisse. Das Problem tritt auf, wenn die Alarm- und Erinnerungsberechtigung für Secure Mail widerrufen wird. [CXM-109036]

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Mail für Android 23.6.0

Behobene Probleme

Bei der Anzeige von E-Mail-Anhängen wird möglicherweise ein Wasserzeichen mit der Aufschrift "Lizenz abgelaufen"angezeigt. Das Problem tritt bei Secure Mail für Android Version 23.3.5 oder früheren Versionen auf. Um E-Mail-Anhänge ohne Wasserzeichen anzuzeigen, führen Sie ein Upgrade auf Secure Mail für Android Version 23.6.0 oder höher durch. [CXM-110137]

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Secure Mail für iOS 23.5.0

Behobene Probleme

- Wenn Sie digital signierte E-Mails erhalten und in Secure Mail öffnen, werden die E-Mail-Anhänge möglicherweise nicht angezeigt. [XMHELP-4247]

Bekannte Probleme

Es gibt keine bekannten Probleme in diesem Release.

Bekannte und behobene Probleme in älteren Versionen

Bekannte und behobene Probleme in älteren Versionen von Secure Mail finden Sie unter Verlauf bekannter und behobener Probleme in Secure Mail.

Bereitstellen von Secure Mail

February 28, 2024

Das generelle Verfahren zum Bereitstellen von Secure Mail mit 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]

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.

> 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

November 7, 2023

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

Moderne Authentifizierung mit Microsoft Office 365

February 28, 2024

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.

> **Hinweis:**
>
> - Informationen zum Migrieren oder Erstellen einer Postfachlösung mit Exchange-Hybridbereitstellung finden Sie in der Microsoft-Dokumentation unter Exchange ActiveSync-Geräteeinstellungen mit Exchange-Hybridbereitstellungen.

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.
- **Web-SSO zum Tunneln:** Mit dieser Richtlinie können Sie den OAuth-Datenverkehr über Web-SSO tunneln. Vorgehensweise:
  - Legen Sie Richtlinie **Web-SSO zum Tunneln verwenden** auf **Ein** fest.
  - Wählen Sie die Option **Tunnel - Web-SSO** für die Netzwerkzugriffsrichtlinie.

    > **Hinweis:**
    >
    > Informationen zur Aktivierung der STA finden Sie unter Verbindung mit einem E-Mail-Server über die STA.

  - Schließen Sie alle Hostnamen, die mit OAuth in Verbindung stehen, von der Richtlinie für **Hintergrunddienste** aus.

Richtlinien für iOS- und Android-Geräte:

- **Benutzerdefinierter Benutzeragent für moderne Authentifizierung:** Verwenden Sie diese Richtlinie zum Ändern der Standard-Benutzeragent-Zeichenfolge für die moderne Authentifizierung.
- **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. Mit dieser Richtlinie können Sie je nach Anforderung entweder die on-premises Serveradresse oder die Cloud-Serveradresse definieren.
- **Konfigurieren der HTTP 451-Umleitung:** Informationen zum Konfigurieren der Umleitungen finden Sie im Knowledge Center-Artikel Secure Mail ActiveSync redirect 451.

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-Media-Inhalt unter iOS möglich. Informationen zu Pushbenachrichtigungen mit Rich-Media-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	Office 365-Authentifizierungsmethode/Moderne Authentifizierung mit O365	Vertrauenswürdige AD FS-Hostnamen	Vertrauenswürdige Exchange Online-Hostnamen
On-Premises	AUS	Nicht verfügbar	Nicht verfügbar
Hybrid*	EIN	AD FS/IDP	`Outlook.office365.com` oder Vanity-URL

Exchange-Infrastruktur	Office 365-Authentifizierungsmethode/Moderne Authentifizierung mit O365	Vertrauenswürdige AD FS-Hostnamen	Vertrauenswürdige Exchange Online-Hostnamen
Exchange Online	EIN	AD FS/IDP	`Outlook.office365.com` oder Vanity-URL

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

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

Wird ein On-Premises-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.

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

Hybride moderne Authentifizierung mit on-premises Exchange-Unterstützung für iOS und Android

November 7, 2023

Hybride moderne Authentifizierung (HMA) ist eine Lösung für die Verwaltung von Benutzeridentitäten, die eine sicherere Art der Benutzerauthentifizierung und Autorisierungsmethoden verwendet. Sie ist jetzt auch für hybride Bereitstellungen von Exchange Server on-premises verfügbar.

HMA ist eine OAuth-Token-basierte Authentifizierung mit Benutzername und Kennwort. Sie ermöglicht Benutzern von on-premises Mailboxen den Zugriff auf on-premises Exchange mit OAuth-Token. OAuth-Token werden von der Cloud bezogen. Die Verwaltung von Benutzeridentitäten mit moderner Authentifizierung bietet Administratoren viele verschiedene Tools zur Sicherung von Ressourcen und bietet zudem sicherere Methoden der Identitätsverwaltung für on-premises Exchange.

Weitere Informationen zu HMA finden Sie unter Announcing Hybrid Modern Authentication for Exchange On-Premises.

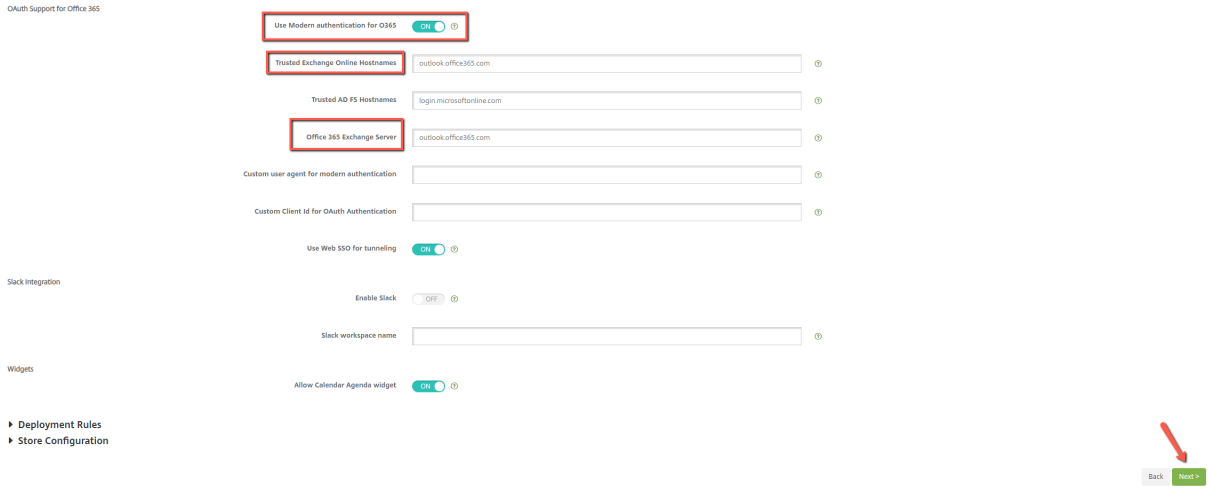
Erforderliche Änderungen an MDX-Richtlinien

Damit HMA auf Secure Mail iOS und Android funktioniert, nehmen Sie die folgenden Änderungen an den MDX-Richtlinien unter dem Abschnitt **OAuth-Unterstützung für Office 365** vor:

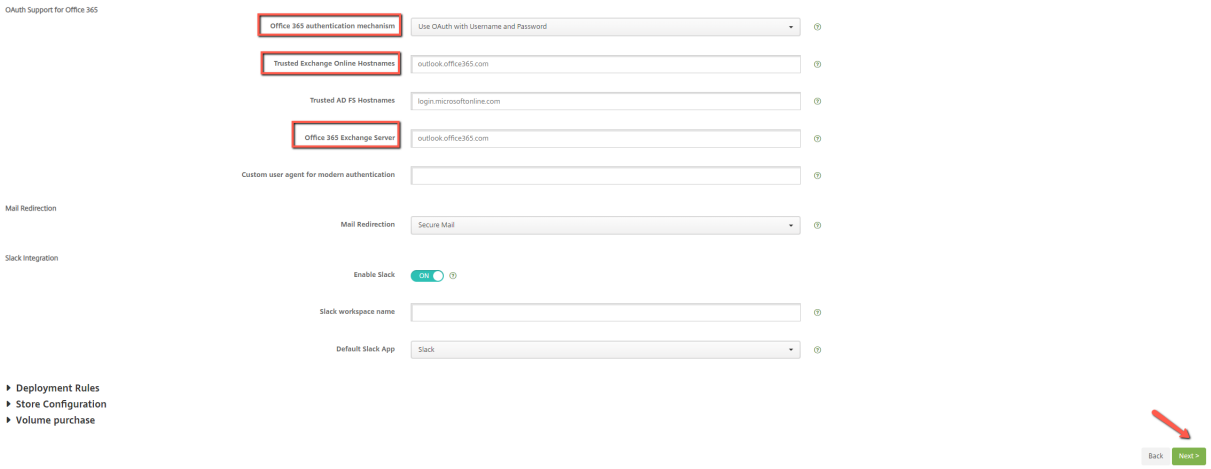
- Für Android aktivieren Sie die Option **Moderne Authentifizierung für O365 verwenden**. Stellen Sie für iOS die **Office 365-Authentifizierungsmethode** auf **OAuth mit Benutzername und Kennwort verwenden**.
- Geben Sie die on-premises Exchange-URL des Kunden in das Textfeld **Vertrauenswürdige Exchange Online-Hostnamen** ein.
- Geben Sie die on-premises Exchange-URL des Kunden in das Textfeld **Office 365 Exchange Server** ein.
- Klicken Sie auf **Weiter**.

Hinweis: Bevor Sie die oben genannten Änderungen an den MDX-Richtlinien vornehmen, müssen Sie sicherstellen, dass die HMA-Einstellungen auf dem Exchange aktiviert sind. Deaktivieren Sie andernfalls die Option **Moderne Authentifizierung für O365 verwenden**.

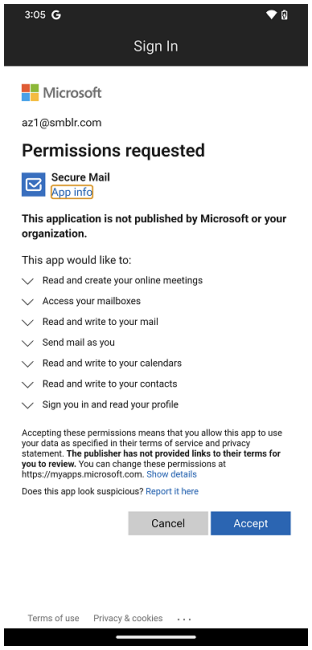
Abschnitt **OAuth-Unterstützung für Office 365** in Android:



Abschnitt **OAuth-Unterstützung für Office 365** in iOS:

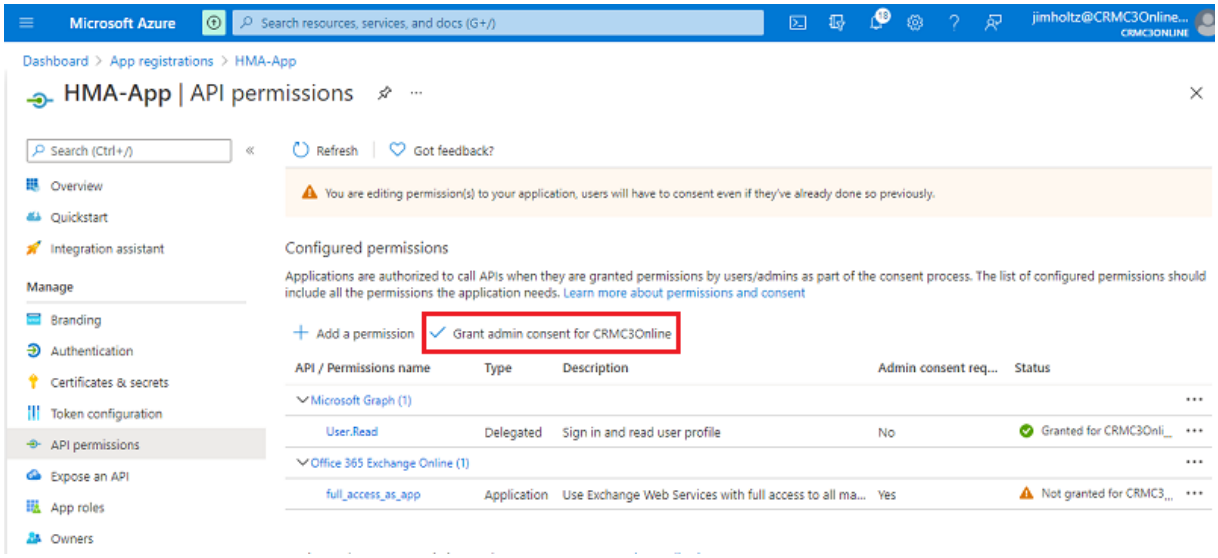


Die folgende Zustimmungsseite wird nach der ersten erfolgreichen Benutzeranmeldung angezeigt. Klicken Sie auf **Akzeptieren**.



Optional: Führen Sie die folgenden Schritte aus, um diese Zustimmungsseite nicht mehr zu erhalten:

- Öffnen Sie das Microsoft Azure-Portal.
- Navigieren Sie im Dashboard zu **App registrations > HMA-App**.
- Aktivieren Sie unter dem Abschnitt **Configured permissions** die Option **Grant admin consent for CRMC3Online**.



Einschränkungen

- Um von HMA zu einer Basisautorisierung zu wechseln, müssen Sie das bestehende Konto in Secure Mail löschen und dann ein neues Konto erstellen.
- Benutzer können sich nicht bei Secure Mail anmelden, wenn die MDX-Richtlinie und die Exchange-Richtlinie nicht übereinstimmen.

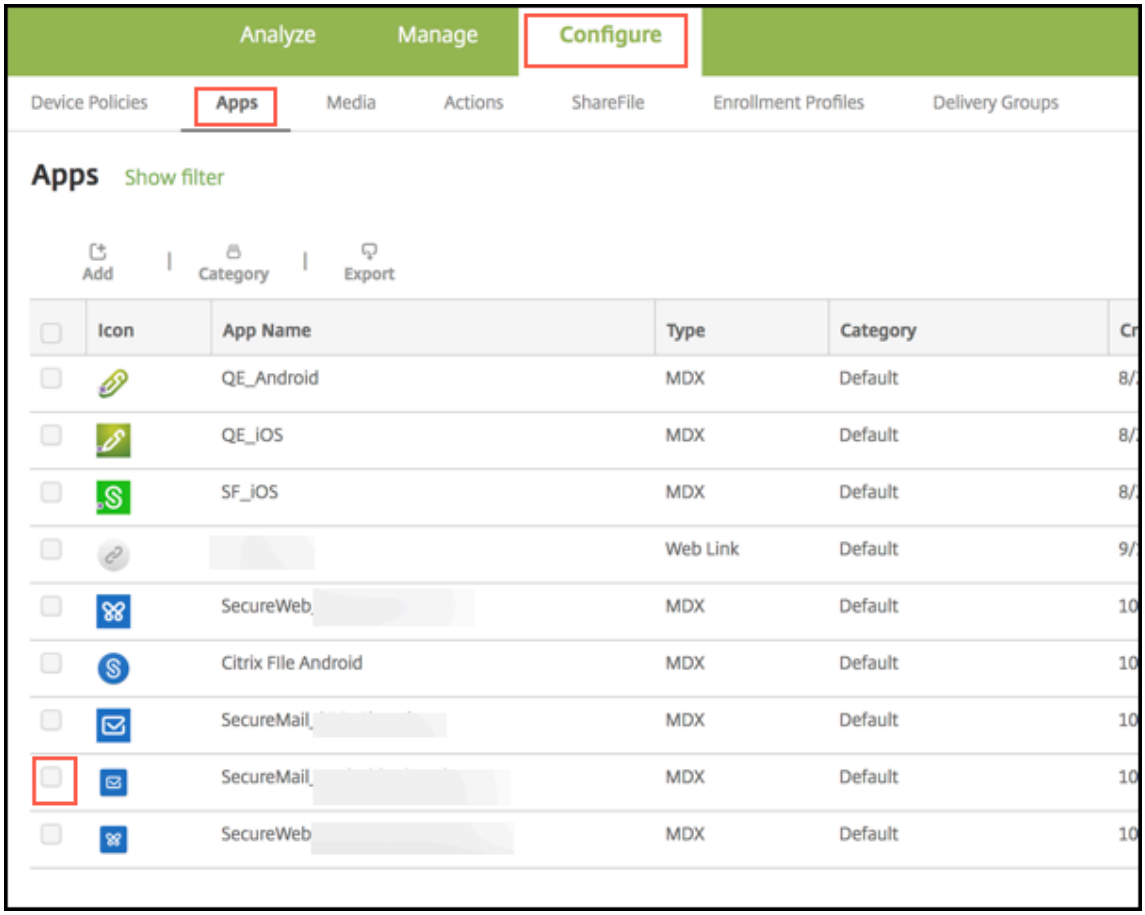
Hintergrunddienste für Secure Mail

February 28, 2024

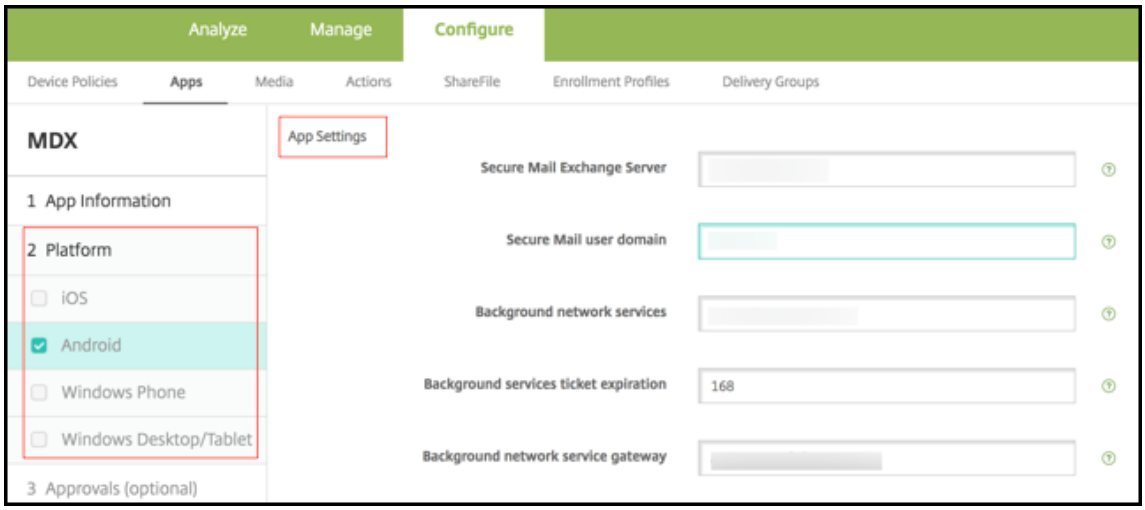
Für den Zugriff auf den E-Mail-Server über Citrix Gateway müssen Sie Hintergrunddienste für Secure Mail konfigurieren. Wenn Sie Secure Mail zu Citrix Endpoint Management (zuvor "XenMobile") hinzufügen, konfigurieren Sie Hintergrunddienste in MDX-App-Richtlinieneinstellungen.

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.

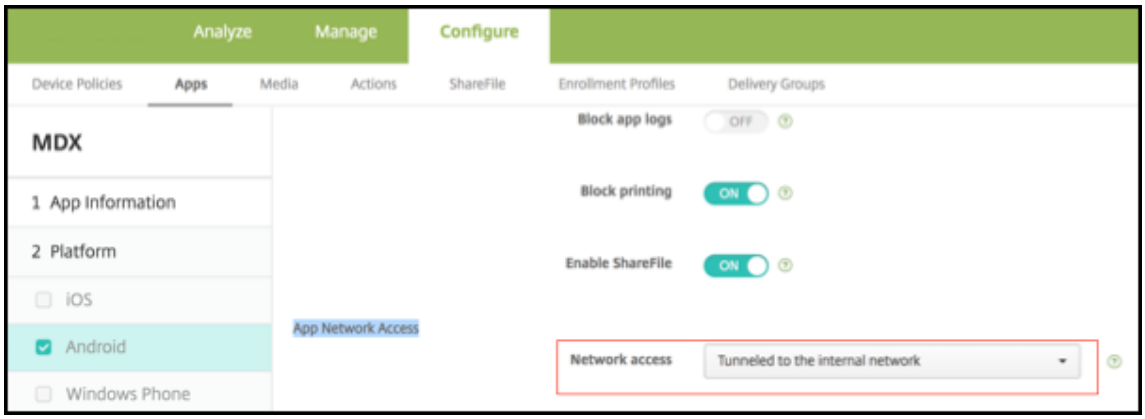


MDX-App-Richtlinien für die Konfiguration von Hintergrunddiensten

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`.

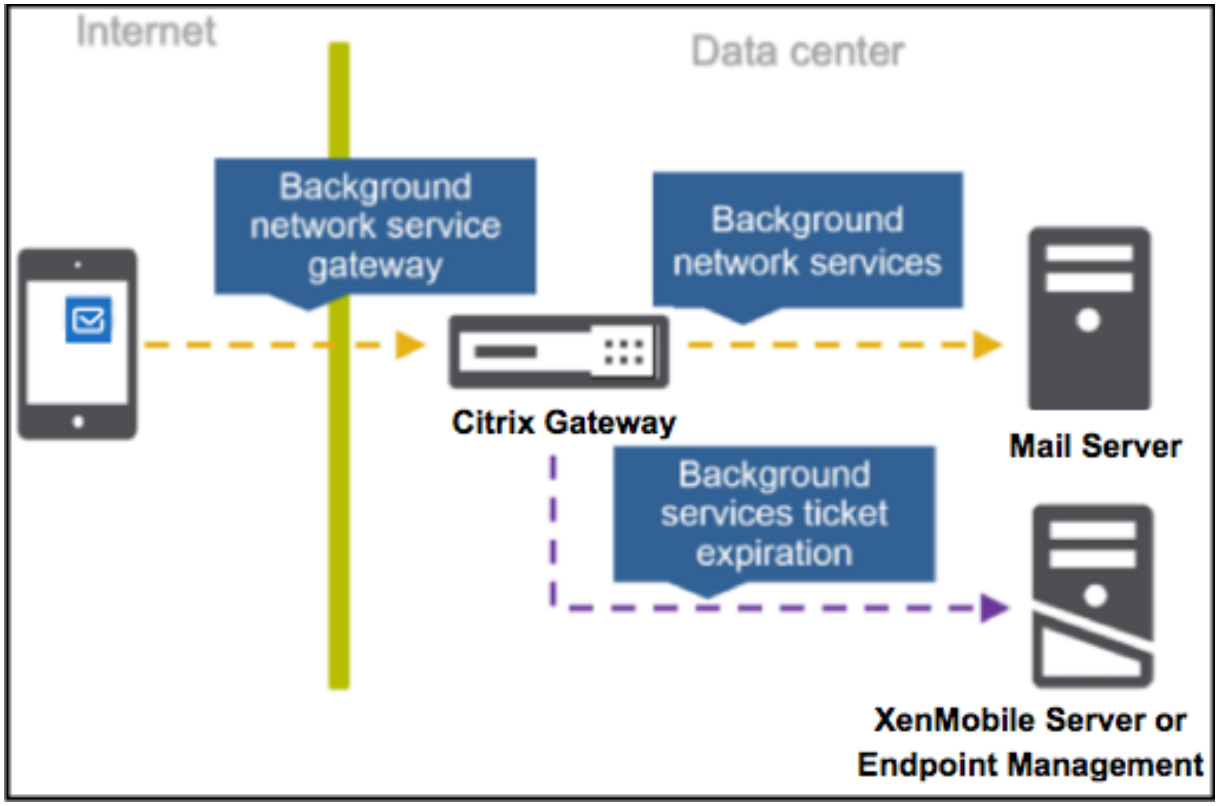
Ticketablauf für Hintergrunddienste: Mit dieser Richtlinie legen Sie die Gültigkeitsdauer des

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:

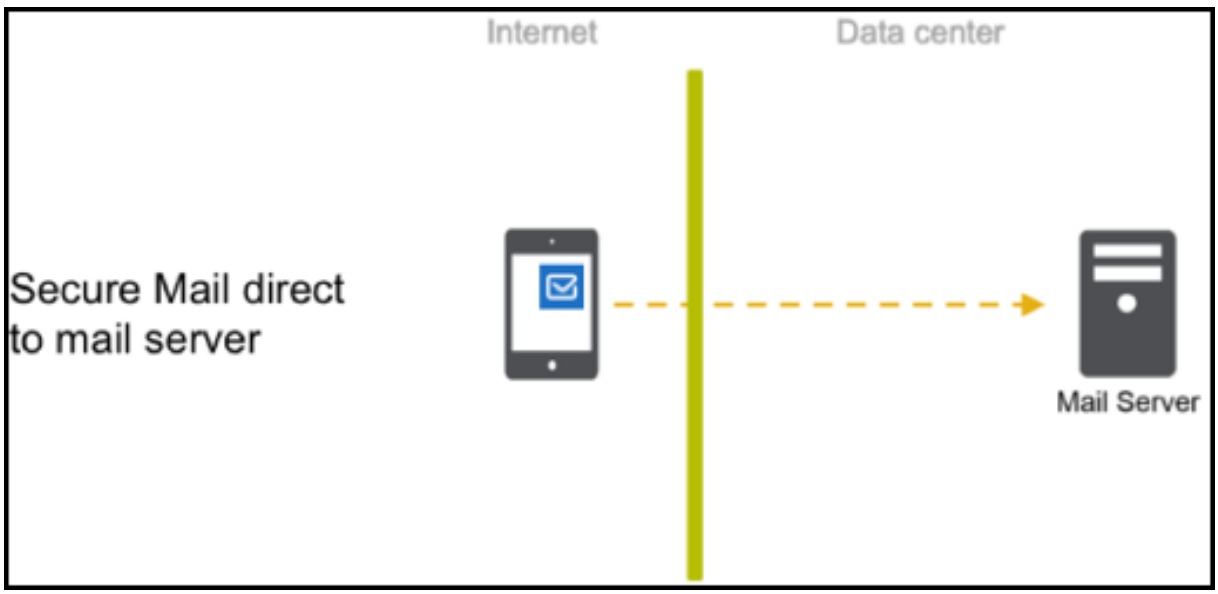
- Richtlinien für Secure Mail-App-Einstellungen für Android
- Richtlinien für Secure Mail-App-Einstellungen für iOS

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



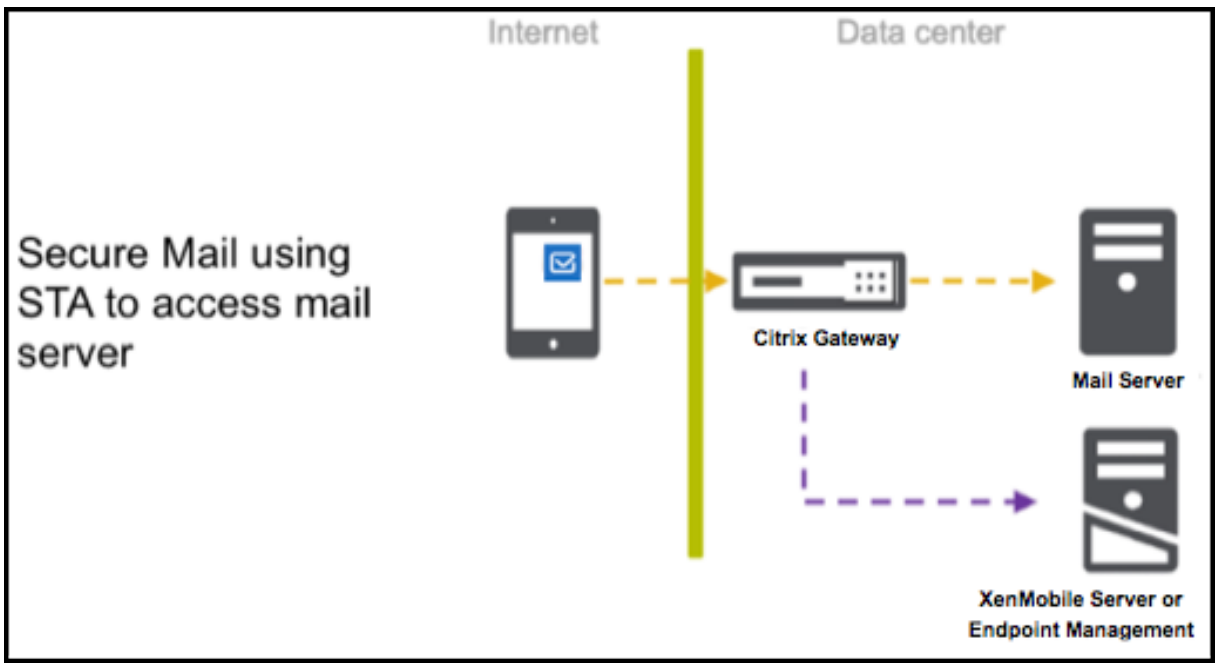
Richtlinien für eine direkte Verbindung mit einem Mailserver:

- 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 - Web-SSO**
- Hintergrundnetzwerkdienste: `mail.example.com:443,mail1.example1.com:443, outlook.office365.com:443 or vanity URL:443`
- Ticketablauf für Hintergrunddienste: **168**
- Gateway für Hintergrundnetzwerkdienst: `gateway3.example.com:443`

> Hinweis:
>
> Citrix empfiehlt die Verwendung einer STA-Verbindung für Secure Mail, da eine STA-Verbindung eine langlebige Sitzungsverbindung unterstützt.

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

Integration von Exchange Server oder IBM Notes Traveler-Server

February 28, 2024

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]

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

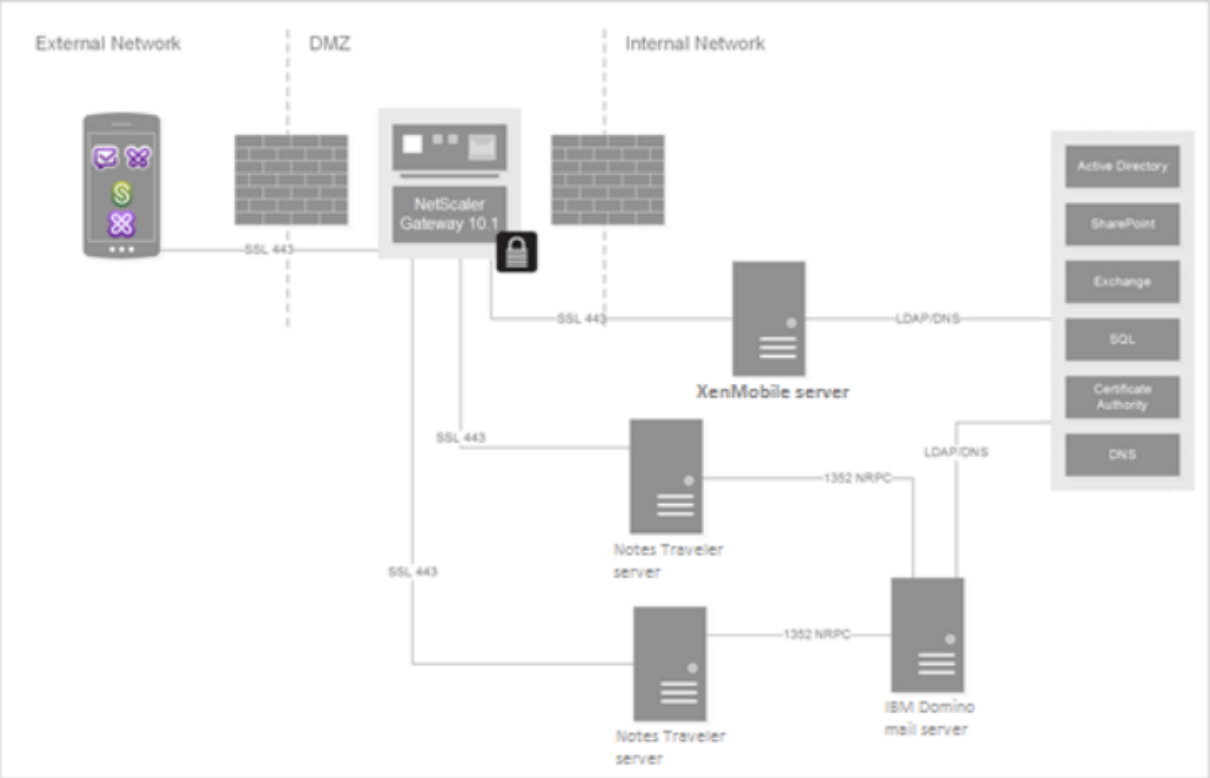
In IBM Notes-Umgebungen müssen Sie den IBM Notes Traveler-Server konfigurieren, bevor Sie Secure Mail bereitstellen. Dieser Abschnitt enthält eine Darstellung der Bereitstellung dieser Konfiguration und die Systemanforderungen.

> **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 9.0.1
- 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).

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

Betriebssystemtyp	SSLv3	TLS
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

February 28, 2024

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.

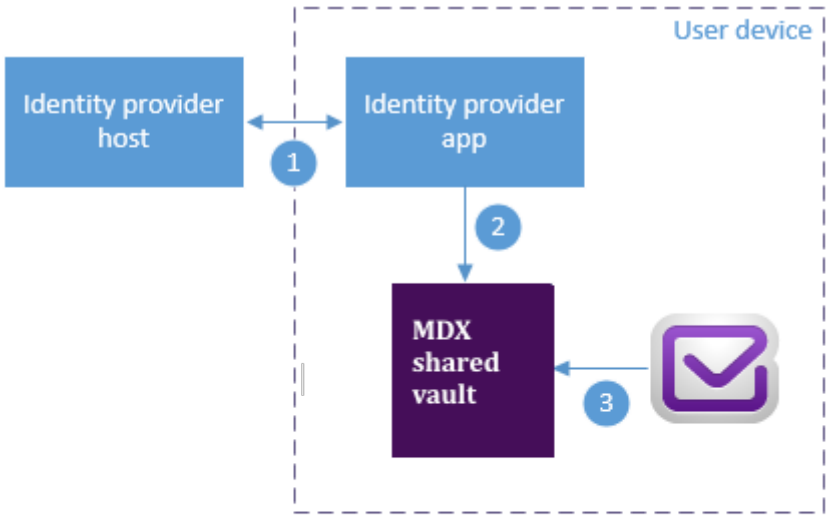
S/MIME-Feature	iOS	Android
Integration mit digitalen Identitätsanbietern: Sie können Secure Mail in einen unterstützten digitalen Identitätsanbieter (Drittanbietertool) integrieren. Der Identitätsanbieterhost stellt einer Identitätsanbieter-App auf Benutzergeräten Zertifikate zur Verfügung. Diese Anwendung 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	

S/MIME-Feature	iOS	Android
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 in der Citrix Endpoint Management-Dokumentation.	
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 Zertifikate per E-Mail verteilen.	X	X

S/MIME-Feature	iOS	Android
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 (Drittanbietertool) integrieren.



1. The identity provider host verifies user identity and sends certificates to the identity provider app on the client device
2. Using the Worx API, the identity provider app sends certificates to the shared vault.
3. Secure Mail gets certificate from the shared vault

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**.

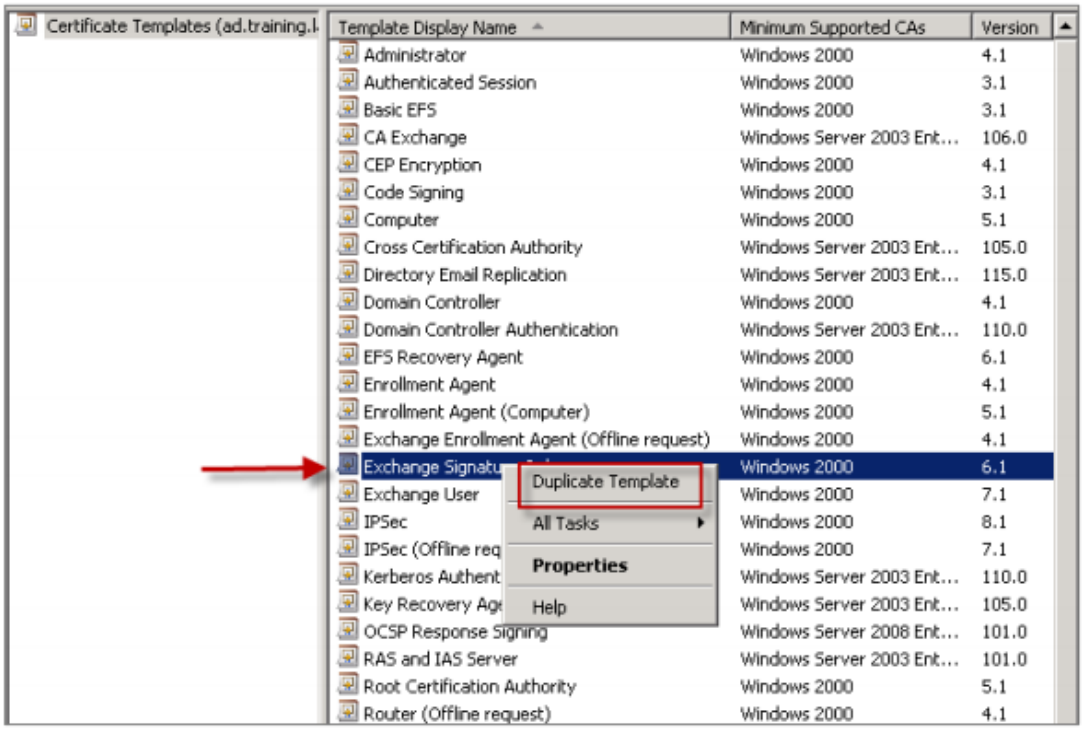
Erstellen von Zertifikatvorlagen

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:

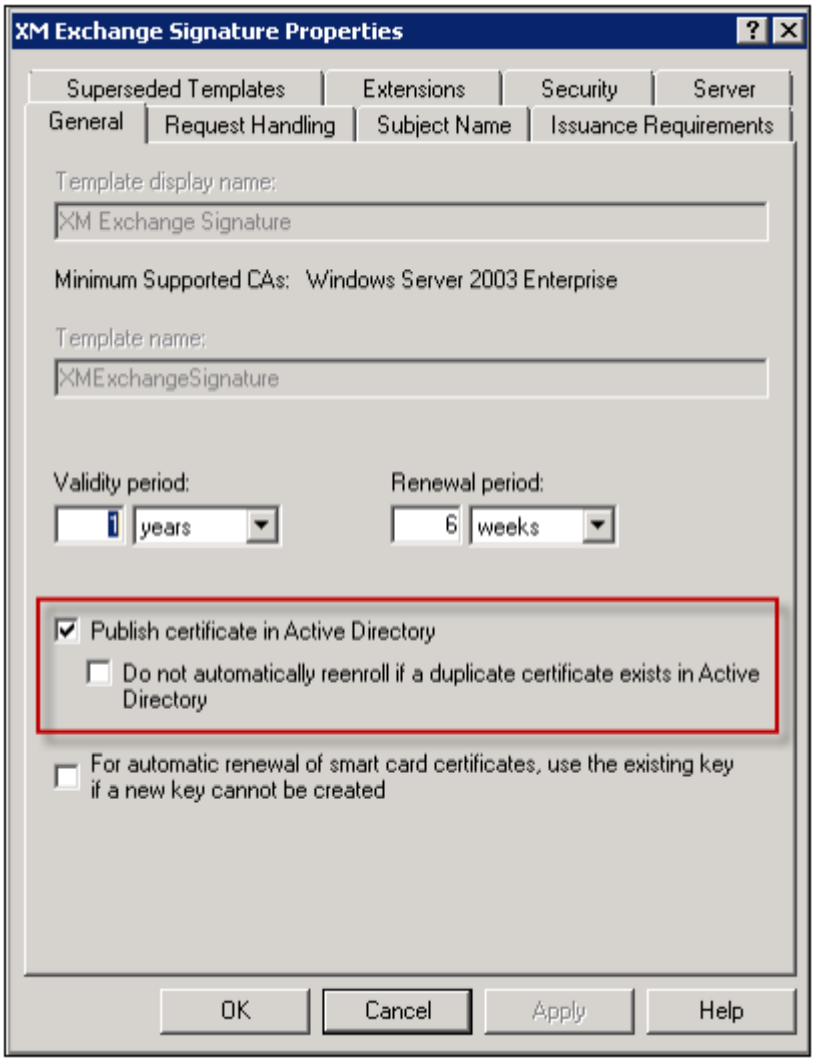
- Nur Exchange-Signatur (zum Signieren)
- Exchange-Benutzer (zur Verschlüsselung)

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**.



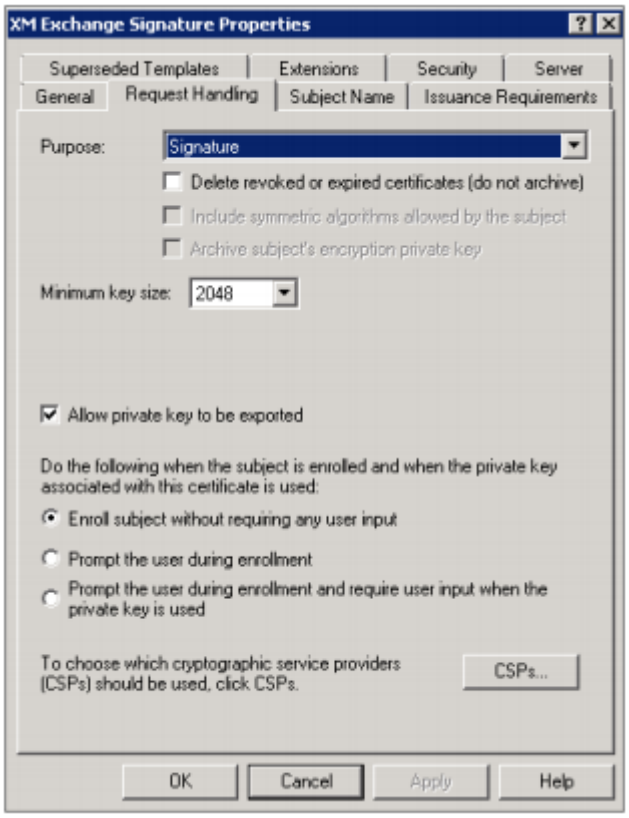
5. Weisen Sie einen Namen zu.
6. Aktivieren Sie das Kontrollkästchen für **Zertifikat in Active Directory veröffentlichen**.

> **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**.

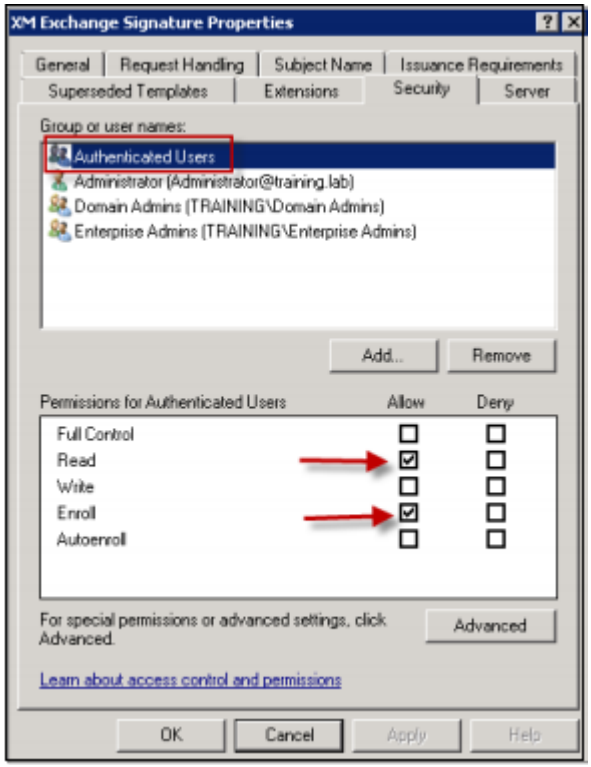


7. Klicken Sie auf die Registerkarte **Anforderungsverarbeitung** und legen Sie folgende Parameter fest:

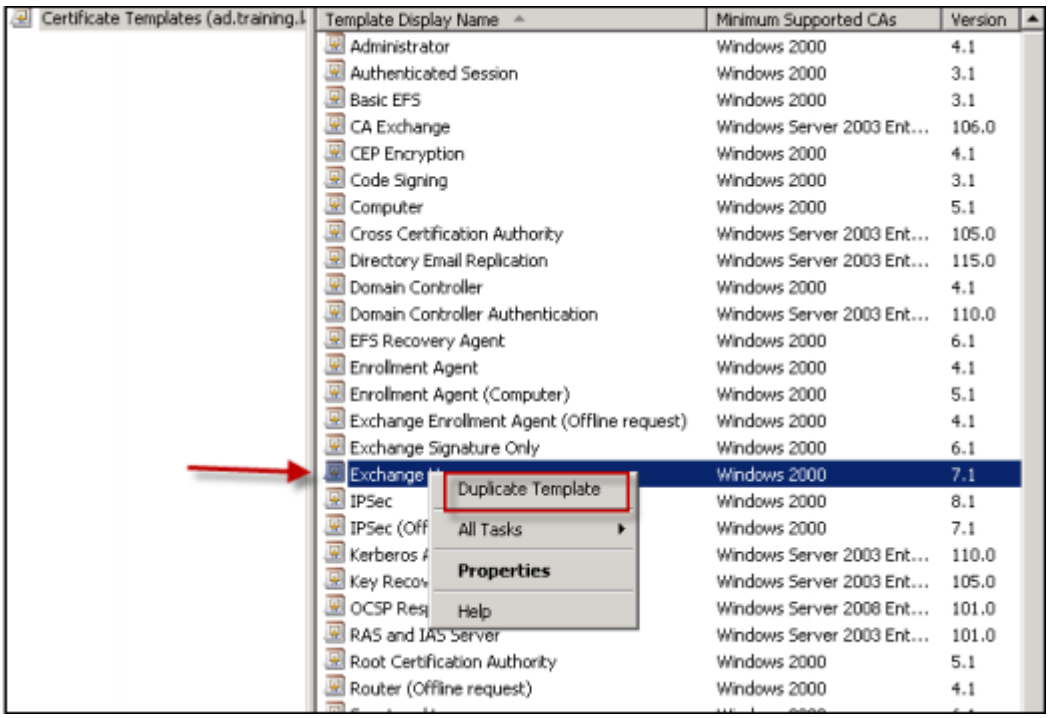
   - **Zweck:** Signatur
   - **Minimale Schlüsselgröße:** 2048
   - Kontrollkästchen **Exportieren von privatem Schlüssel zulassen** aktiviert
   - Kontrollkästchen **Antragsteller ohne Benutzereingabe registrieren** aktiviert



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.

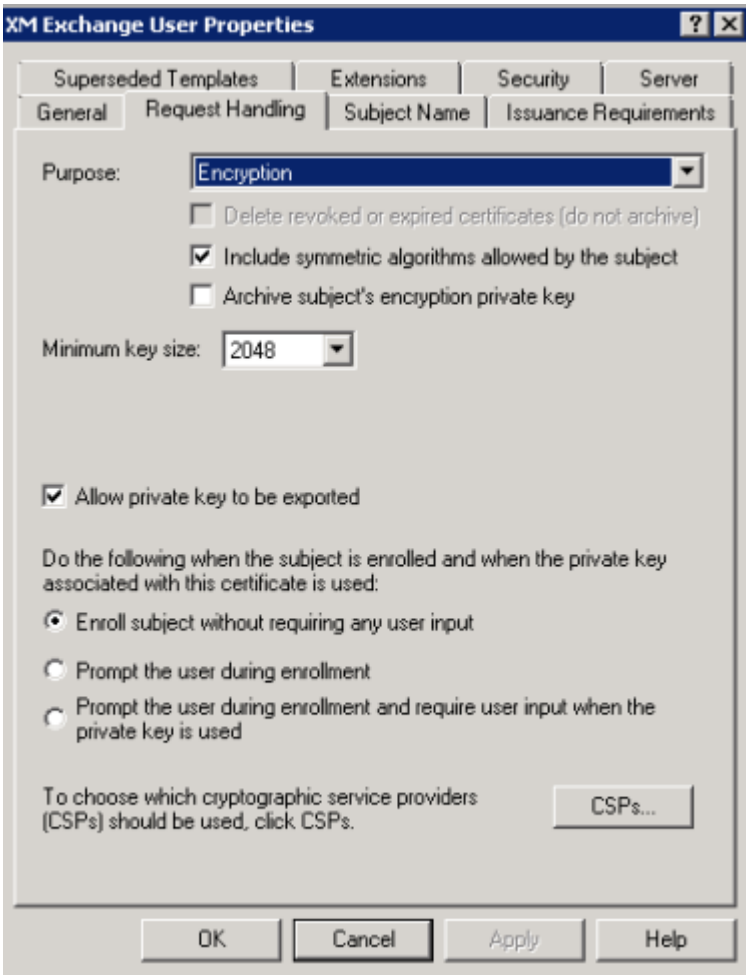


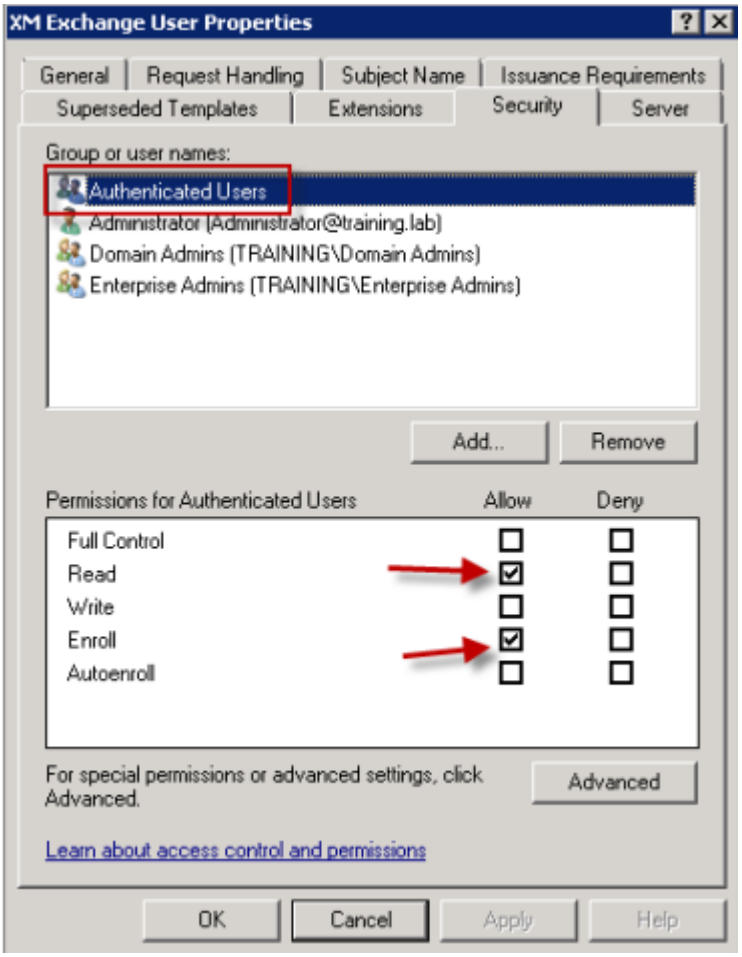
Verwenden Sie für die neue Exchange-Benutzervorlage die gleichen Standardeinstellungen wie

für die Originalvorlage.

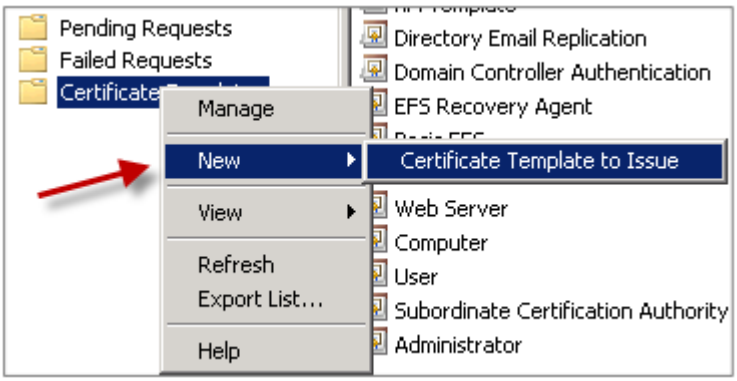
11. Klicken Sie auf die Registerkarte **Anforderungsverarbeitung** und legen Sie folgende Parameter fest:

    - **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

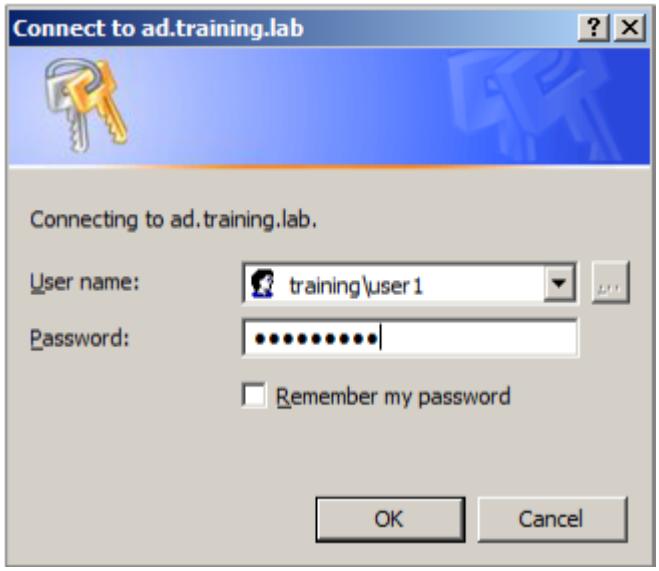
Bei dieser Vorgehensweise wird “User1”zum Navigieren zur Webregistrierungsseite, z. B. `https://ad.domain.com/certsrv/`, verwendet. Bei der Vorgehensweise werden zwei neue Benutzerzer-

tifikate 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.

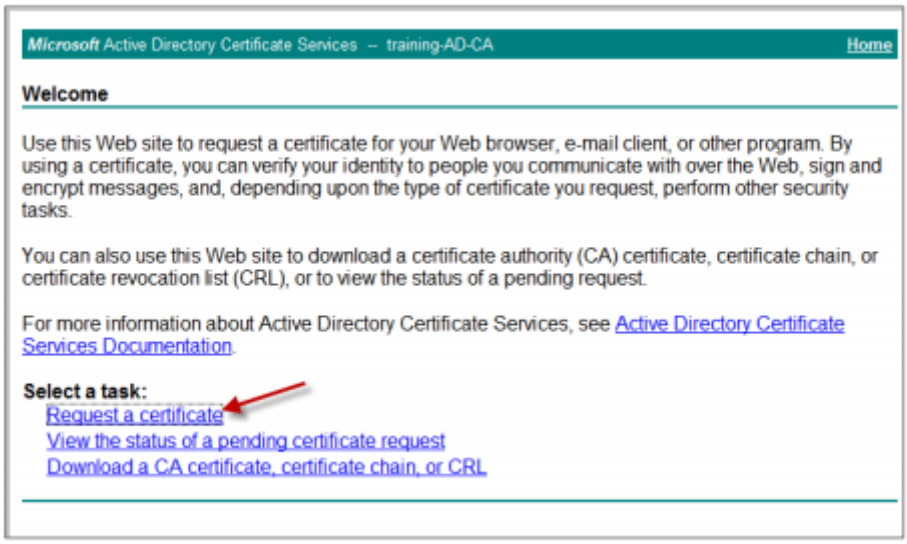
Zum Erstellen der Benutzerzertifikate für die Signierung und Verschlüsselung wird die manuelle Registrierung über die Webregistrierungssite (z. B. `https://ad.domain.com/certsrv/`) auf Microsoft-Zertifikatdienste verwendet. Eine Alternative wäre das Konfigurieren einer automatischen Registrierung über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

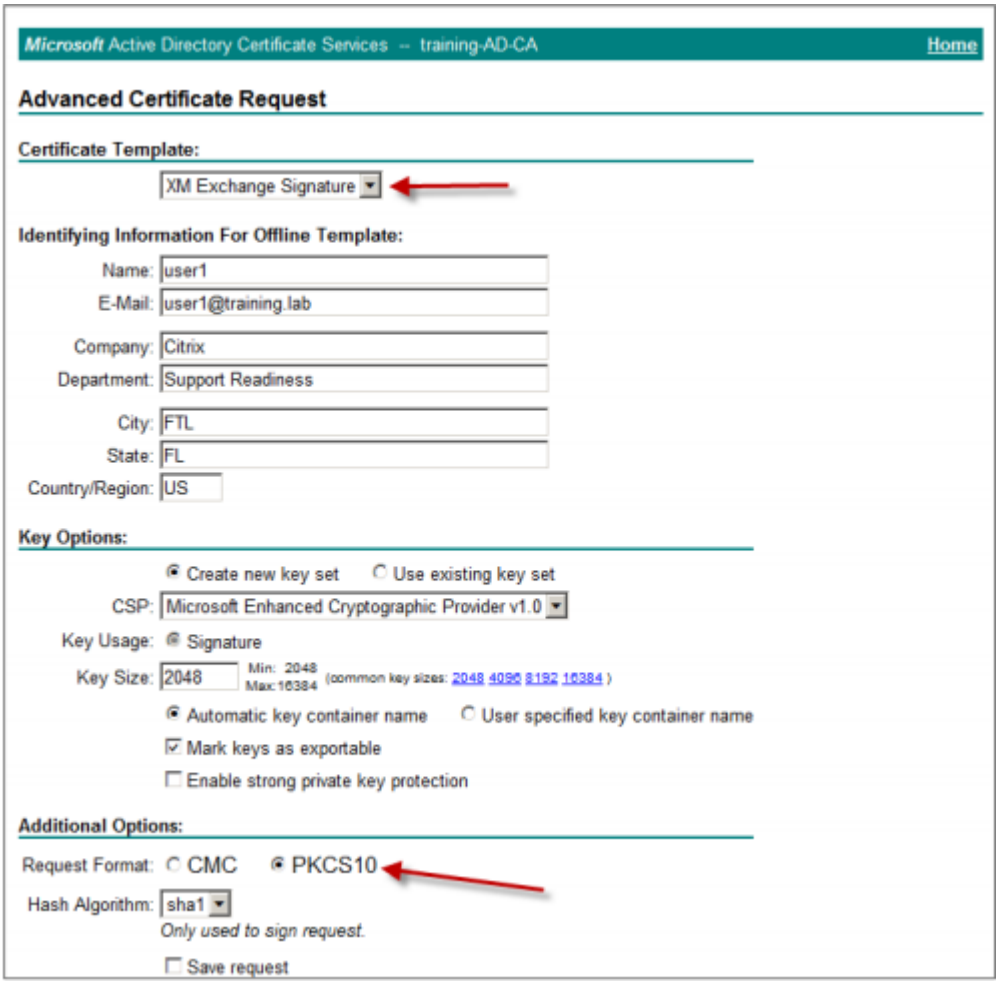


2. Wenn Sie angemeldet sind, klicken Sie auf **Zertifikat anfordern**.

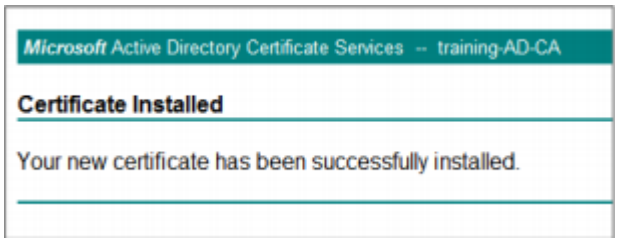


3. Klicken Sie auf **Erweiterte Zertifikatanforderung**.
4. Klicken Sie auf **Eine Zertifikatanforderung an diese Zertifizierungsstelle erstellen und einreichen**.
5. Erstellen Sie das Benutzerzertifikat zum Signieren. Wählen Sie den entsprechenden Vorlagennamen aus, geben Sie Ihre Benutzereinstellungen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

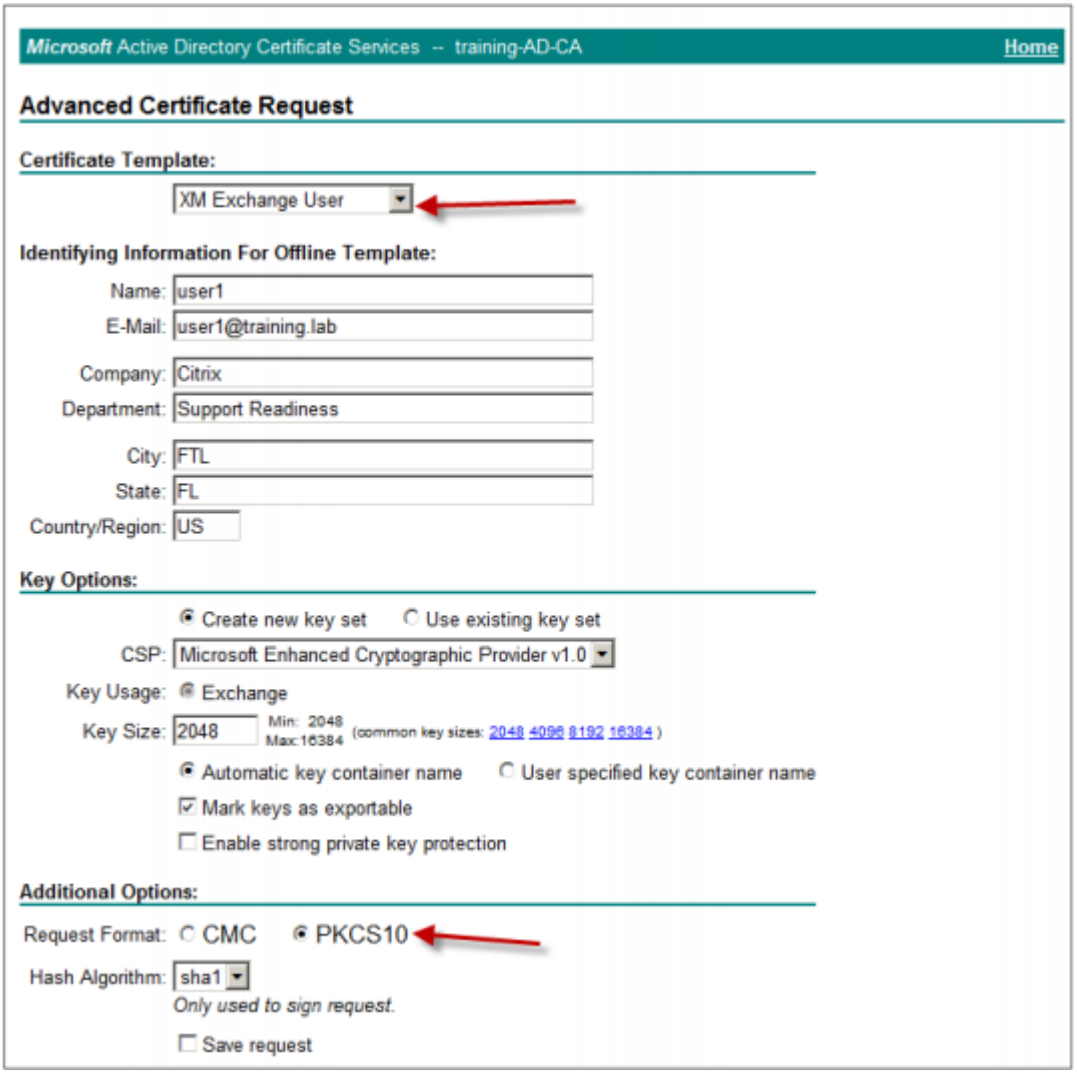
   Die Anforderung wurde gesendet.



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.

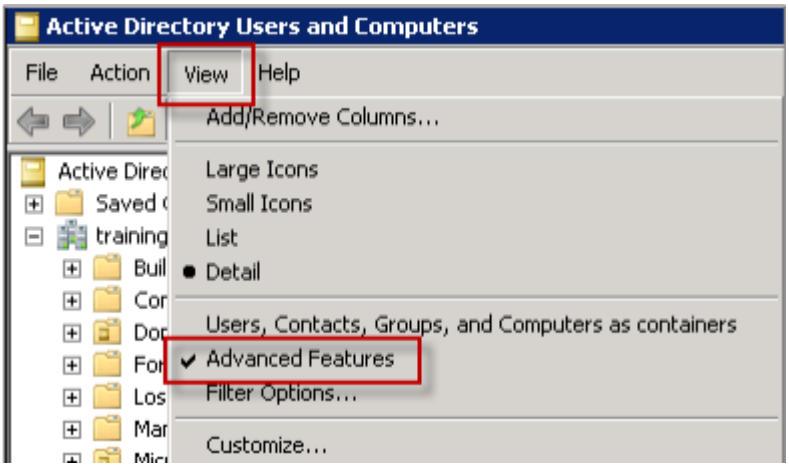


10. Stellen Sie sicher, dass das Zertifikat erfolgreich installiert wurde, und wiederholen Sie das Verfahren zum Erstellen eines Benutzerzertifikatpaars für einen weiteren Domänenbenutzer. Bei diesem Verfahren werden die gleichen Schritte ausgeführt und ein Zertifikatpaar für "User2" erstellt.

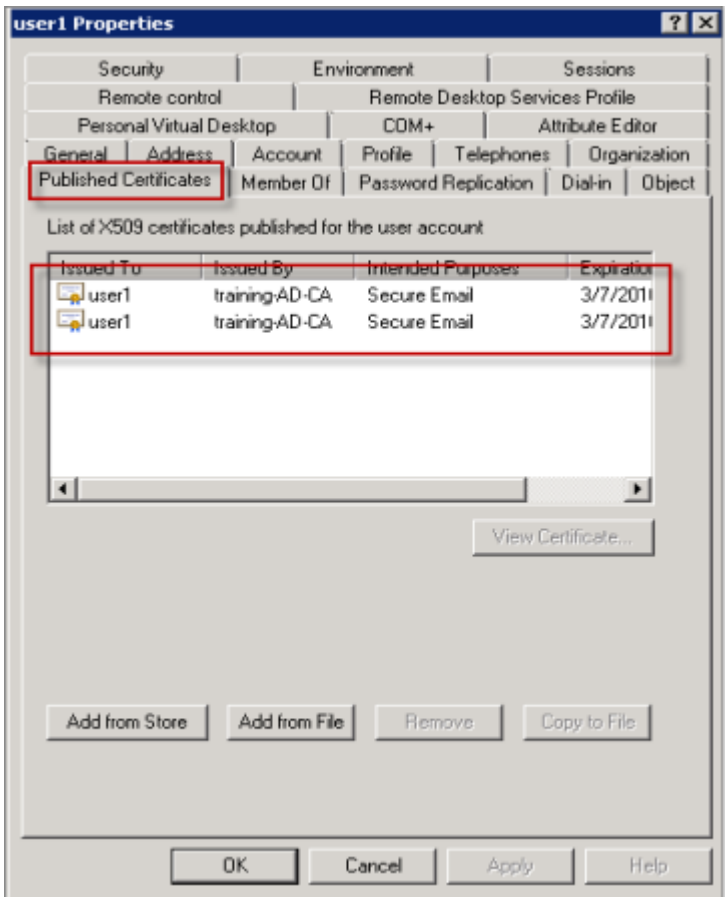
> **Hinweis:**
>
> Bei dem Verfahren wird der gleiche Windows-Computer zum Anfordern des zweiten Zertifikatpaars für "User2"verwendet.

Überprüfen veröffentlichter Zertifikate

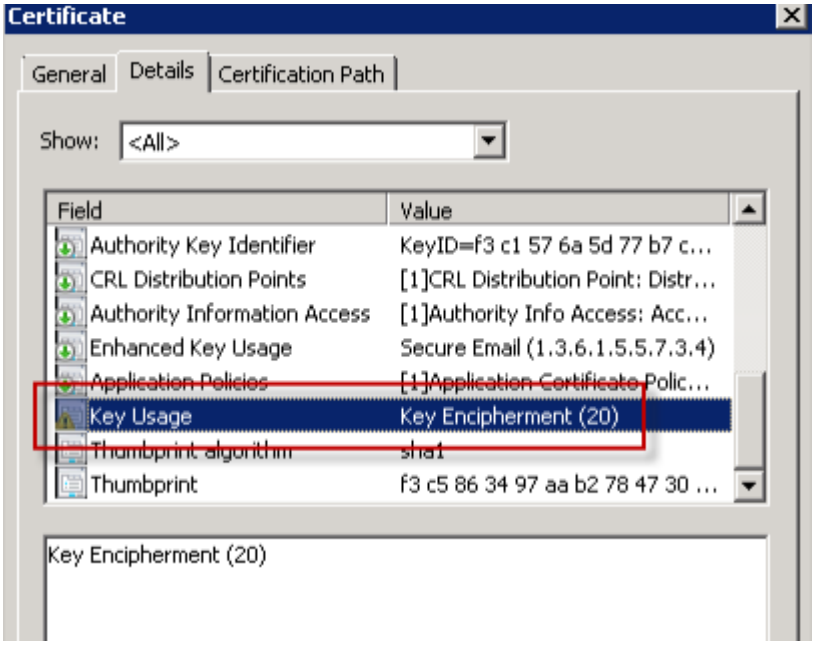
1. Um sich zu vergewissern, dass die Zertifikate im Domänenbenutzerprofil richtig installiert sind, wechseln Sie zu **Active Directory-Benutzer und -Computer > Anzeigen > Erweiterte Funktionen**.



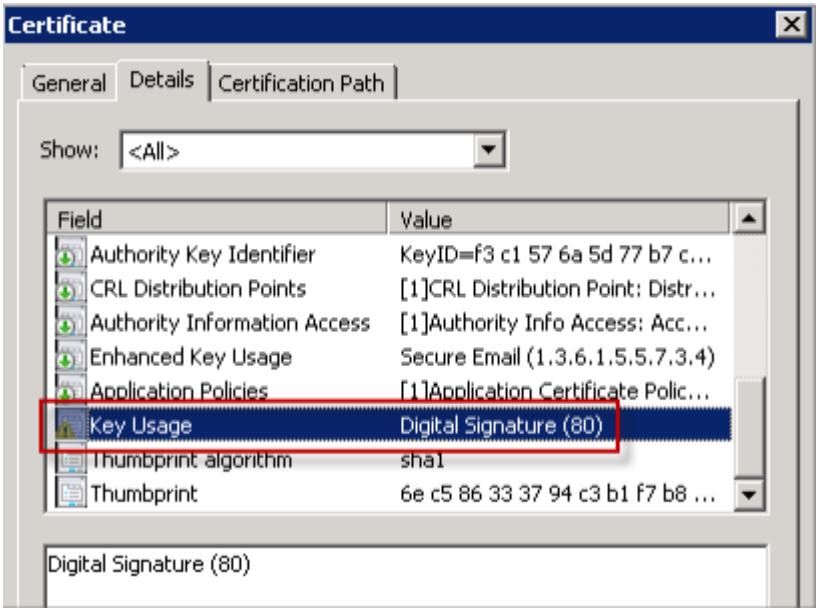
2. Wechseln Sie zu den Eigenschaften des Benutzers (User1 für dieses Beispiel) und klicken Sie dann auf die Registerkarte **Veröffentlichte Zertifikate**. Vergewissern Sie sich, dass beide Zertifikate verfügbar sind. Sie können auch sicherstellen, dass jedes Zertifikat einen bestimmten Zweck hat.



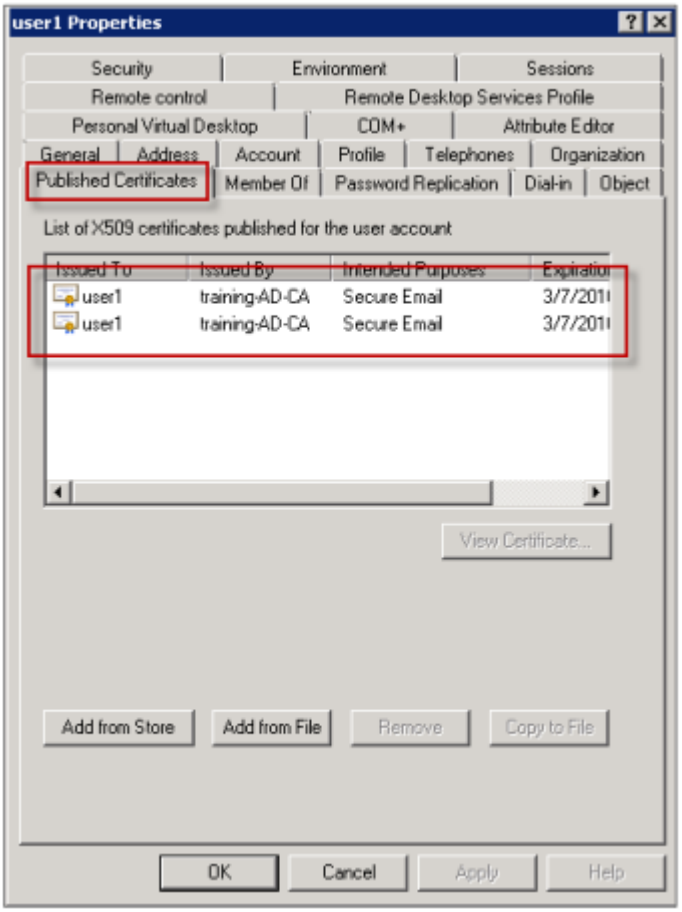
Diese Abbildung zeigt ein Zertifikat für die Verschlüsselung von E-Mail.



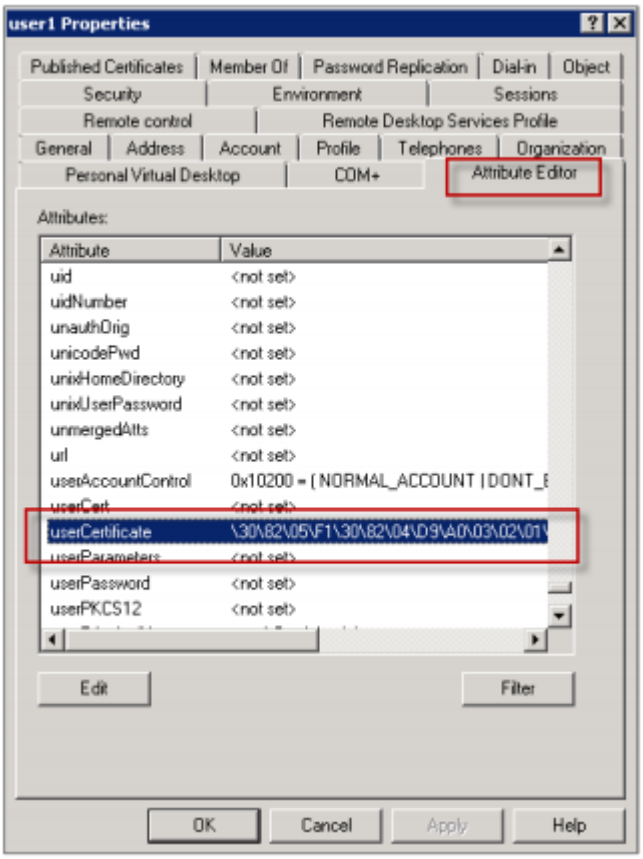
Diese Abbildung zeigt ein Zertifikat zum Signieren von E-Mail.



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



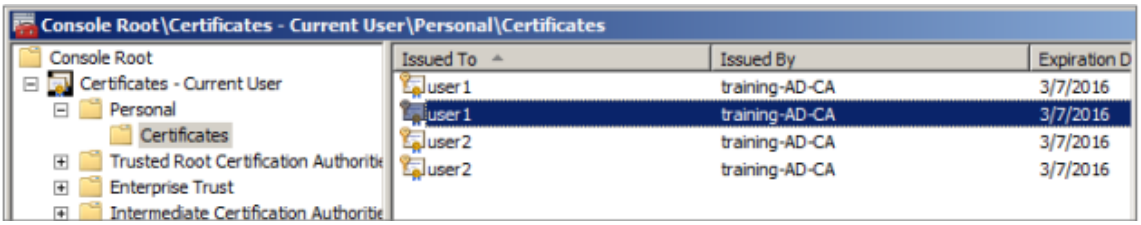
Secure Mail prüft das Benutzerobjektattribut userCertificate über LDAP-Abfragen. Sie können diesen Wert auf der Registerkarte **Attribut-Editor** ablesen. Wenn dieses Feld leer ist oder das falsche Benutzerzertifikat für die Verschlüsselung enthält, kann Secure Mail Nachrichten weder verschlüsseln noch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



Exportieren von Benutzerzertifikaten

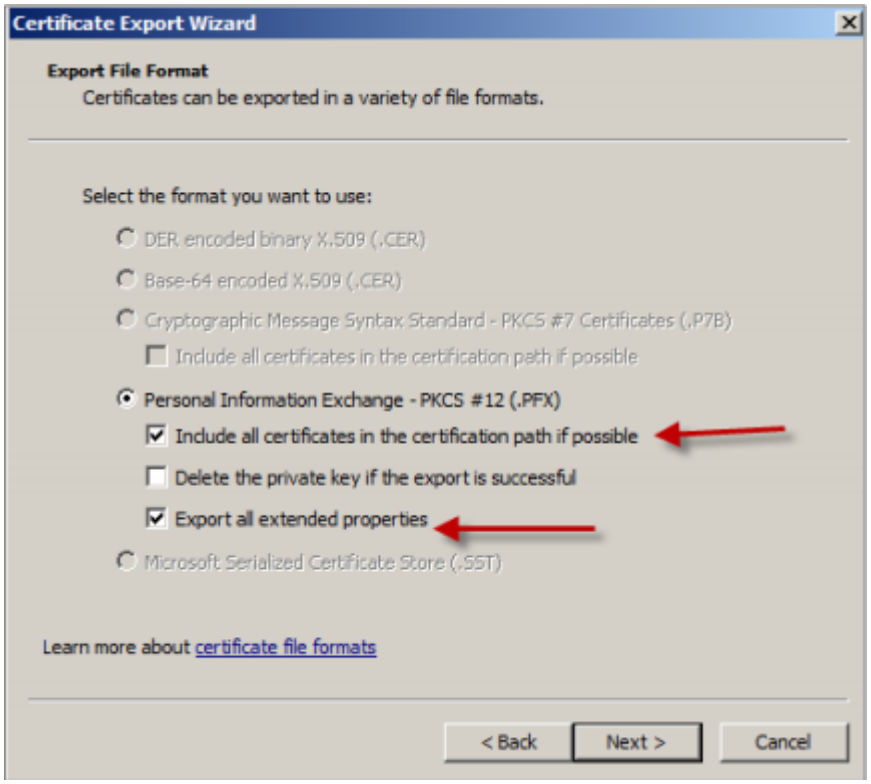
Mit diesem Verfahren werden die Zertifikatpaare für “User1”und “User2”im PFX-Format (PKCS #12) mit dem privaten Schlüssel exportiert. Nach dem Export werden die Zertifikate per E-Mail und unter Verwendung von Outlook Web Access (OWA) an den Benutzer gesendet.

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.



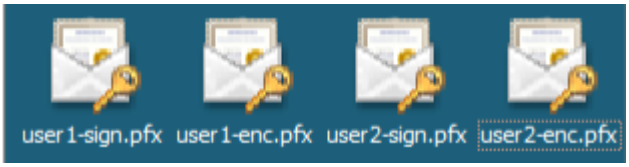
2. Klicken Sie mit der rechten Maustaste auf das Zertifikat und dann auf **Alle Aufgaben > Exportieren**.
3. Exportieren Sie den privaten Schlüssel durch Auswahl von **Ja, privaten Schlüssel exportieren**.

4. Aktivieren Sie die Kontrollkästchen **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen** und **Alle erweiterten Eigenschaften exportieren**.



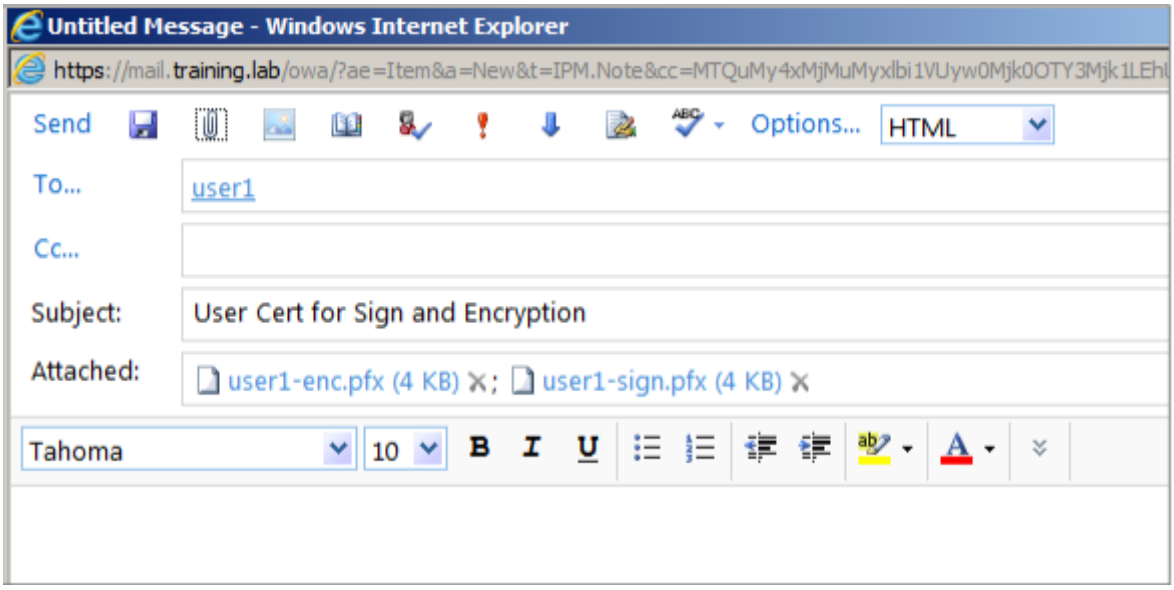
5. Wiederholen Sie beim Exportieren des ersten Zertifikats das gleiche Verfahren für die restlichen Zertifikate für die Benutzer.

> **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.



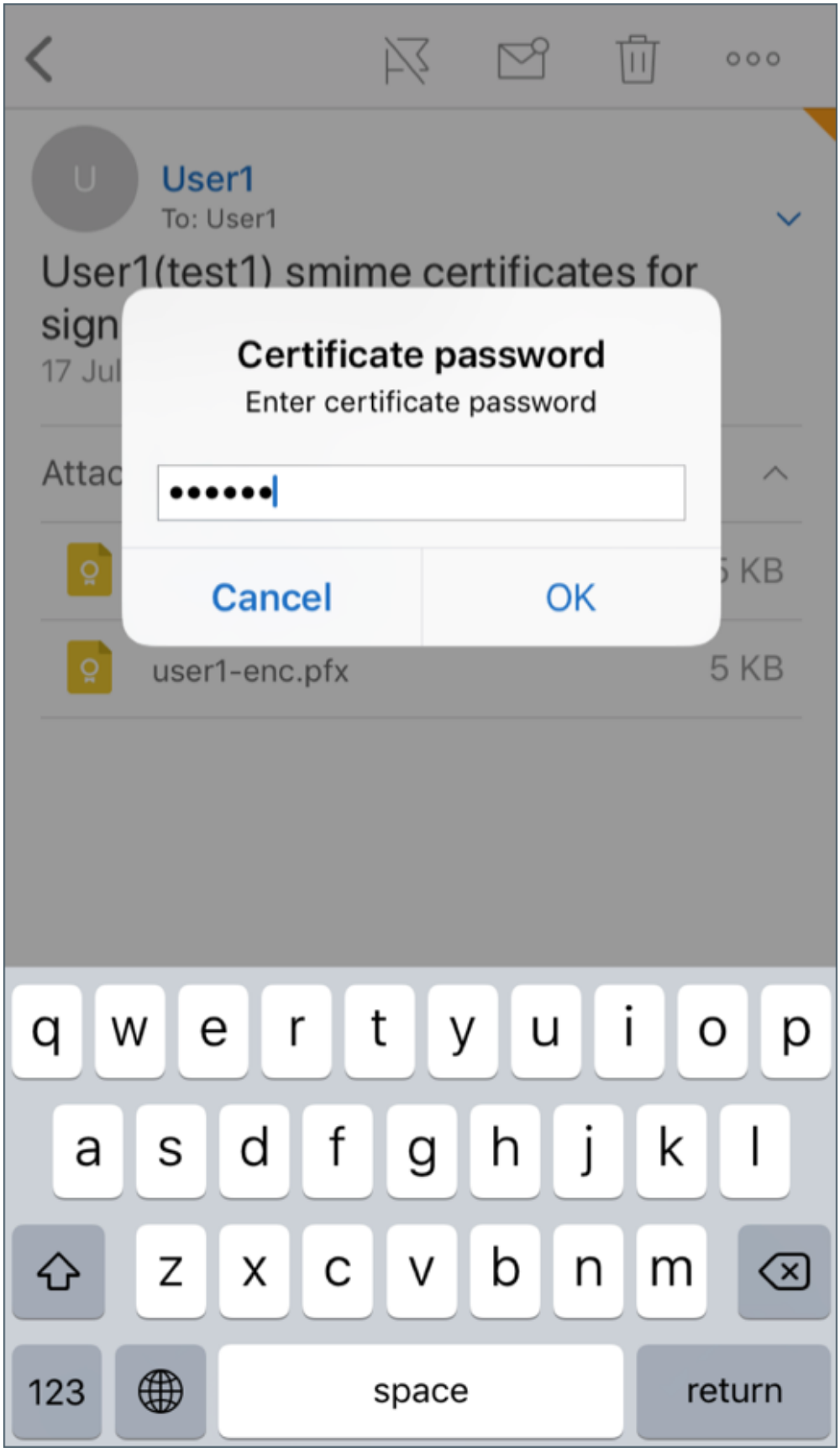
Wiederholen Sie diesen Vorgang für “User2”bzw. weitere Benutzer in der Domäne.

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.

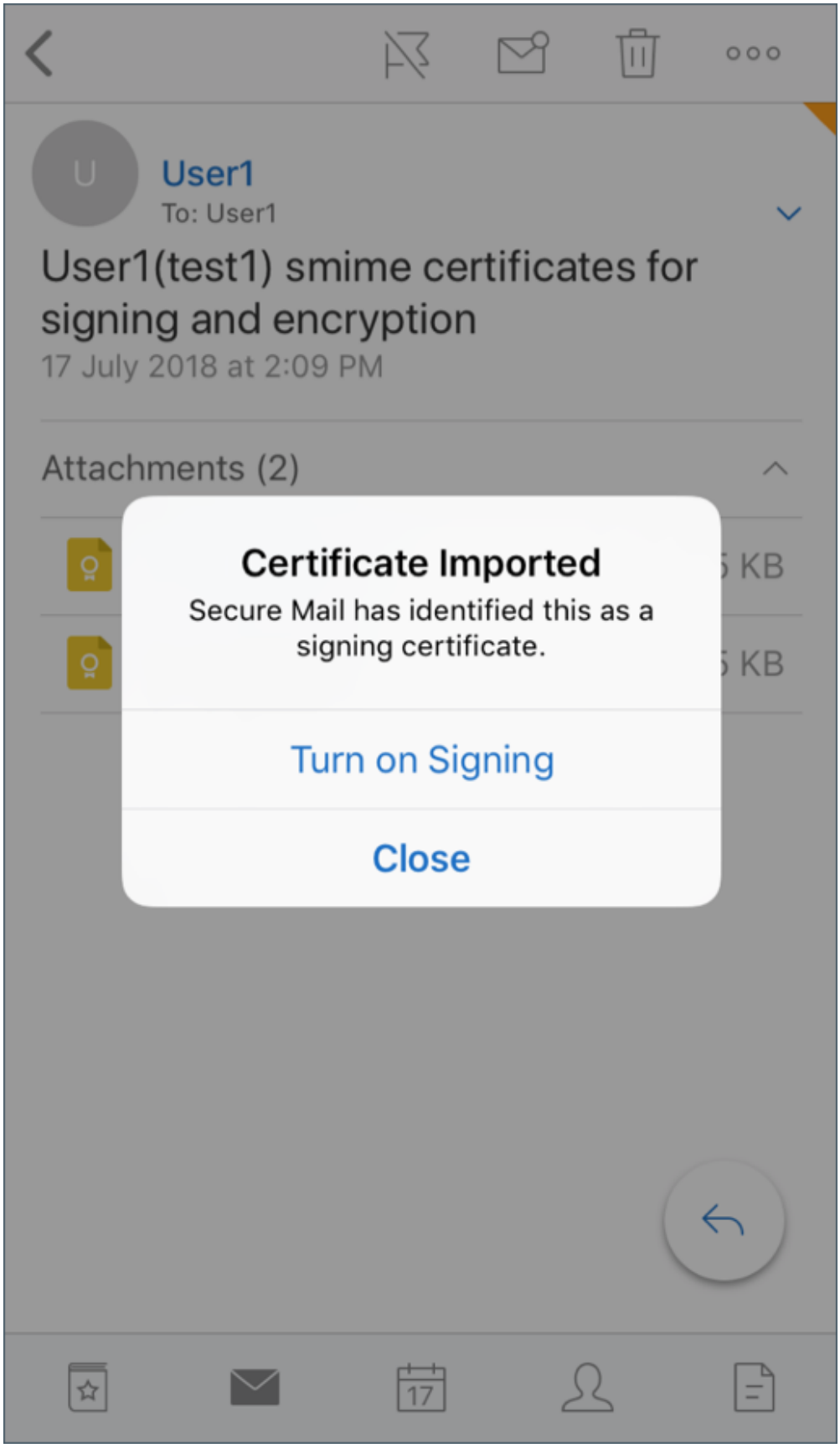
Aktivieren von S/MIME mit einzelnen Signatur- und Verschlüsselungszertifikaten

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.

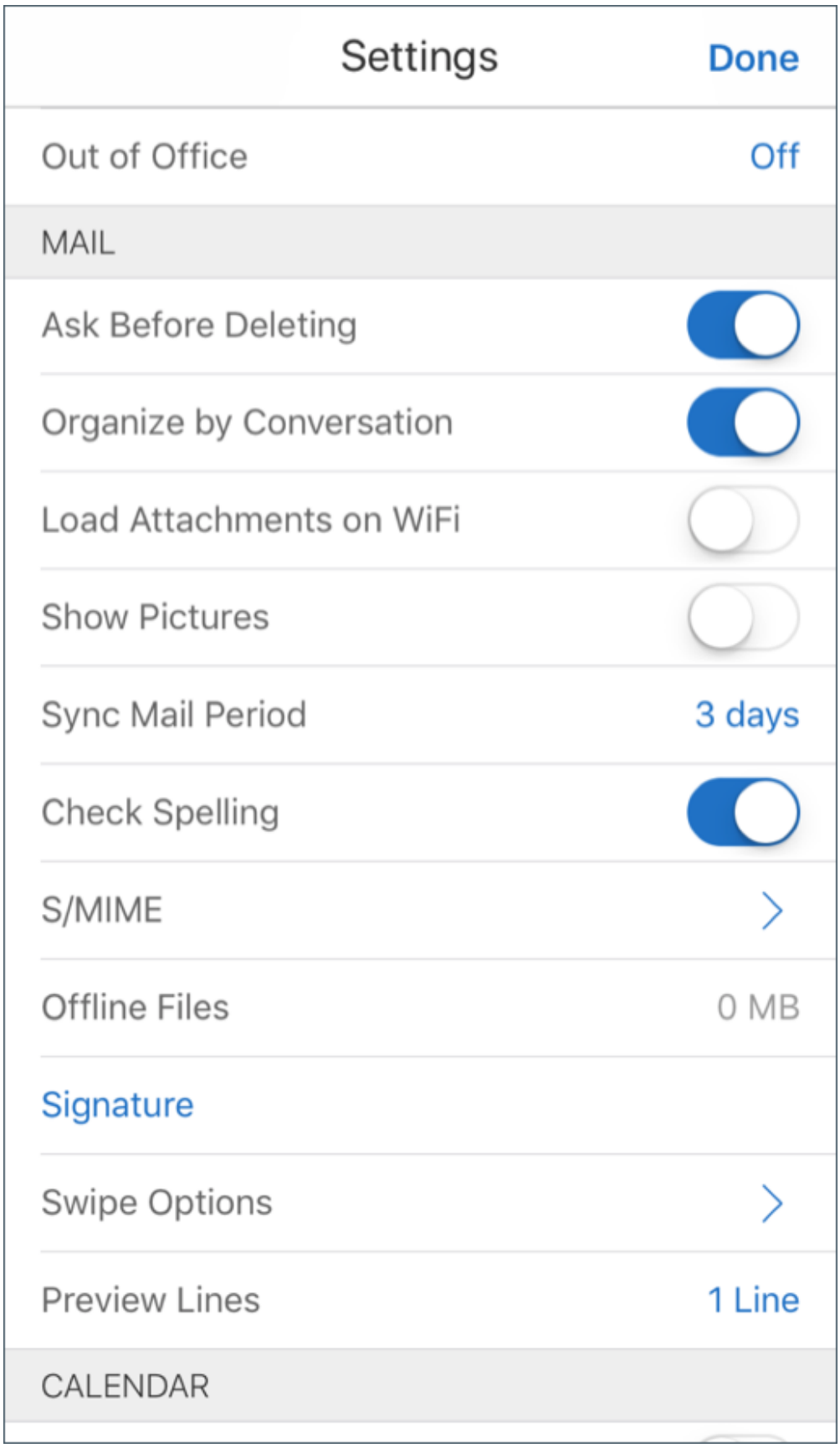


Ihr Zertifikat wurde importiert.

4. Tippen Sie auf **Signatur aktivieren**

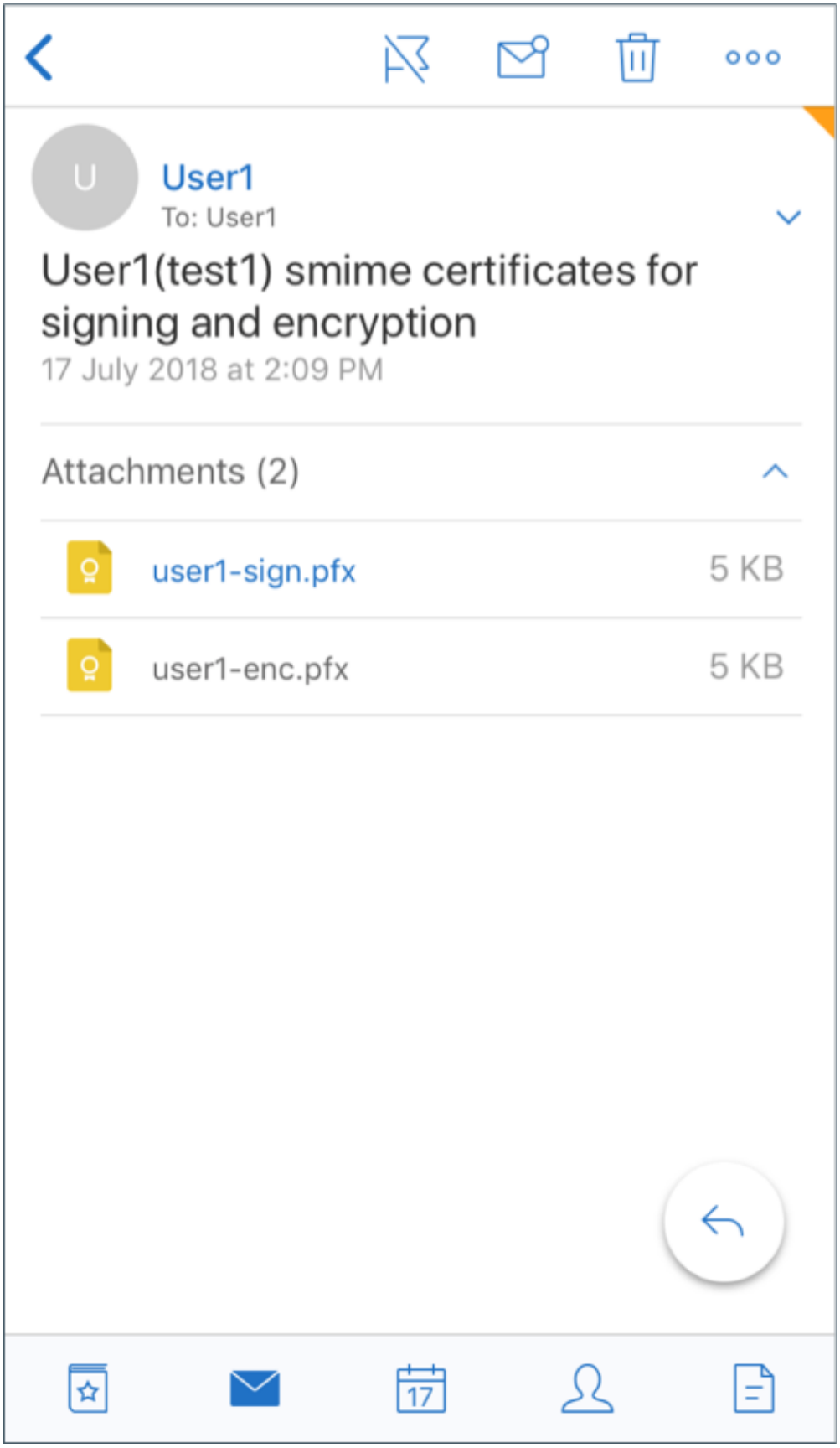


5. Alternativ dazu können Sie auch zu **Einstellungen** > **S/MIME** navigieren und auf “S/MIME”tippen, um das Signaturzertifikat zu aktivieren.

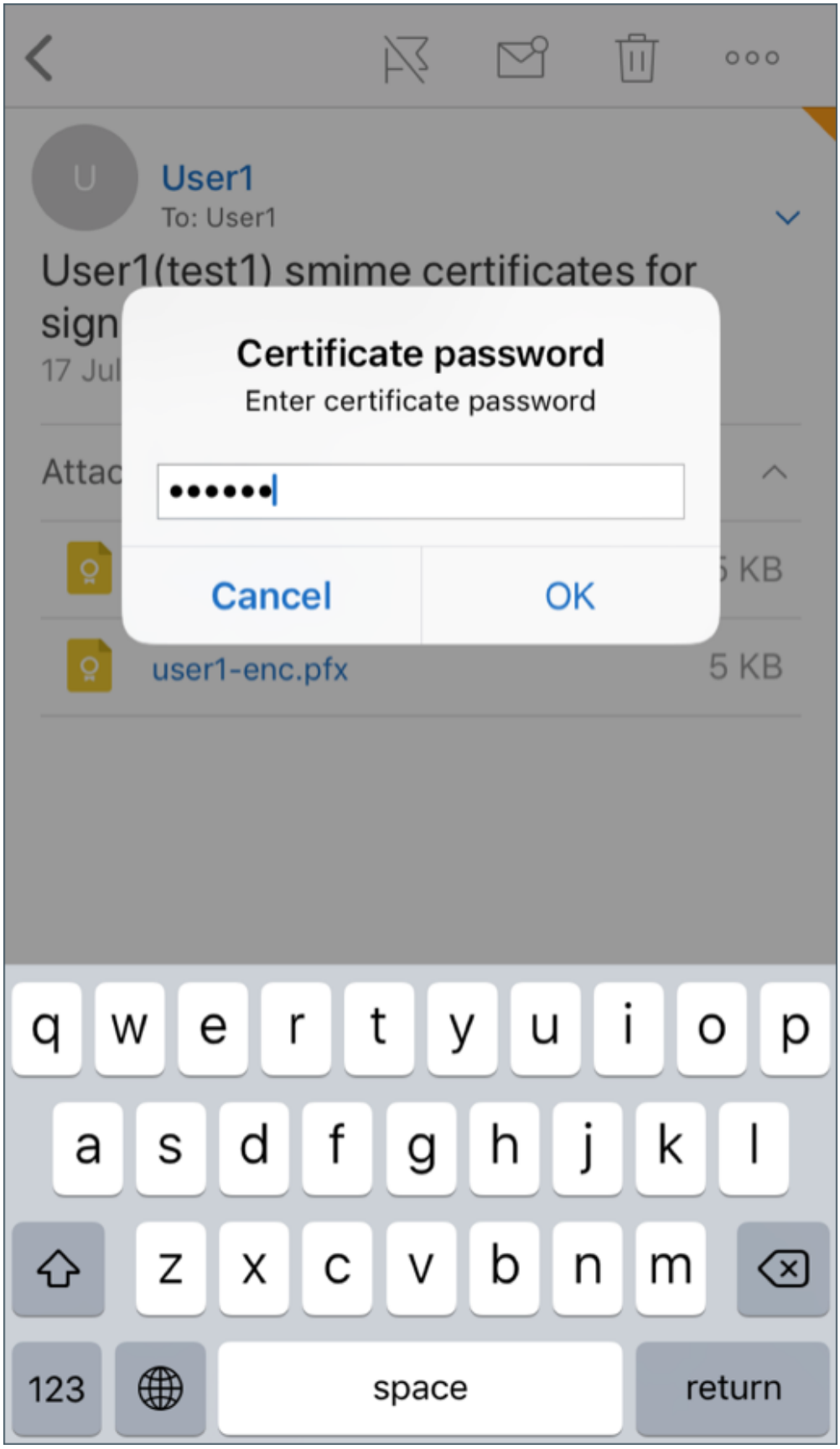


6. Stellen Sie im Bildschirm **Signieren** sicher, dass das richtige Signaturzertifikat importiert wurde.

7. Wechseln Sie zurück zu der E-Mail und tippen Sie auf das Verschlüsselungszertifikat, das heruntergeladen und importiert werden soll.

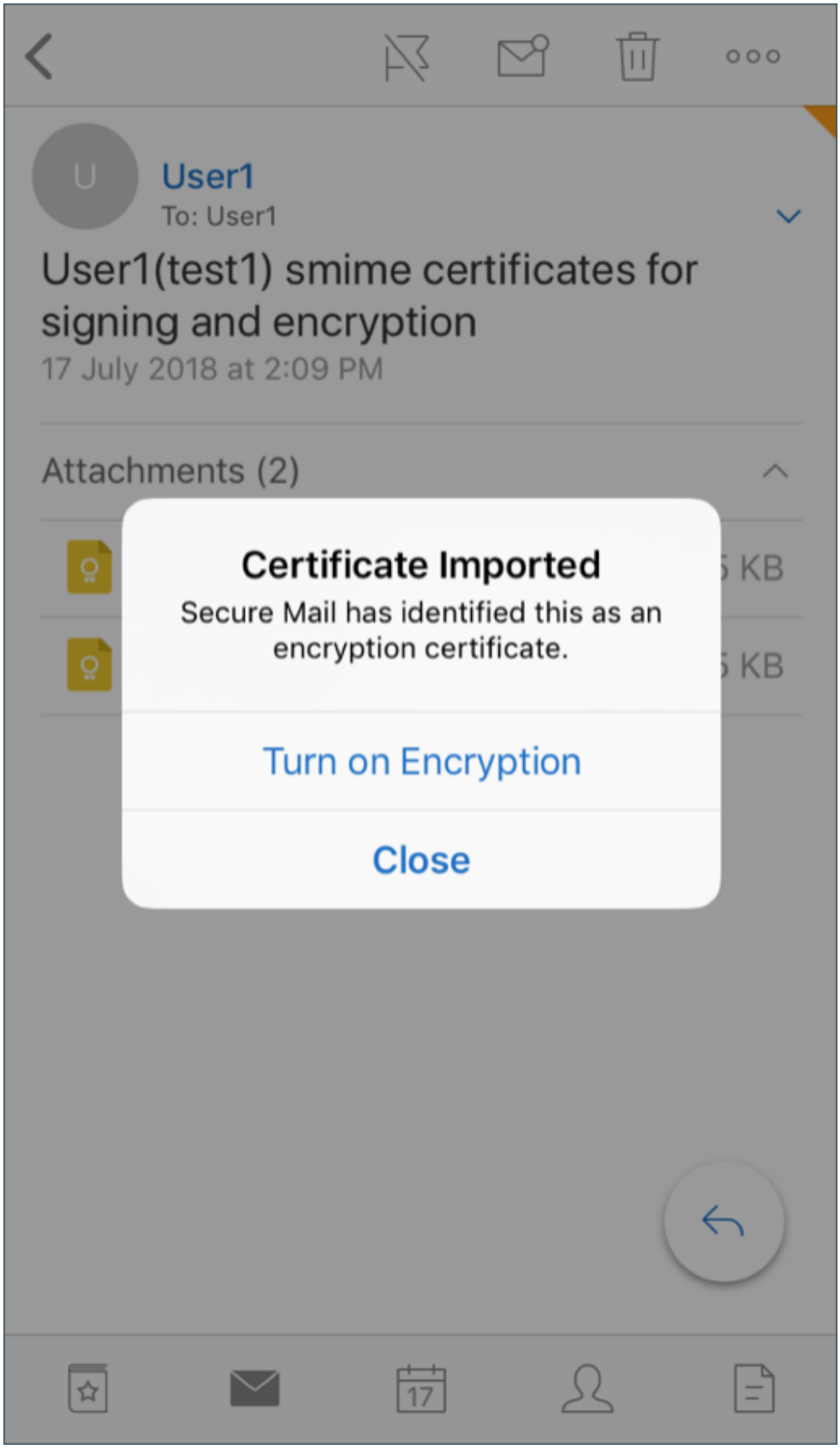


8. Geben Sie das dem privaten Schlüssel zugewiesene Kennwort ein, wenn das Verschlüsselungszertifikat vom Server exportiert wurde.

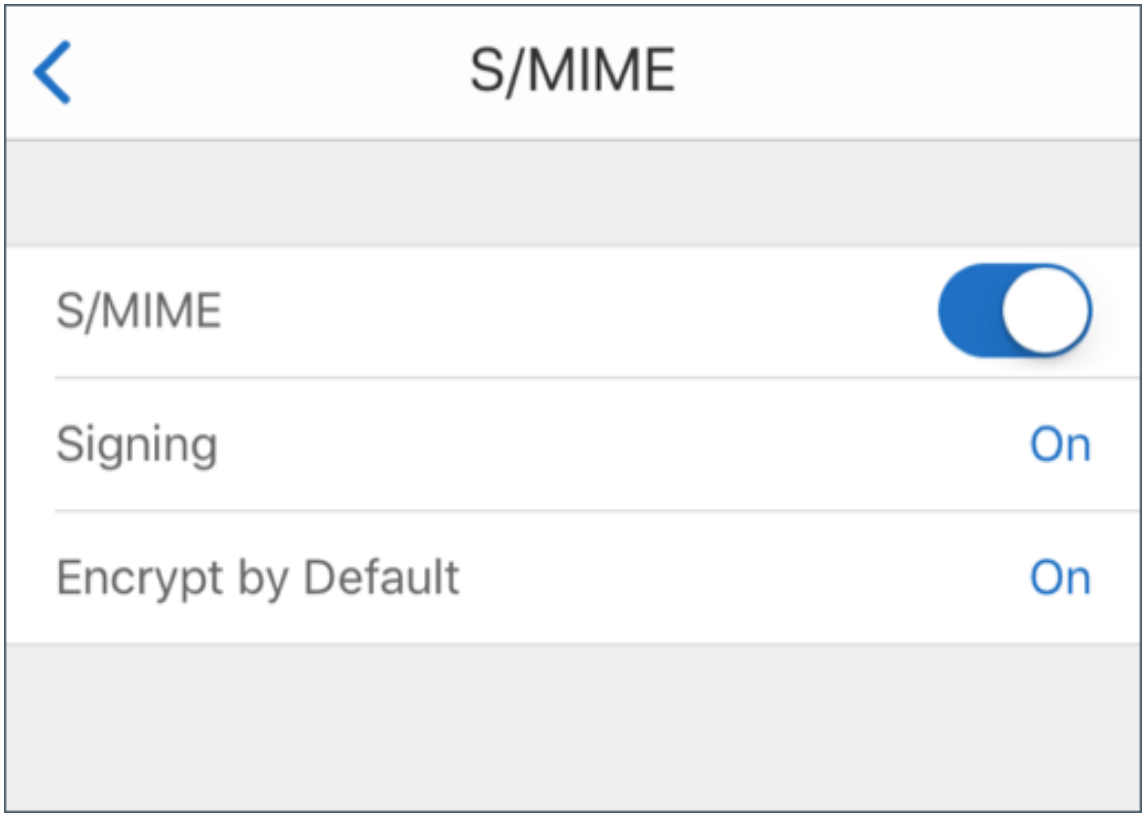


Ihr Zertifikat wurde importiert.

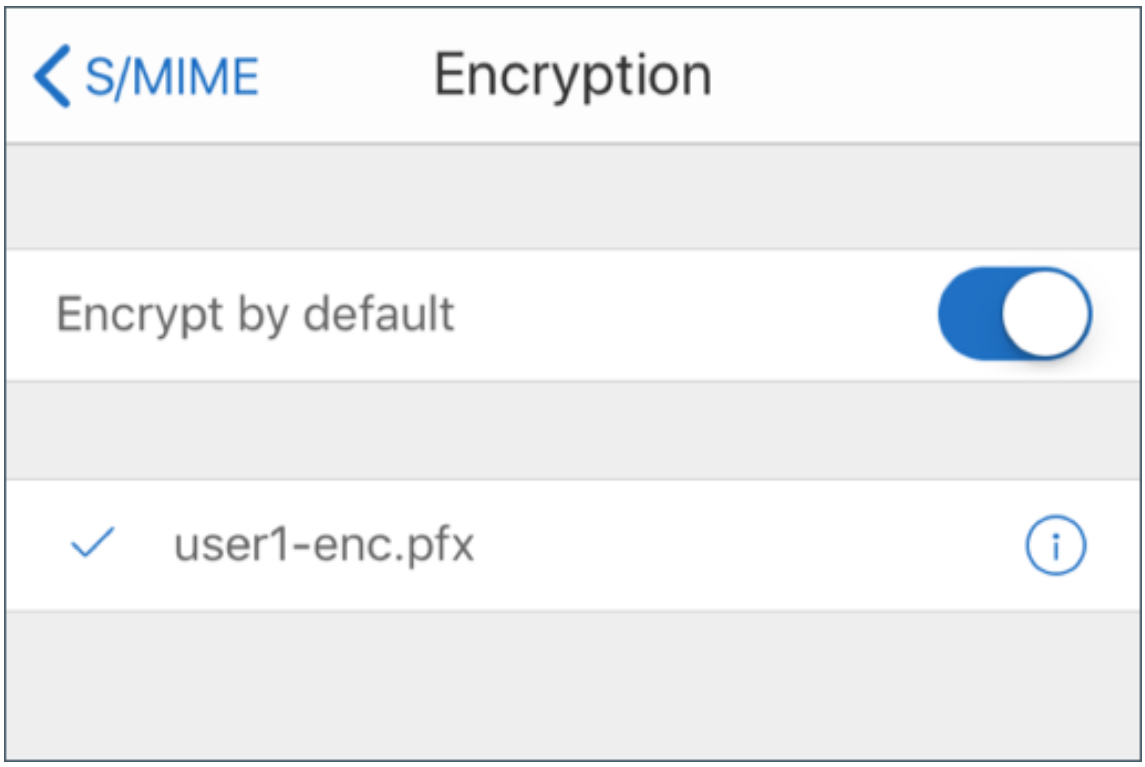
9. Tippen Sie auf **Verschlüsselung aktivieren**



10. Alternativ dazu können Sie auch zu **Einstellungen** > **S/MIME** navigieren und auf “S/MIME”tippen, um die Option **Standardmäßig verschlüsseln** zu aktivieren.



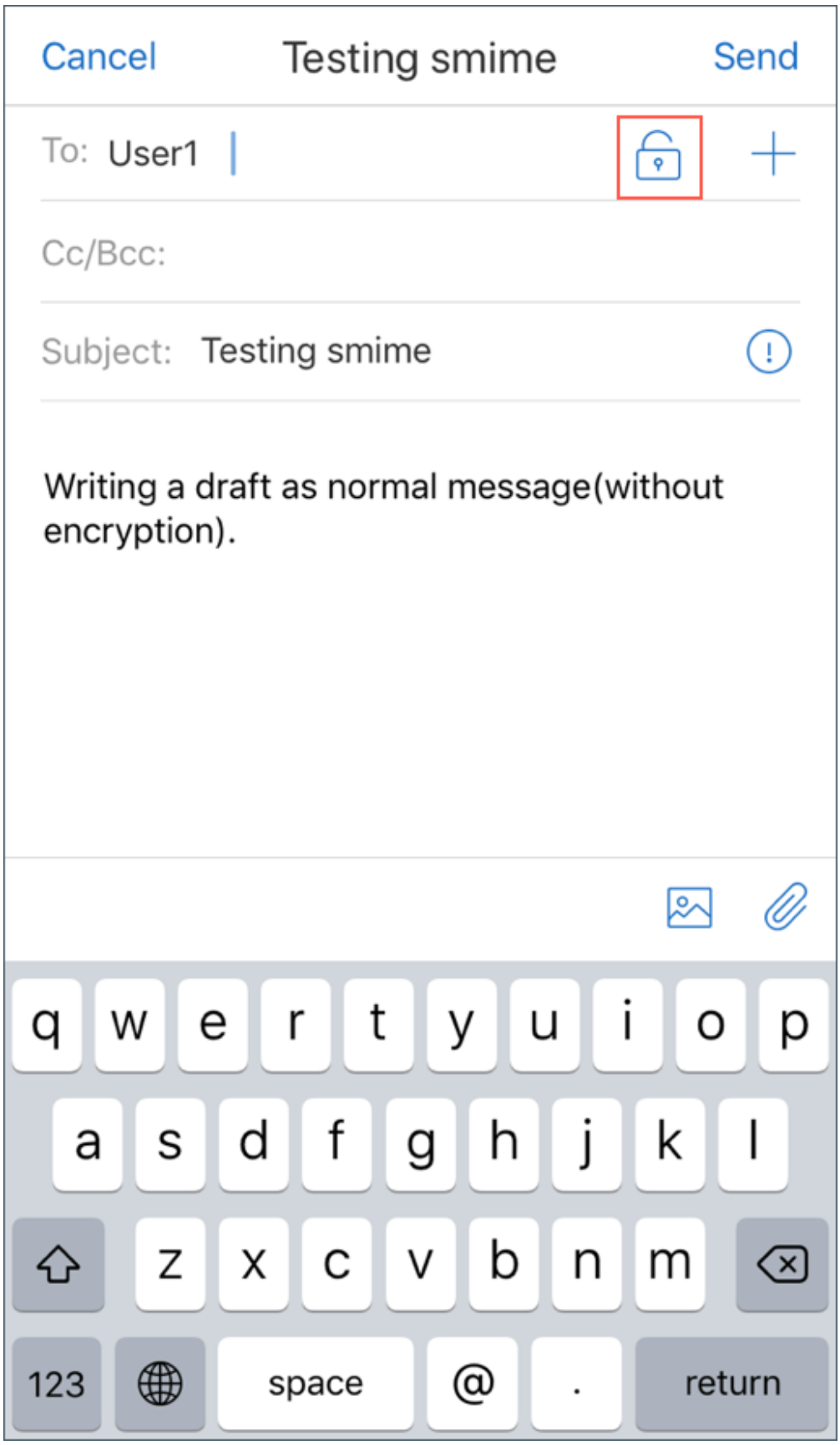
11. Stellen Sie im Bildschirm **Verschlüsselung** sicher, dass das richtige Verschlüsselungszertifikat importiert wurde.



Hinweis:

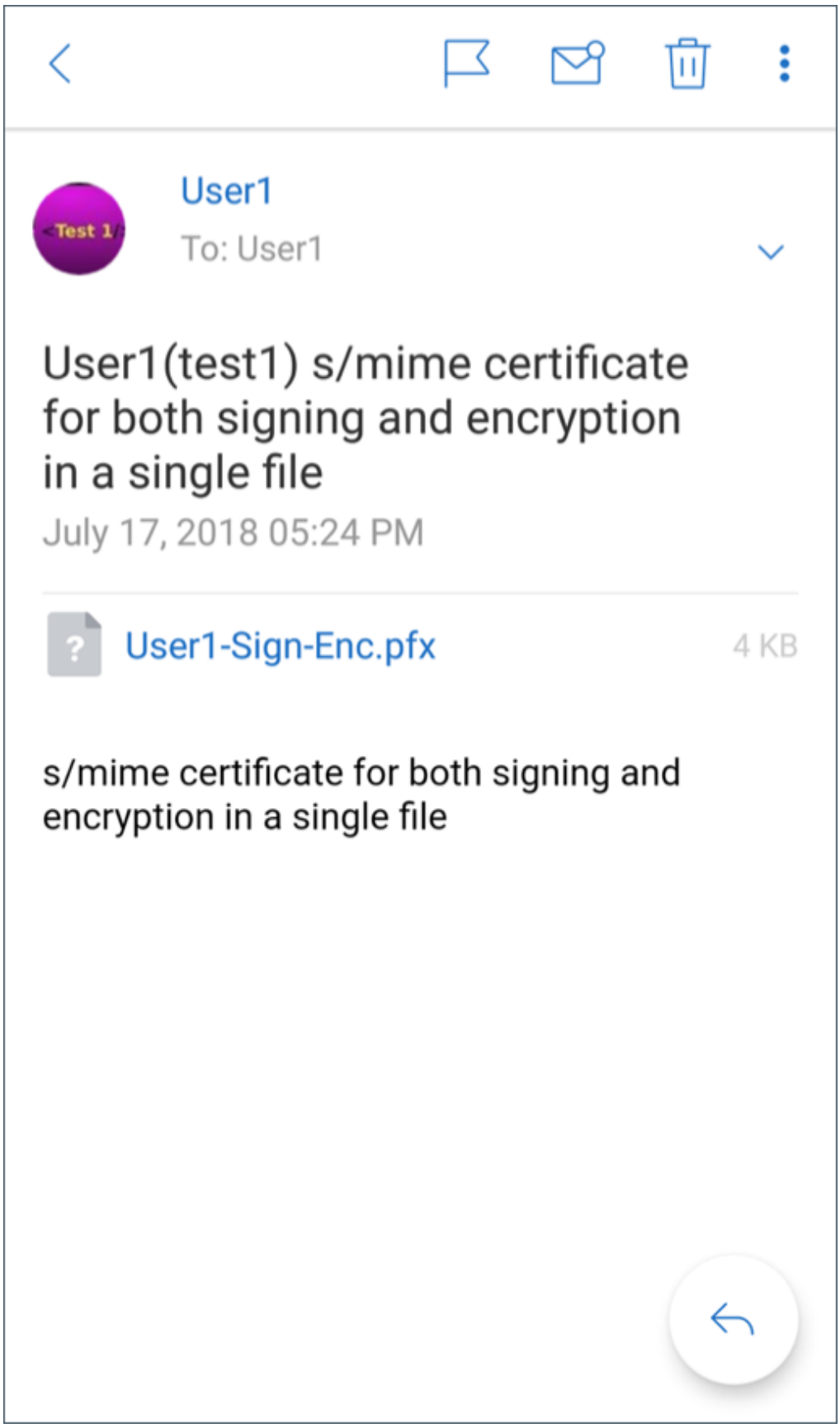
```
1.  Wenn eine mit S/MIME digital signierte E-Mail Anlagen hat und der Empfänger S/MIME nicht aktiviert hat, werden die Anlagen nicht empfangen. Dieses Verhalten ist eine Einschränkung von Active Sync. Damit Sie mit S/MIME signierte E-Mails wirklich erhalten, aktivieren Sie S/MIME in den Secure Mail-Einstellungen.

1.  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 verschlüsselten 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.
```

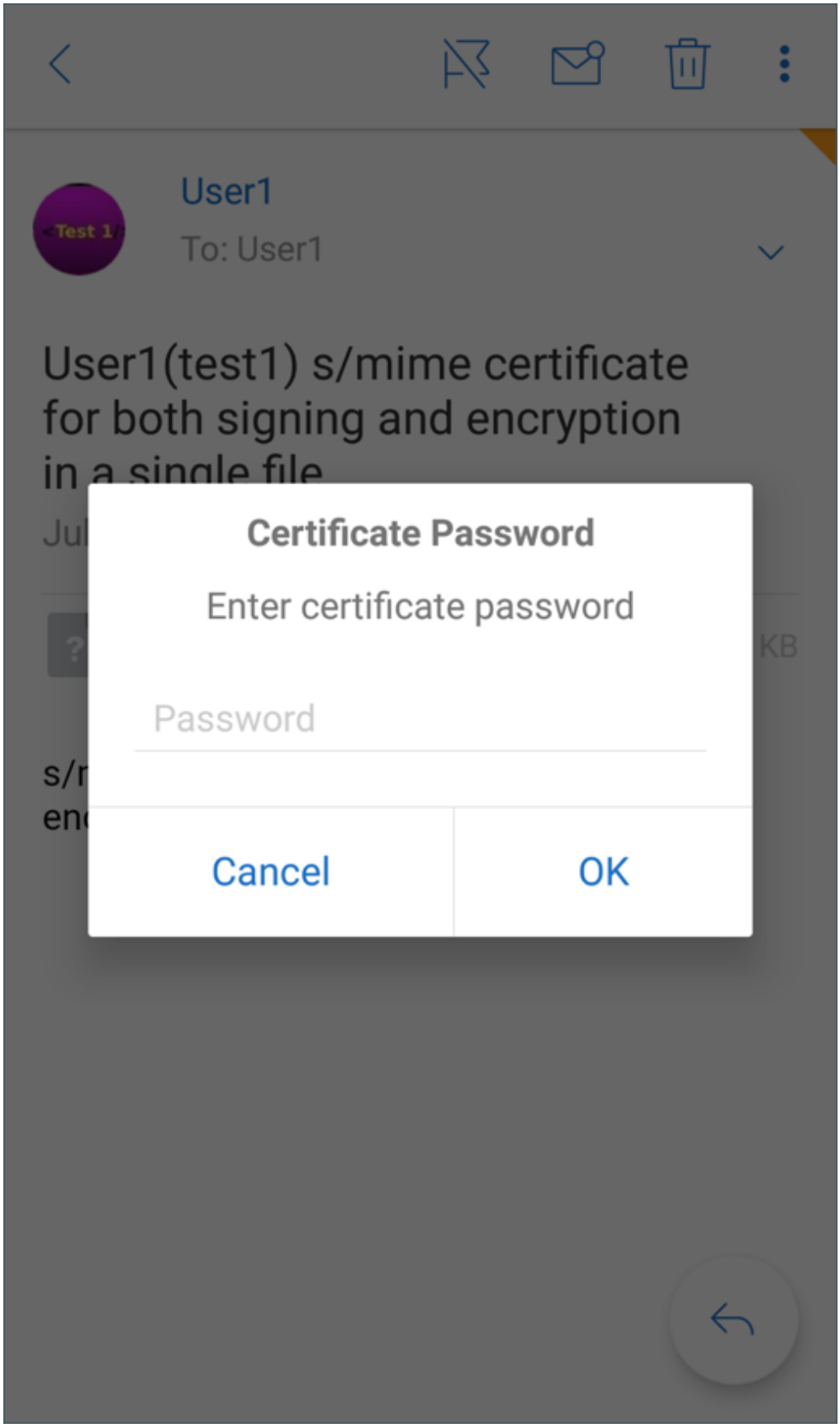



Aktivieren von S/MIME mit einem einzelnen Signatur- und Verschlüsselungszertifikat

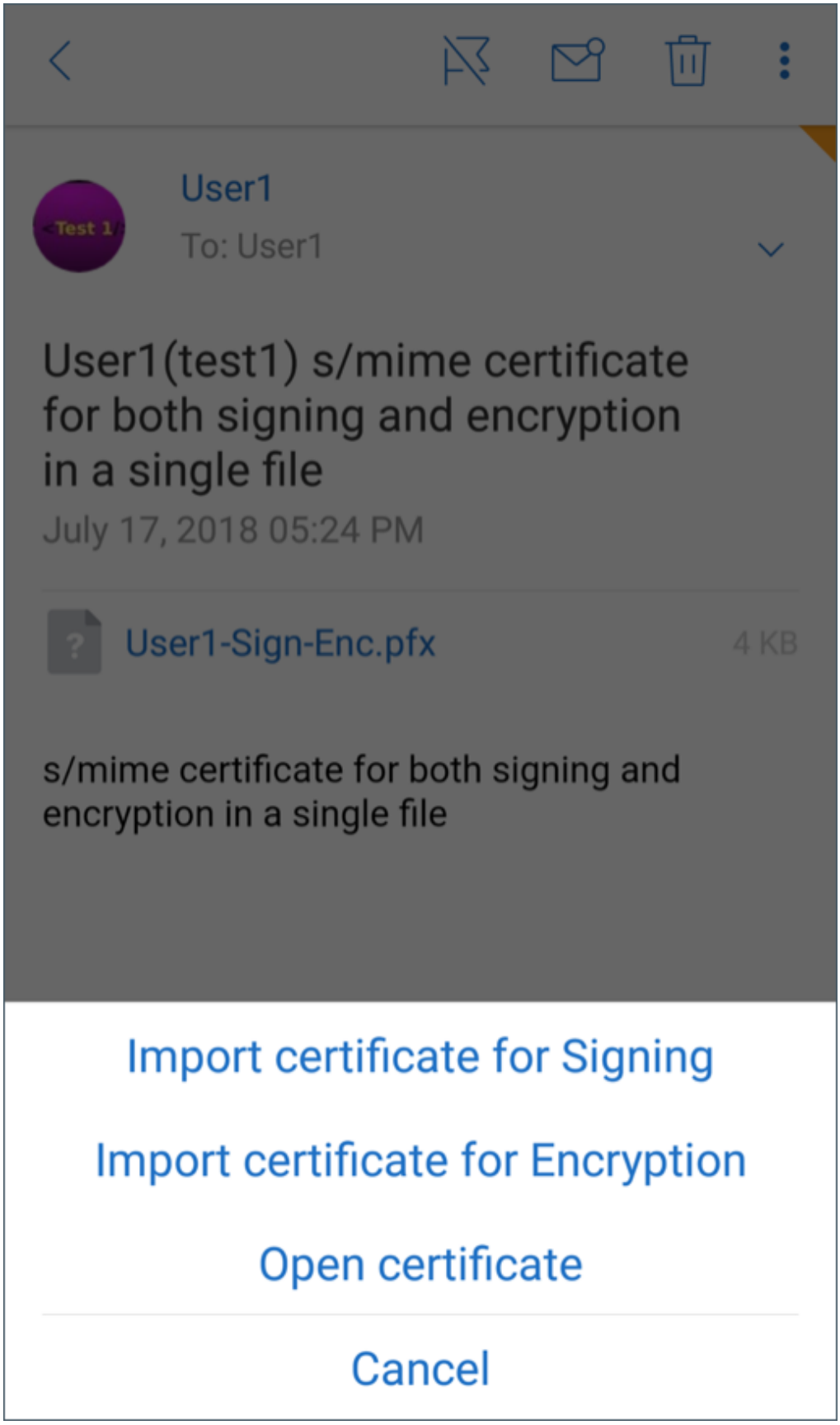
1. Öffnen Sie Secure Mail und navigieren Sie zu der E-Mail mit dem S/MIME-Zertifikat.



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.



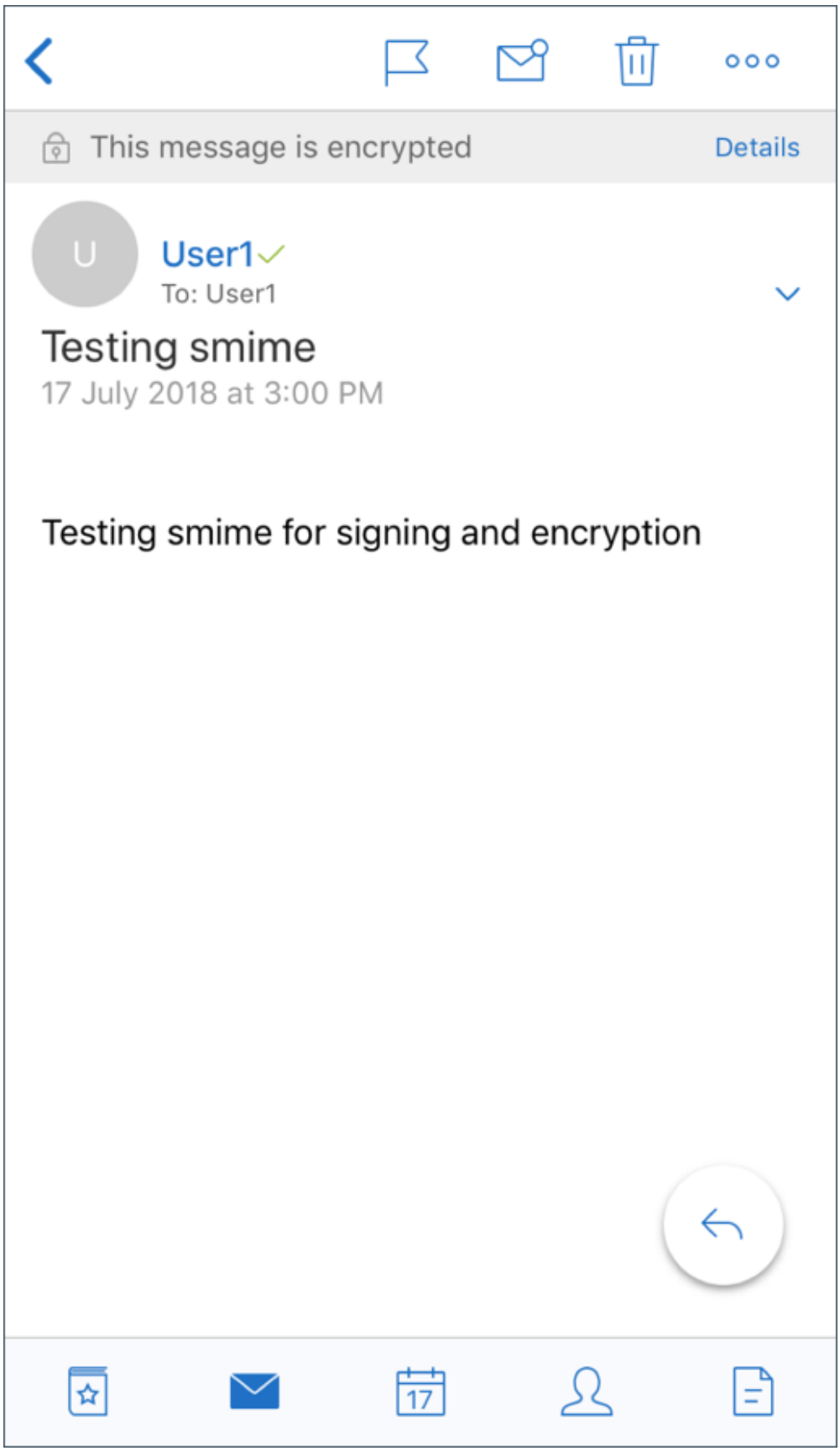
Ihr Zertifikat wurde importiert.

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

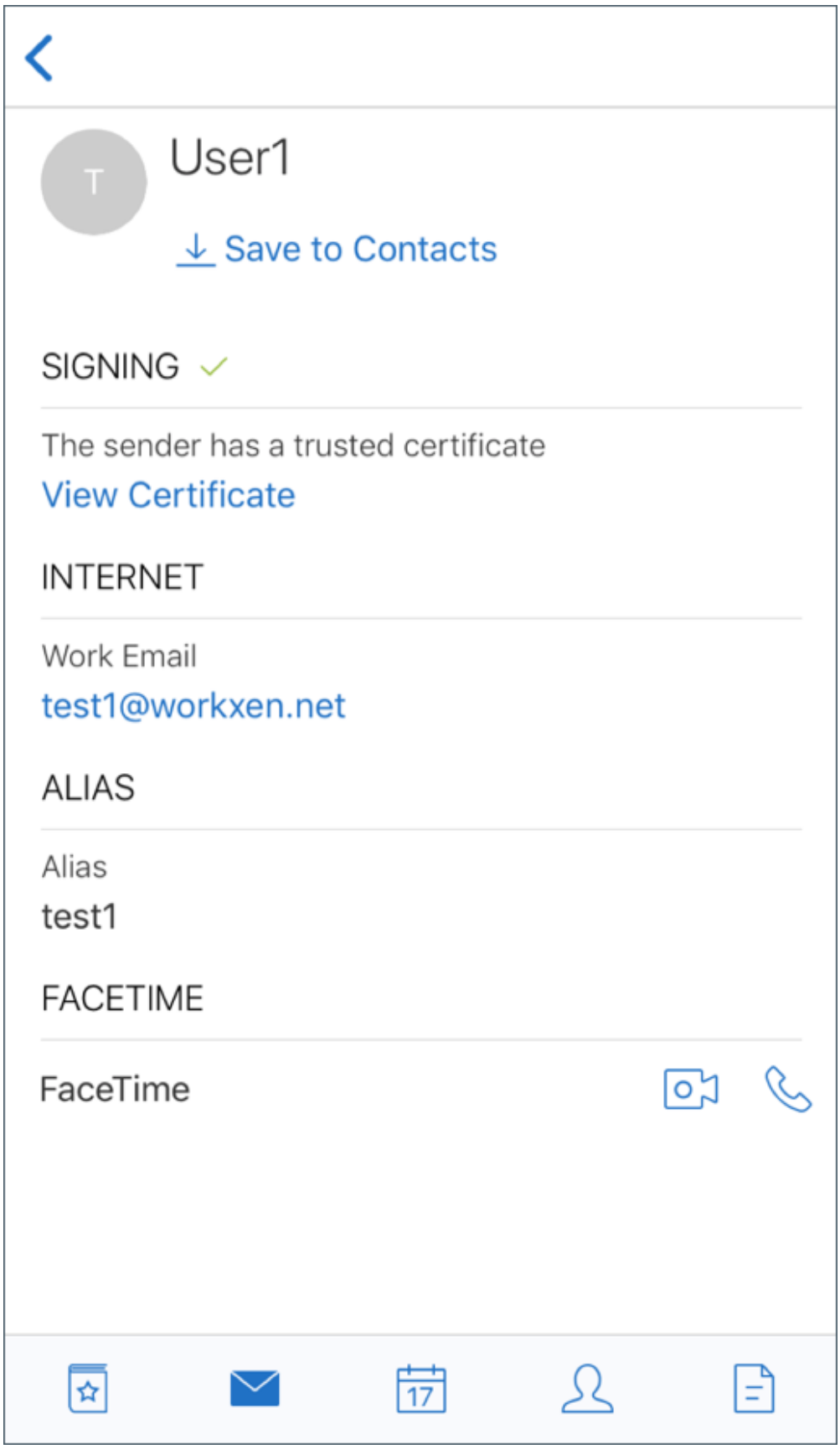
Testen von S/MIME in iOS und Android

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

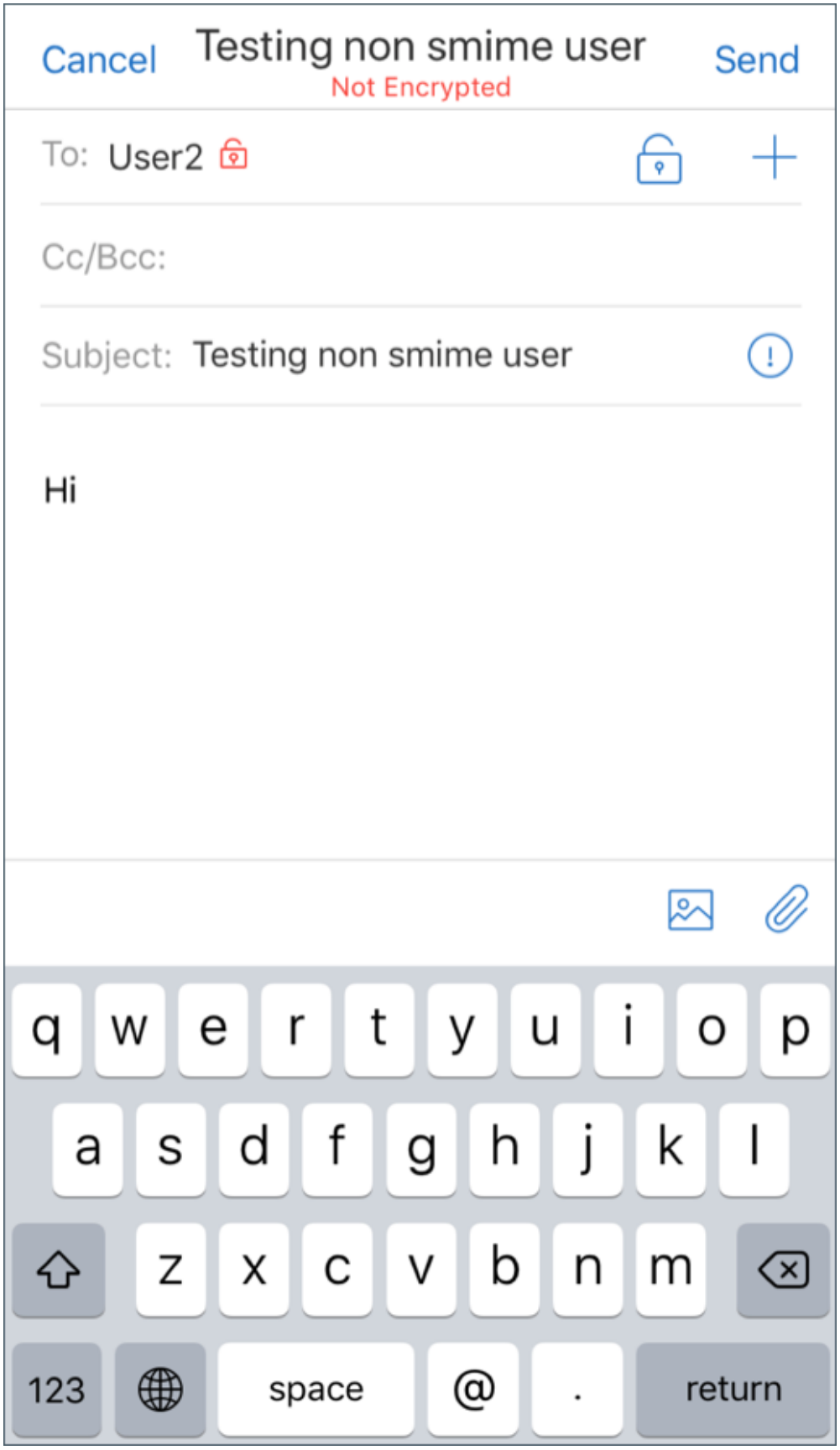
Die folgende Abbildung zeigt ein Beispiel einer verschlüsselten E-Mail, die vom Empfänger gelesen wird.



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

December 7, 2021

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 **userPrincipal-Name** 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 **userPrincipal-Name** 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 Microsoft AutoErmittlungsdienst finden Sie unter Autodiscover service in Exchange Server.

Sicherheitsüberlegungen

February 28, 2024

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

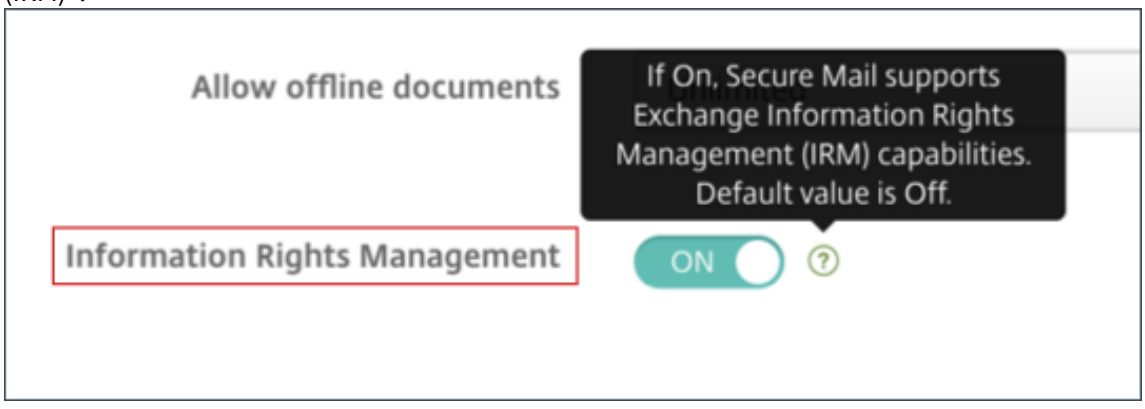
Unterstützung von E-Mails mit Microsoft IRM- und AIP-Schutz

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

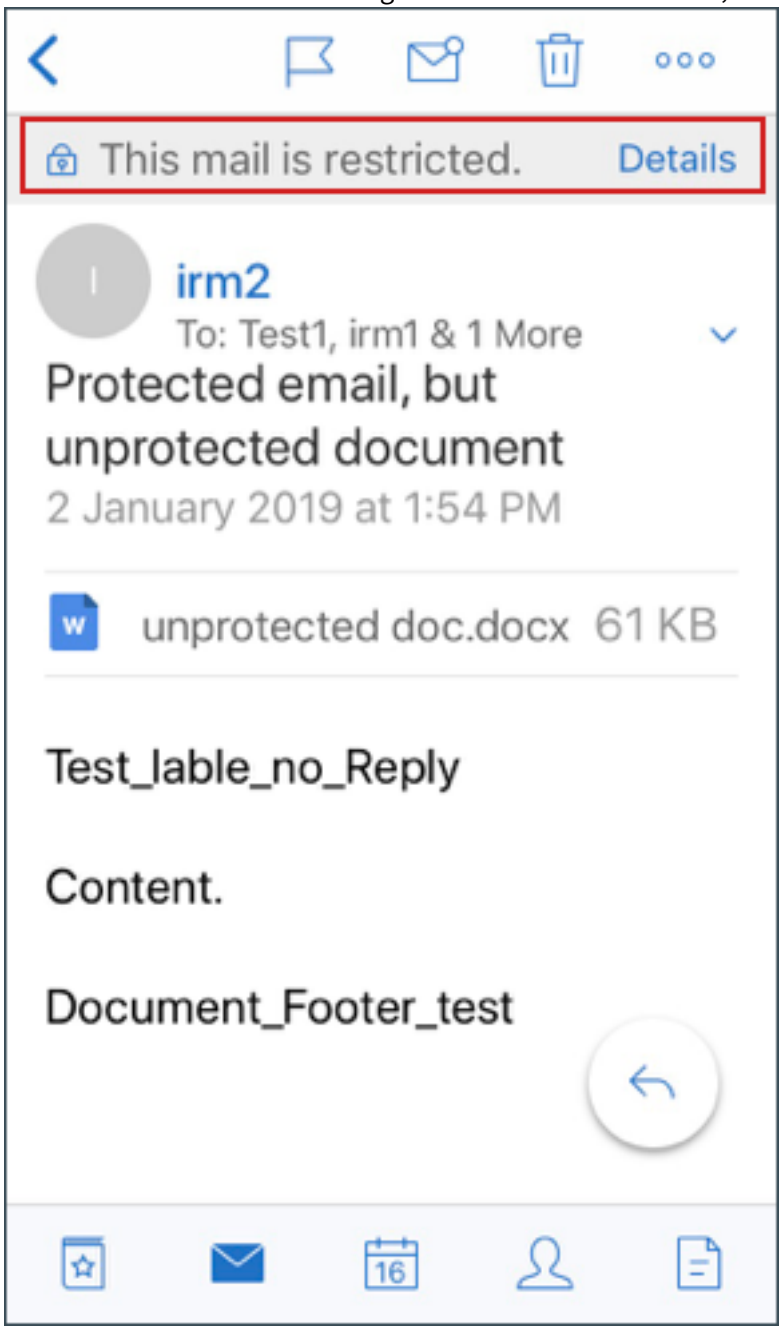
1. Melden Sie sich bei Endpoint Management an, navigieren Sie zu **Konfigurieren** > **Apps** und klicken Sie auf **Hinzufügen**.
2. Klicken Sie auf der Seite **Add App** auf **MDX**.
3. Geben Sie im Fenster **App-Informationen** die App-Details ein und klicken Sie auf **Weiter**.
4. Wählen Sie die MDX-Datei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



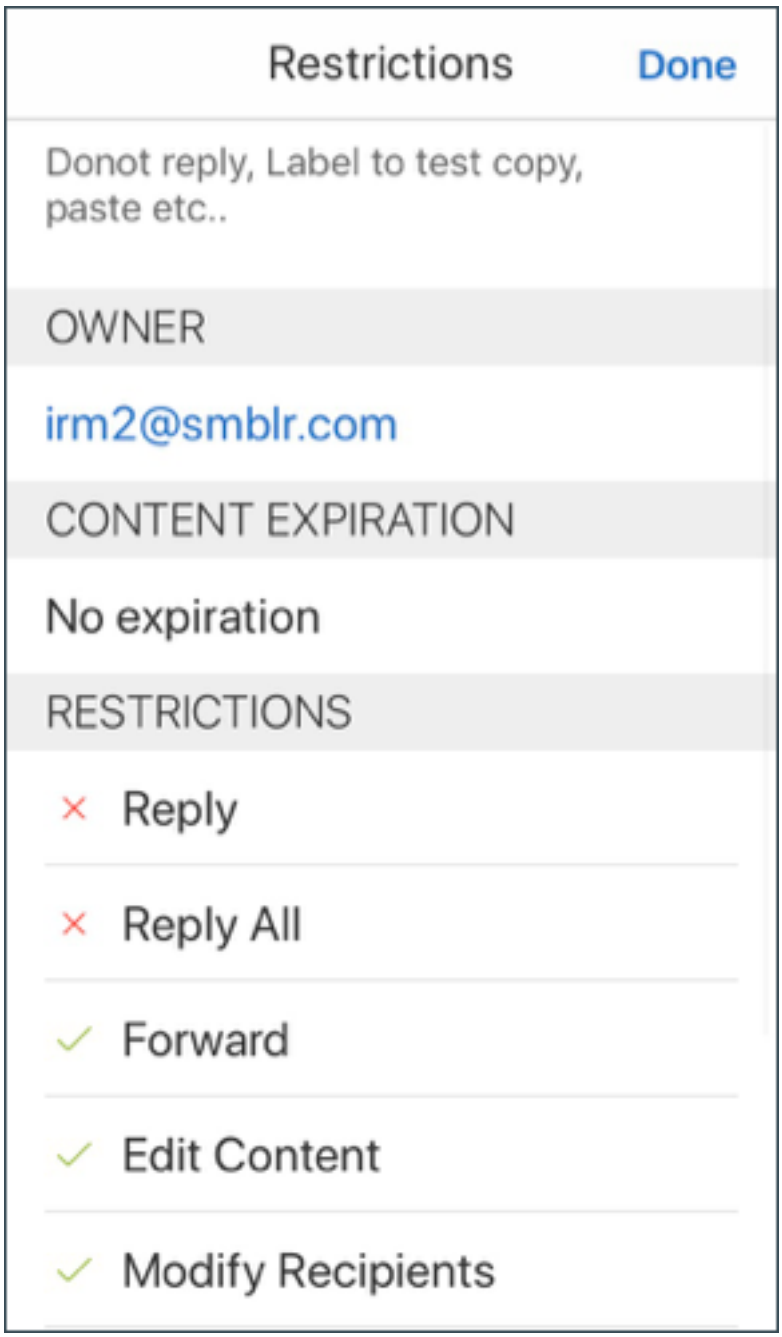
> Hinweis:
>
> Aktivieren Sie IRM für iOS und Android.

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.



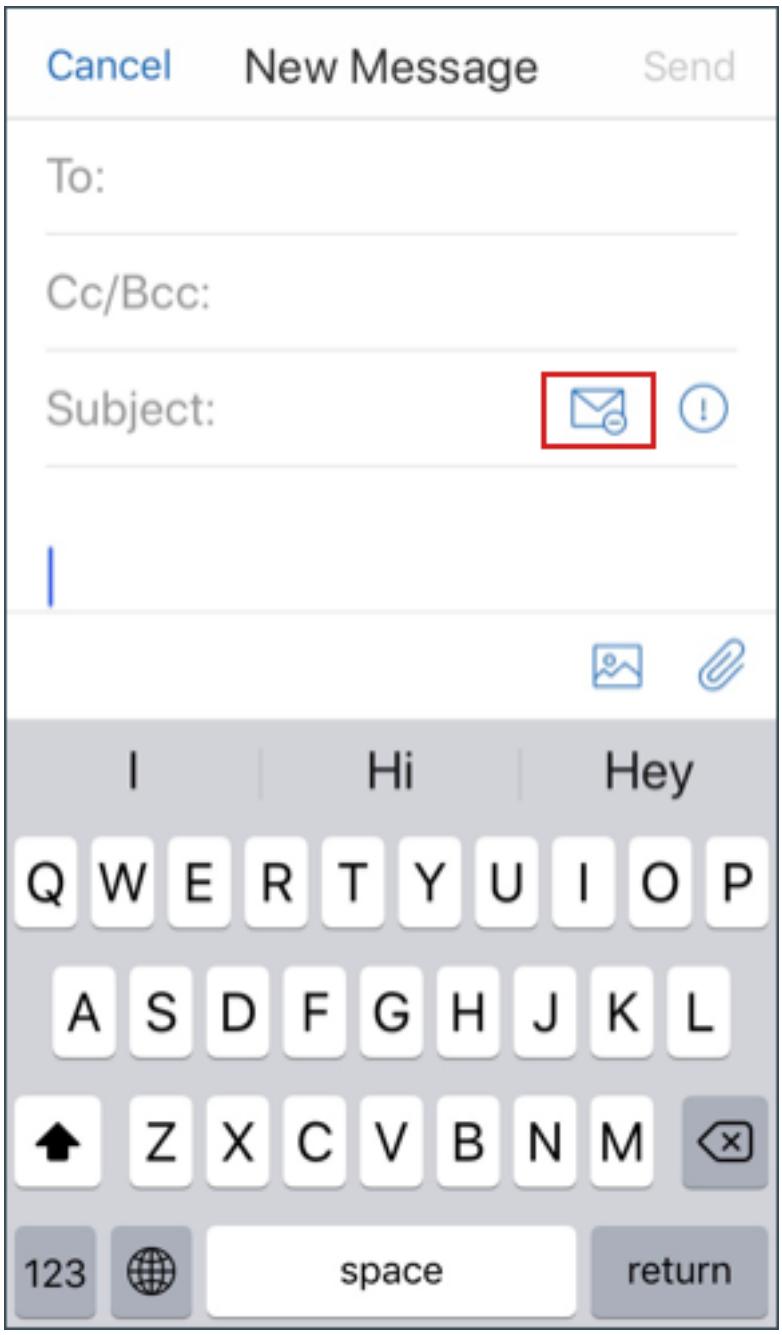
Verfassen einer geschützten E-Mail

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

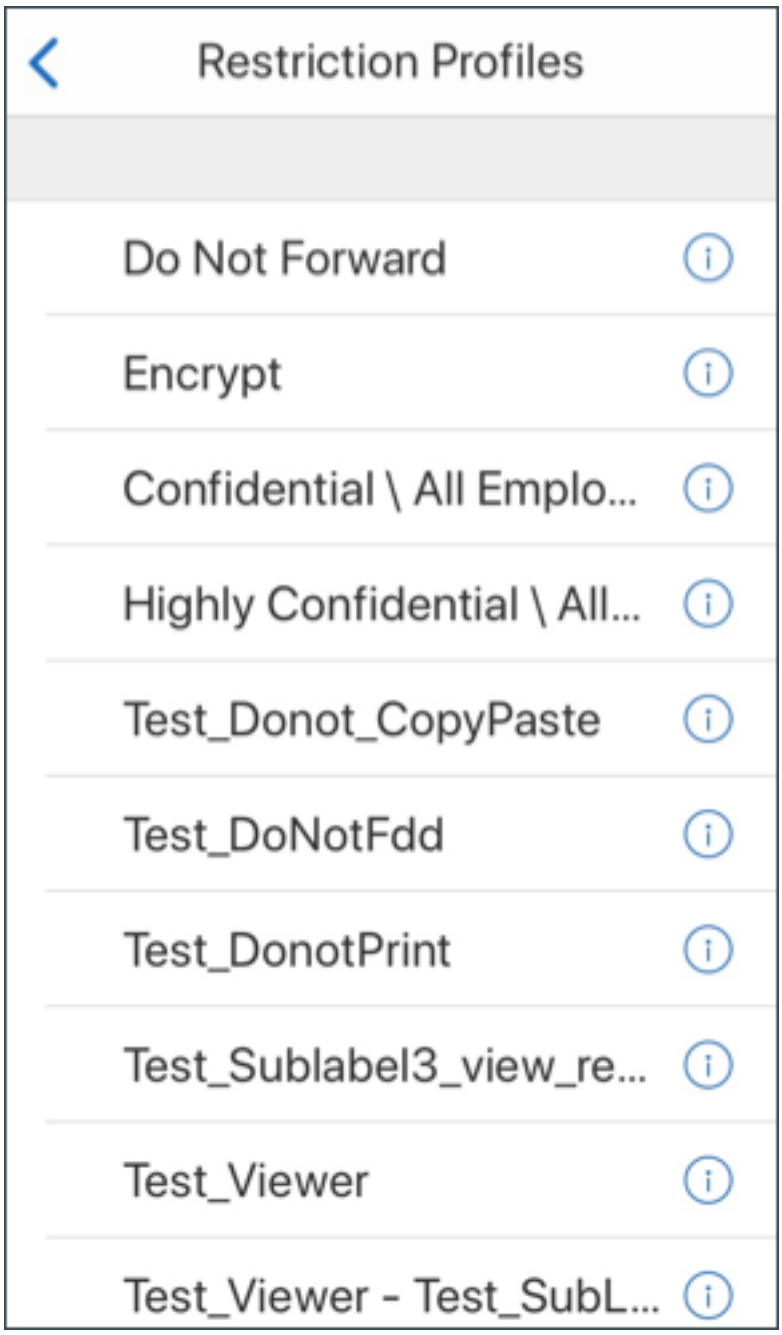
Festlegen von Einschränkungen für Ihre E-Mail:

1. Melden Sie sich in Secure Mail an und tippen Sie auf das Symbol **Verfassen**.

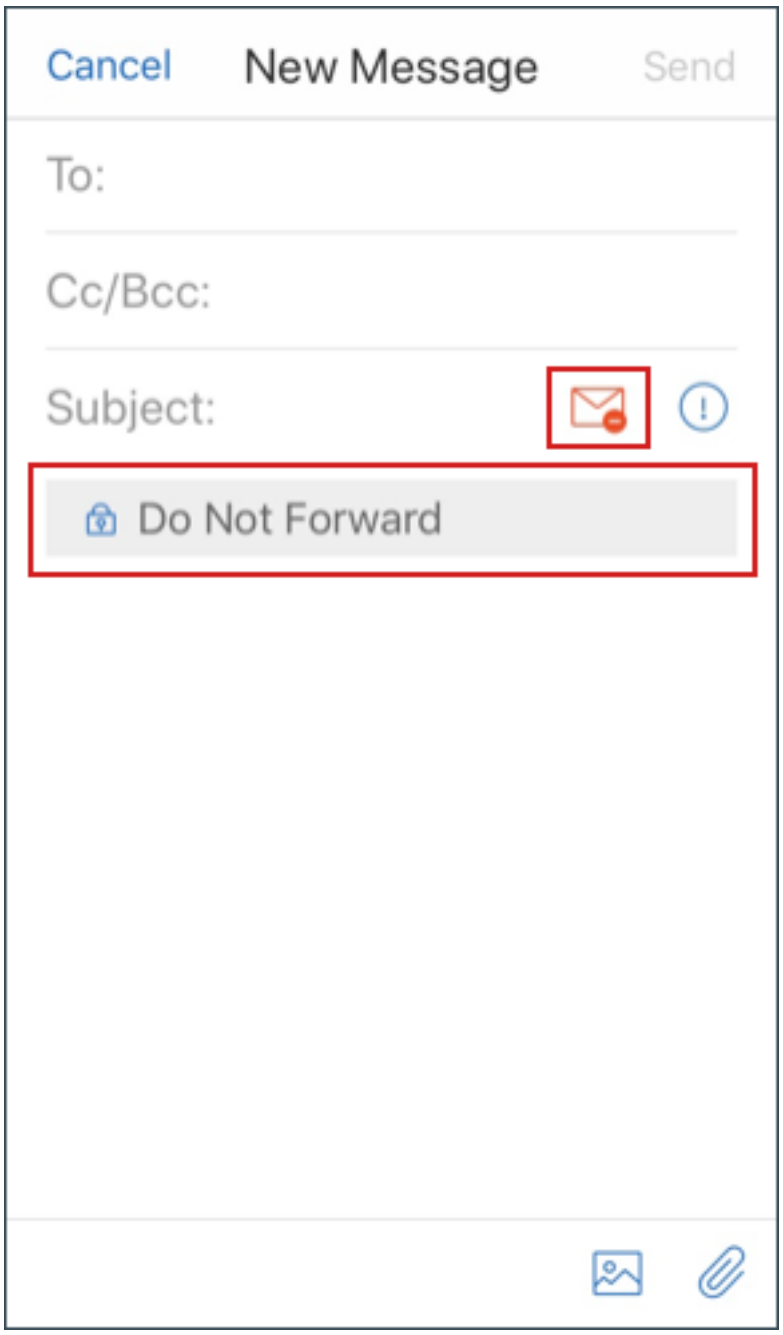
2. Tippen Sie im Bildschirm zum Verfassen einer E-Mail auf das Symbol zur **E-Mail-Beschränkung**.



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:

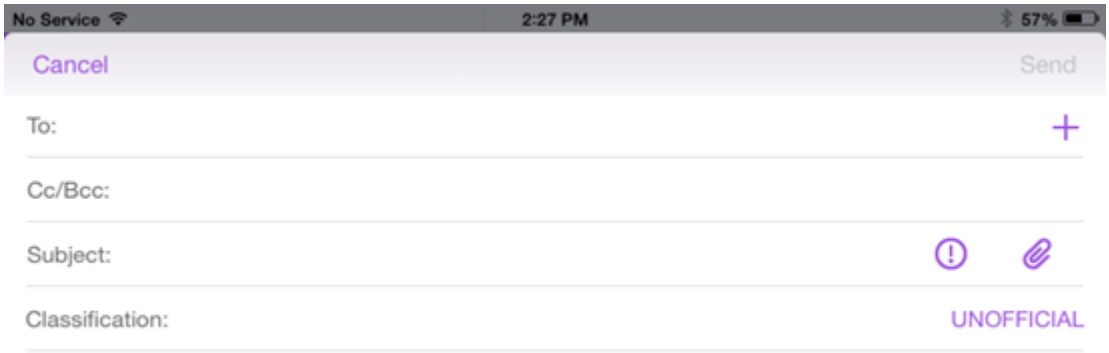
- Lesen Sie die Sicherheitsinformationen des Geräteherstellers.
- Konfigurieren Sie die Geräte entsprechend, entweder über Endpoint Management-Funktionen

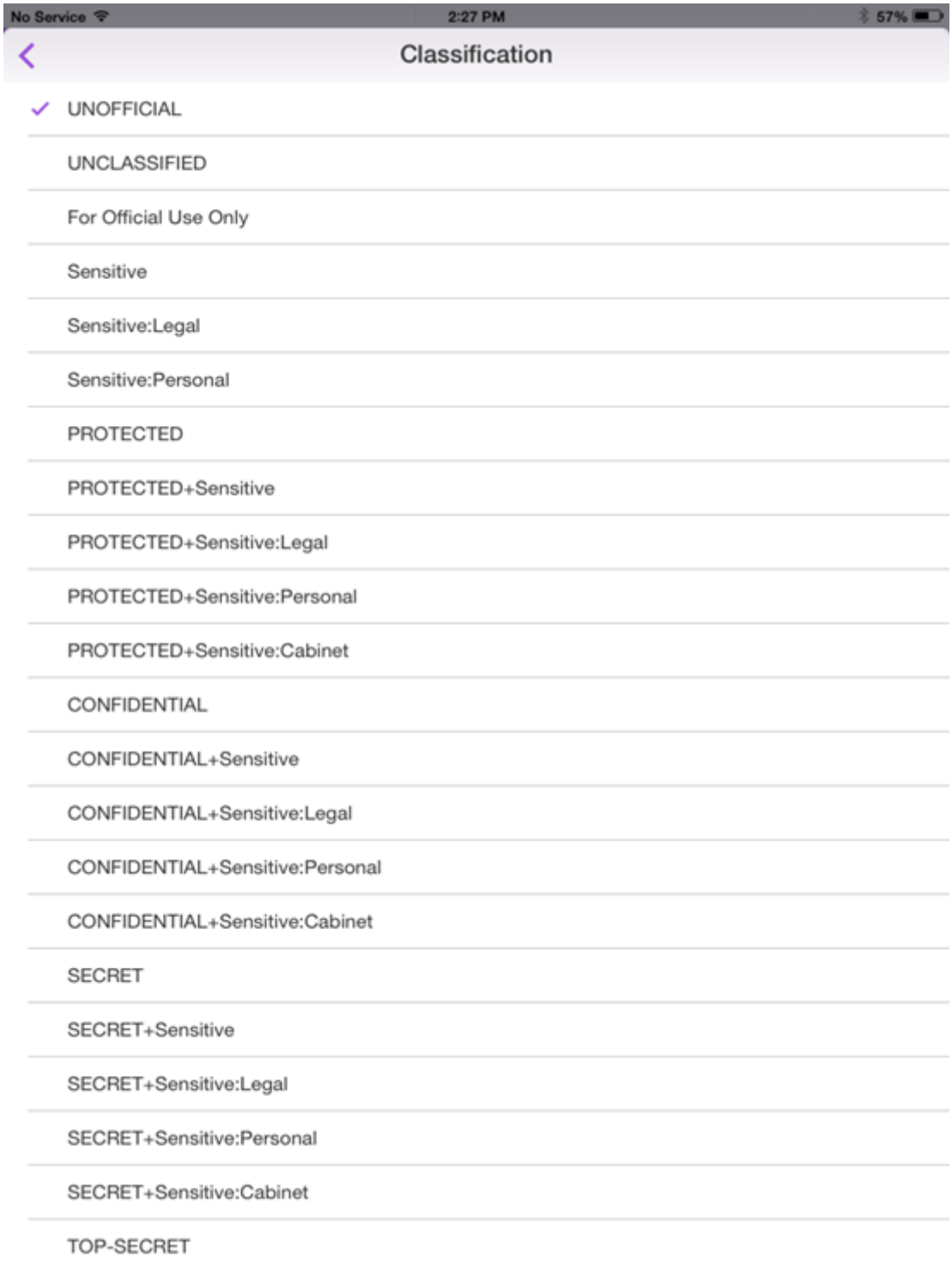
oder alternative Funktionen.

- 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. 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

Betreff: 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 (ASD) erfüllt werden müssen, können die neuen **Richtlinien zum Aktivieren des iOS-Datenschutzes** für Secure Mail und Secure Web verwendet werden. Die Standardeinstellung der

Richtlinien ist **Aus**.

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

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

1. Laden Sie mit der Endpoint Management-Konsole die MDX-Dateien für Secure Web and Secure Mail in Endpoint Management: Bei neuen Apps navigieren Sie zu **Konfigurieren > Apps > Hinzufügen** und klicken Sie auf **MDX**. Bei Upgrades gehen Sie wie unter Durchführen eines Upgrades von MDX- oder Unternehmensapps beschrieben vor.
2. 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.

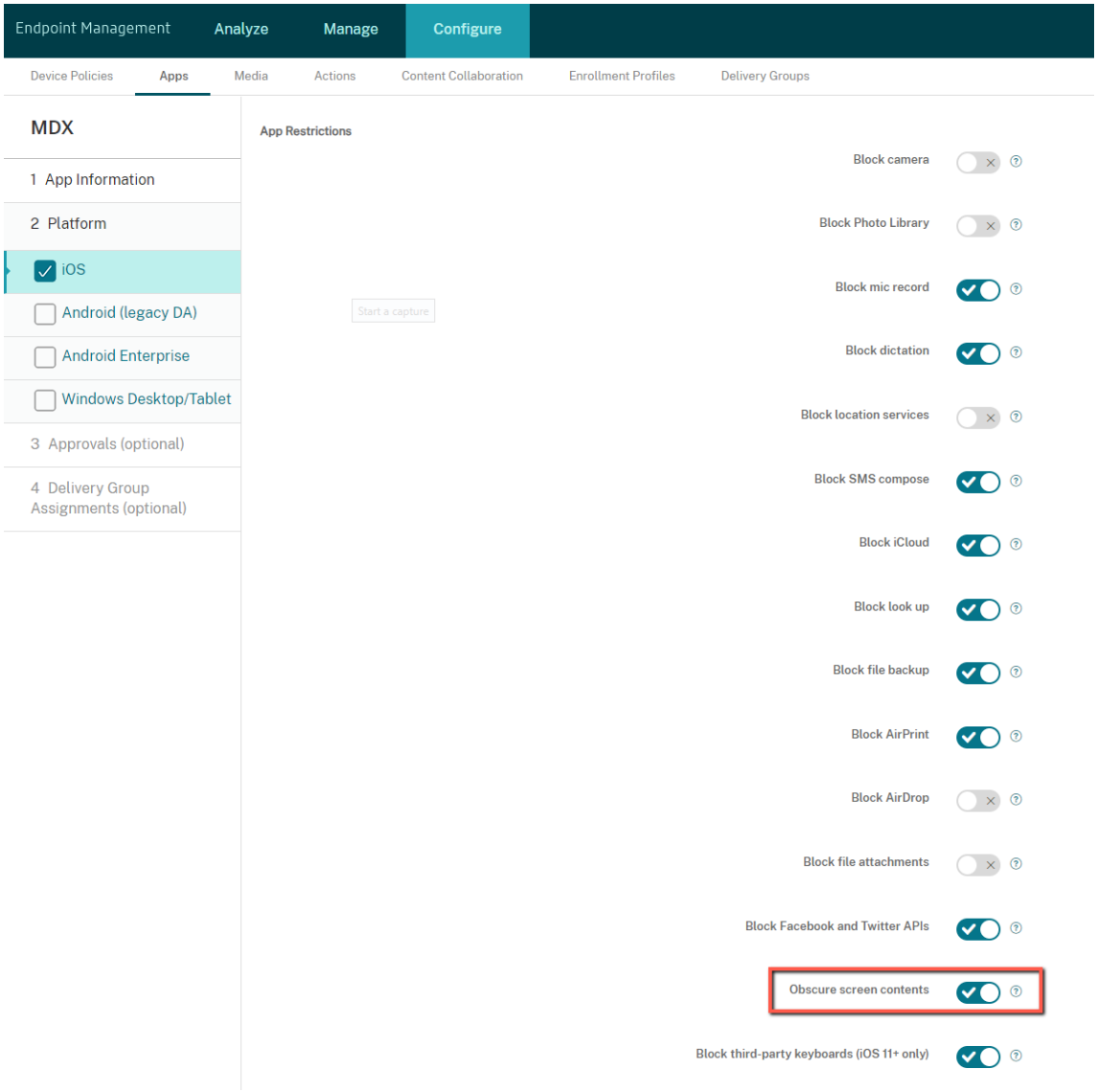
Citrix empfiehlt, beim Aktivieren dieser Richtlinie die Secure Mail-Protokollierung nur dann zu aktivieren, wenn sie unbedingt erforderlich ist, um das Erstellen von gemäß Klasse C geschützten Protokolldateien zu vermeiden.

Bildschirminhalt verbergen

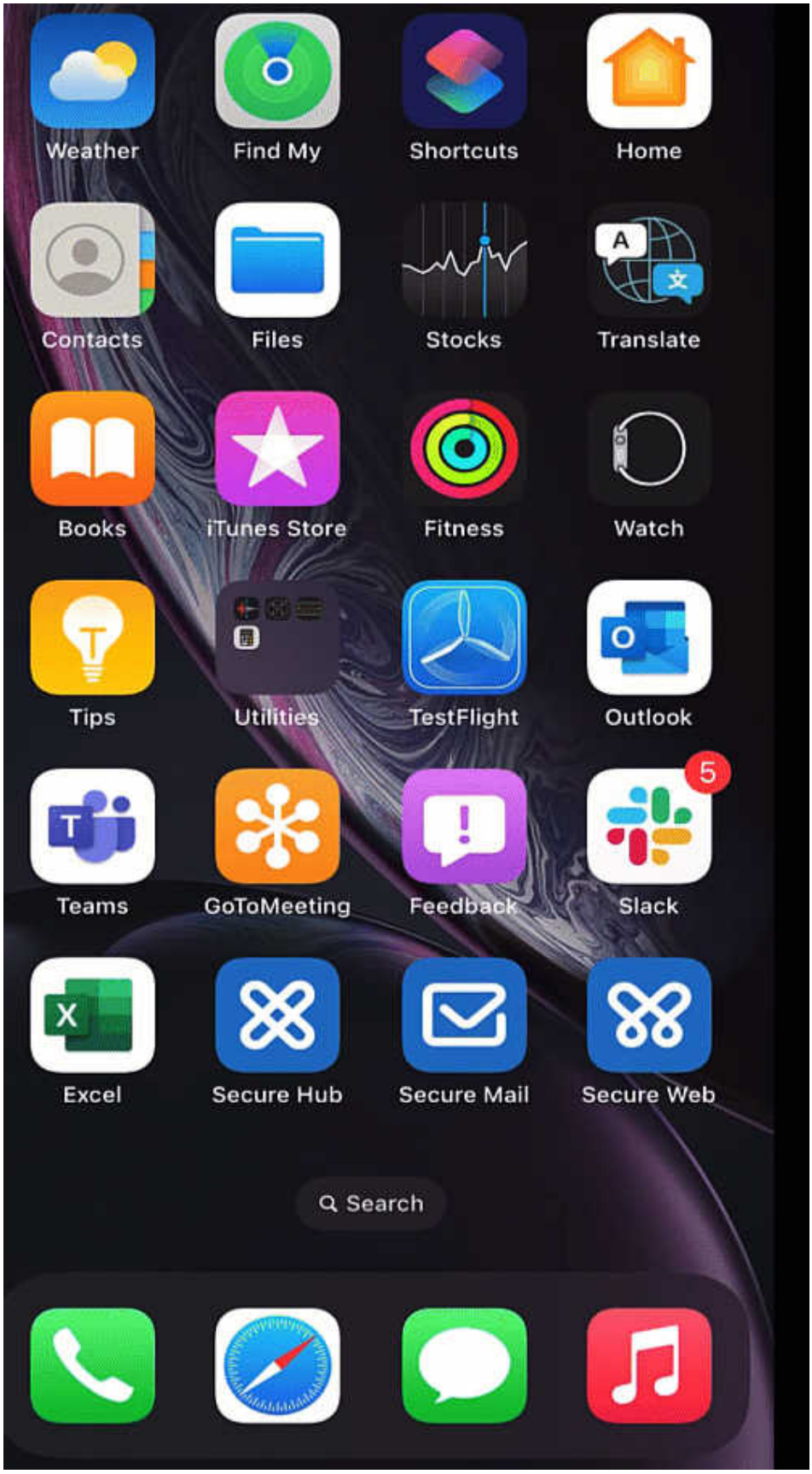
Secure Mail für Android und iOS unterstützt die Verdunkelung des Bildschirms, wenn die App in den Hintergrund tritt. Diese Funktion verbessert die Privatsphäre der Benutzer, schützt sensible Daten und verhindert unbefugten Zugriff. Informationen zum Aktivieren dieser Funktion für Secure Mail auf iOS- oder Android-Geräten finden Sie in den folgenden Abschnitten.

Auf iOS-Geräten:

1. Melden Sie sich mit Administratoranmeldeinformationen bei der Citrix Endpoint Management-Konsole an.
2. Navigieren Sie zu **Konfigurieren** > **Apps** > **MDX**.
3. Wählen Sie im Abschnitt **Plattform** die Option **iOS** aus.
4. Aktivieren Sie im Abschnitt **App-Einschränkungen** die Option **Bildschirminhalte verdecken**.



Sobald Sie die Option **Bildschirminhalte verbergen** aktiviert haben, zeigt Secure Mail einen grauen Bildschirm an, wenn die App in den Hintergrund tritt.



Auf Android-Geräten:

Um den Inhalt der Secure Mail-App zu verbergen, können Sie die Richtlinie verwenden, die zum Einschränken der Bildschirmaufnahme verwendet wird. Das ist die Richtlinie **Screenshot zulassen**. Durch das Deaktivieren dieser Richtlinie werden auch App-Inhalte verdeckt, wenn die App in den Hintergrund tritt. Weitere Informationen zum Deaktivieren der Richtlinie **Screenshot zulassen** finden Sie in den Android-Einstellungen in der Citrix Endpoint Management-Dokumentation.

iOS-Features

February 3, 2022

Dieser Artikel beschreibt die iOS-Features, die in Secure Mail unterstützt werden.

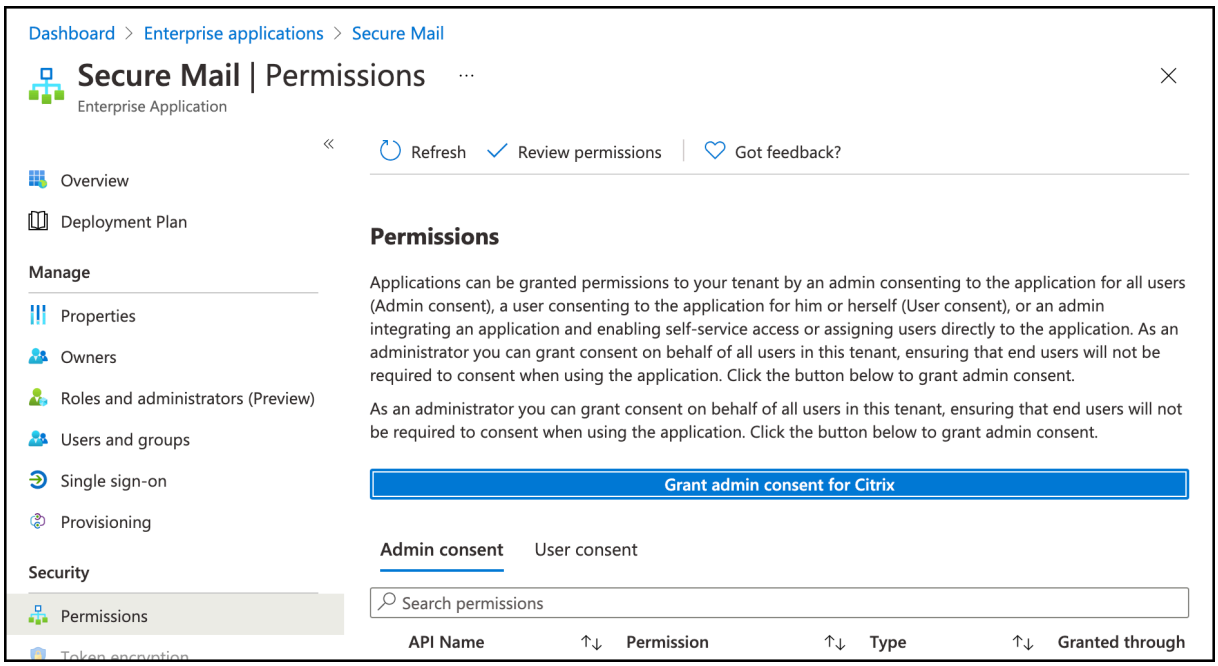
Erstellen von Microsoft Teams-Besprechungen in Secure Mail-Kalenderereignissen

In Secure Mail für iOS können Sie Einladungen für Microsoft Teams-Besprechungen erstellen, während Sie Kalenderereignisse erstellen. Um eine Microsoft Teams-Besprechung zu erstellen, aktivieren Sie die Umschaltfläche **Microsoft Teams-Besprechung**. Der Link zur Besprechungseinladung und die Details werden automatisch mit den Ereignisdetails gesendet. Weitere Informationen finden Sie unter Erstellen von Microsoft Teams-Besprechungen in Secure Mail-Kalenderereignissen.

Voraussetzungen:

Stellen Sie sicher, dass der globale Administrator von Azure Active Directory folgende Schritte ausführt:

- Die moderne Authentifizierung (OAuth) aktiviert und sicherstellt, dass ein Exchange Online oder ein Postfachbenutzer mit einer gültigen Microsoft Teams-Lizenz verwendet wird.
- Mandantenweite Admin-Zustimmung für die Secure Mail-App gewährt.
- Das Exchange-Konto in der Secure Mail-App konfiguriert und die App-Berechtigung für alle Benutzer zulässt, die sich anmelden. Sie sehen den folgenden Bildschirm:



- Aktivieren Sie die Microsoft Teams-Integrationsrichtlinie.

Einschränkungen:

Für Meetings, die mit Secure Mail erstellt wurden, hat das Feature derzeit die folgenden Einschränkungen für den Microsoft Outlook-Kalender:

- Die Option **Online teilnehmen** ist nicht verfügbar
- Die Benachrichtigung **Die Besprechung hat begonnen** ist nicht verfügbar

Entwürfe minimieren

In Secure Mail für iOS können Sie einen Entwurf minimieren, während Sie eine E-Mail erstellen, und innerhalb der App navigieren. Diese Funktion ist auf Geräten mit iOS 13 und höher verfügbar. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter E-Mail-Entwurf minimieren.

Melden von Phishing-E-Mails mit MIME-Kopfzeile

Wenn ein Benutzer in Secure Mail für iOS eine Phishing-E-Mail meldet, wird zu der E-Mail eine EML-Datei als Anlange erstellt. Der Empfänger der E-Mail kann die MIME-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. Weitere Informationen finden Sie unter Melden von Phishing-E-Mail (als Anlage).

Unterstützung für WkWebView

Secure Mail für iOS unterstützt WkWebView. Dieses Feature verbessert die Art und Weise, wie Secure Mail-Emails und Kalenderereignisse auf Ihrem Gerät gerendert werden.

Unterstützung für Slack EMM

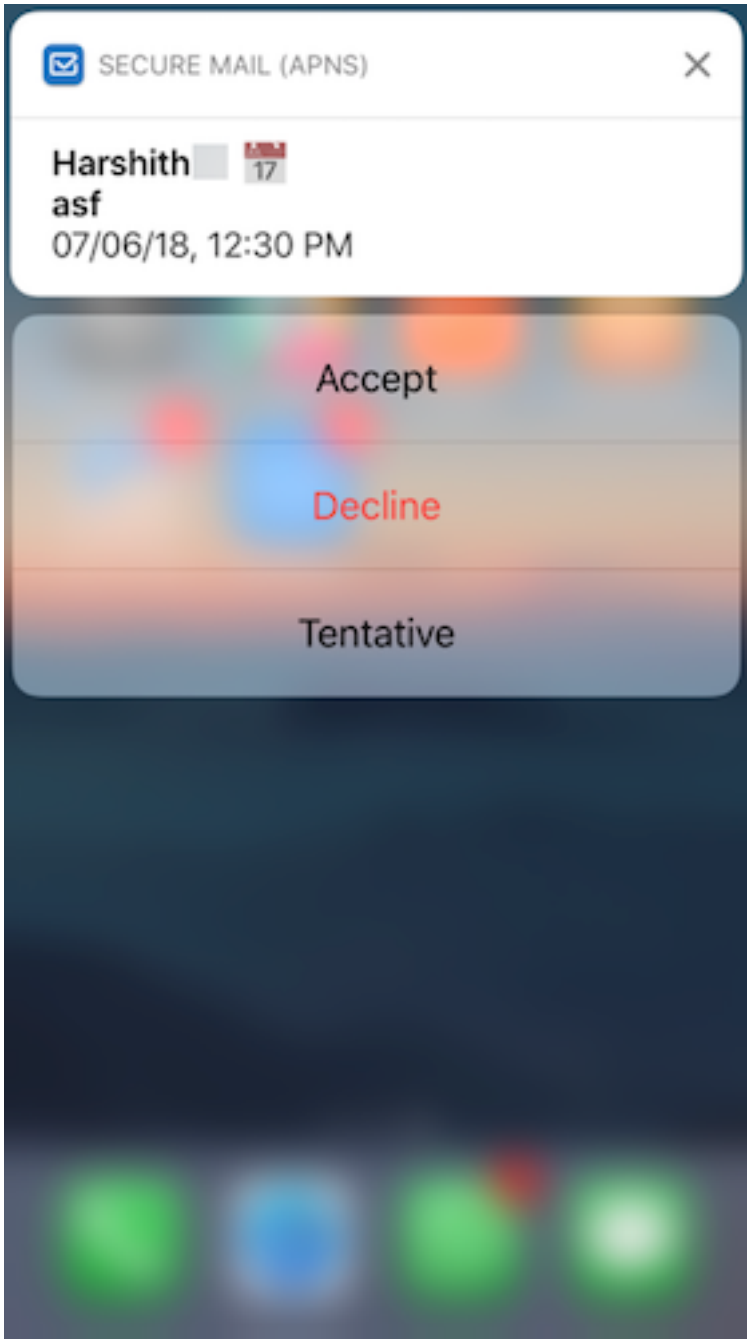
Slack EMM ist eine Funktion für Slack-Kunden mit aktiviertem Enterprise Mobility Management (EMM). Secure Mail für iOS unterstützt die Anwendung **Slack EMM**, mit der Administratoren die Integration von Secure Mail in die **Slack-App** oder die **Slack EMM-App** wählen können.

Gruppenbenachrichtigungen

Mit dem Feature "Gruppenbenachrichtigungen"werden Gespräche in 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. Für dieses Feature ist iOS 12 erforderlich.

Antwortoption 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.



Verbesserte Fehlermeldungen für Pushbenachrichtigungen mit Rich-Media-Inhalt

In Secure Mail für iOS werden je nach Benachrichtigungsfehler Fehlermeldungen zu Pushbenachrichtigungen in der Mitteilungszentrale auf Geräten angezeigt. Weitere Informationen finden Sie unter Secure Mail-Benachrichtigungen.

Unterstützung für Pushbenachrichtigungen mit Rich-Media-Inhalt in Microsoft-Umgebungen

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-Media-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**.

Unterstützung von S/MIME für abgeleitete Anmeldeinformationen

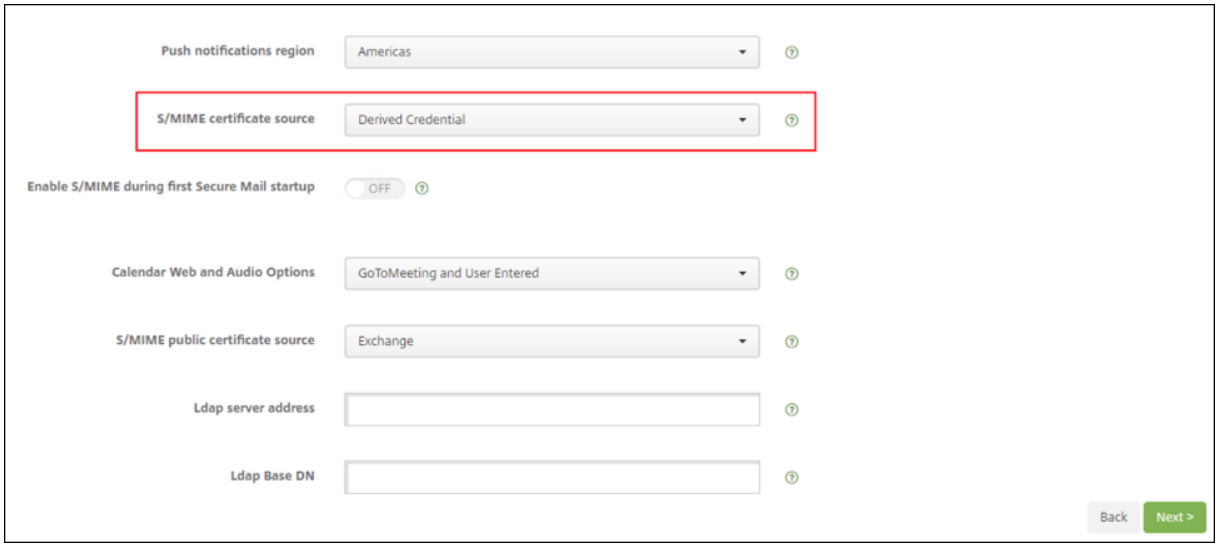
Secure Mail für iOS unterstützt S/MIME für abgeleitete Anmeldeinformationen. Hierfür ist Folgendes erforderlich:

- Wählen Sie "Abgeleitete Anmeldeinformationen"als Quelle des S/MIME-Zertifikats aus. Weitere Informationen finden Sie unter Abgeleitete Anmeldeinformationen für iOS.
- 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).

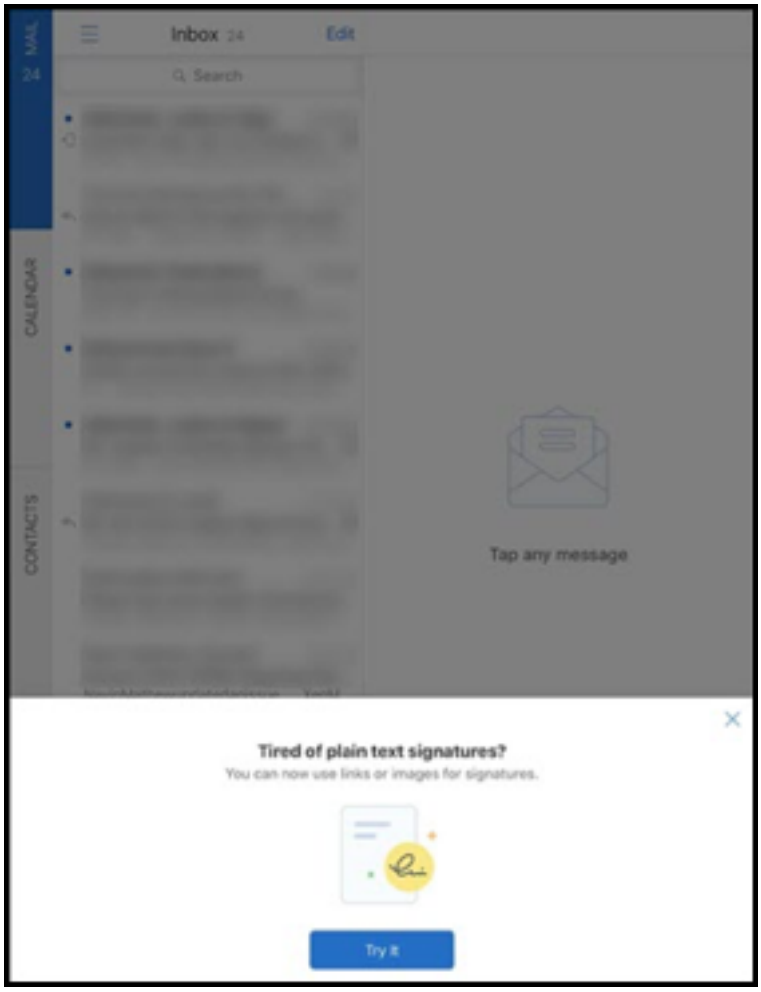
Weitere Informationen zum Registrieren von Geräten mit abgeleiteten Anmeldeinformationen finden Sie unter Registrieren von Geräten mit abgeleiteten Anmeldeinformationen.

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.



Rich-Text-Signaturen

Sie können Bilder oder Links in Ihrer E-Mail-Signatur verwenden. Um Ihre Signatur zu aktualisieren, kopieren Sie einfach Bilder und Links in das Unterschriftsfeld.



Hinzufügen einer Rich-Text-Signatur

1. Kopieren Sie das Bild oder die URL, das bzw. die Sie verwenden möchten.
2. Navigieren Sie zu **Secure Mail > Einstellungen > Signatur**.
3. Fügen Sie das Bild oder die URL ein.

Sie können alternativ das Signaturfeld lange drücken und auf **Bild einfügen** tippen, um ein Bild aus Ihrer Galerie auszuwählen.

Secure Mail-Anrufer-ID

In Secure Mail für iOS können Sie eingehende Anrufe von Ihren Secure Mail-Kontakten identifizieren, indem Sie in den Geräteeinstellungen die Secure Mail-Anrufer-ID aktivieren. Sie müssen die folgende administrative Voraussetzung aktivieren: Stellen Sie in Citrix Endpoint Management sicher, dass die MDX-Richtlinie “CallerIDSupportEnabled”aktiviert ist.

Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Anrufer-ID einrichten.

Festlegen von Farben in Kalendern

Zu diesem Kalenderfeature finden Sie Hilfedokumentation in der Citrix-Benutzerhilfe unter Farben für synchronisierte Secure Mail-Kalender festlegen.

Dateien aus der App "Dateien"anhängen

In Secure Mail für iOS können Sie Dateien über die systemeigene iOS-App **Dateien** anhängen. Weitere Informationen zur iOS-App "Dateien"finden Sie im Apple-Artikel Files App. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Dateien anzeigen und anhängen.

Rechtschreibprüfung

Die Secure Mail-Rechtschreibprüfung interagiert mit den geräteeigenen Einstellungen für automatische Großschreibung und Rechtschreibung (unter **Allgemein > Tastatur**) wie folgt:

Autokorrektur auf dem Gerät	Rechtschreibprüfung auf dem Gerät	Rechtschreibprüfung in Secure Mail	Ergebnis
EIN	EIN	EIN	Rote Linie wird angezeigt. Beim Tippen darauf wird das Wort pink hervorgehoben und ein Vorschlag wird angezeigt.
AUS	AUS	EIN	Rote Linie wird angezeigt. Beim Tippen darauf wird kein Vorschlag angezeigt.

Autokorrektur auf dem Gerät	Rechtschreibprüfung auf dem Gerät	Rechtschreibprüfung in Secure Mail	Ergebnis
EIN	EIN	AUS	Keine rote Linie wird angezeigt. Beim Tippen darauf wird das Wort pink hervorgehoben und ein Vorschlag wird angezeigt.
AUS	AUS	AUS	Keine rote Linie, Markierung und kein Vorschlag werden angezeigt.
EIN	AUS	EIN	Rote Linie wird angezeigt. Beim Tippen darauf wird das Wort pink hervorgehoben und ein Vorschlag wird angezeigt.
AUS	EIN	EIN	Rote Linie wird angezeigt. Beim Tippen darauf wird das Wort pink hervorgehoben und ein Vorschlag wird angezeigt.
EIN	AUS	AUS	Keine rote Linie wird angezeigt. Beim Tippen darauf wird das Wort pink hervorgehoben und ein Vorschlag wird angezeigt.

Autokorrektur auf dem Gerät	Rechtschreibprüfung auf dem Gerät	Rechtschreibprüfung in Secure Mail	Ergebnis
AUS	EIN	AUS	Keine rote Linie wird angezeigt. Beim Tippen darauf wird das Wort pink hervorgehoben und ein Vorschlag wird angezeigt.

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.

Das Postfach **Alle Konten** ist die standardmäßige Gesamtübersicht. Sie enthält E-Mail und Anlagen aller Exchange-Konten, die Sie auf Ihrem Gerät konfiguriert haben.

Das Postfach **Alle Konten** bietet folgende Menüoptionen:

- Alle Anlagen
- Posteingang
  - Ungelesen
  - Gekennzeichnet
- Entwürfe
- Gesendete Elemente
- Postausgang
- Gelöschte Elemente

In der Ansicht **Alle Konten** werden zwar die E-Mails aus mehreren Konten angezeigt, bei folgenden Aktionen wird jedoch 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

Alle konfigurierten Konten erscheinen in Form einer Liste unter **Alle Konten**. 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. Sie können Unterordner durch Tippen auf das **V**-Symbol daneben anzeigen.

Die folgenden Aktionen werden nur auf einzelne Konten angewendet:

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

Kalender

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

Festlegen von Farben für Kalendereereignisse

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 Kalendereereignisse 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.

> **Hinweis:**
>
> Wenn Sie Secure Mail beenden und dann wieder neu starten, werden die zuletzt konfigurierten Kalendereinstellungen auf Ihrem Gerät verwendet.

Suchen

Sie können über die Ansicht **Postfächer** oder **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.

Drucken von E-Mails, Kalenderereignissen oder eingebetteten Bilder unter iOS

Sie können jetzt E-Mails, Kalenderereignisse oder eingebettete Bilder von Ihrem iOS-Gerät aus drucken.

Voraussetzungen

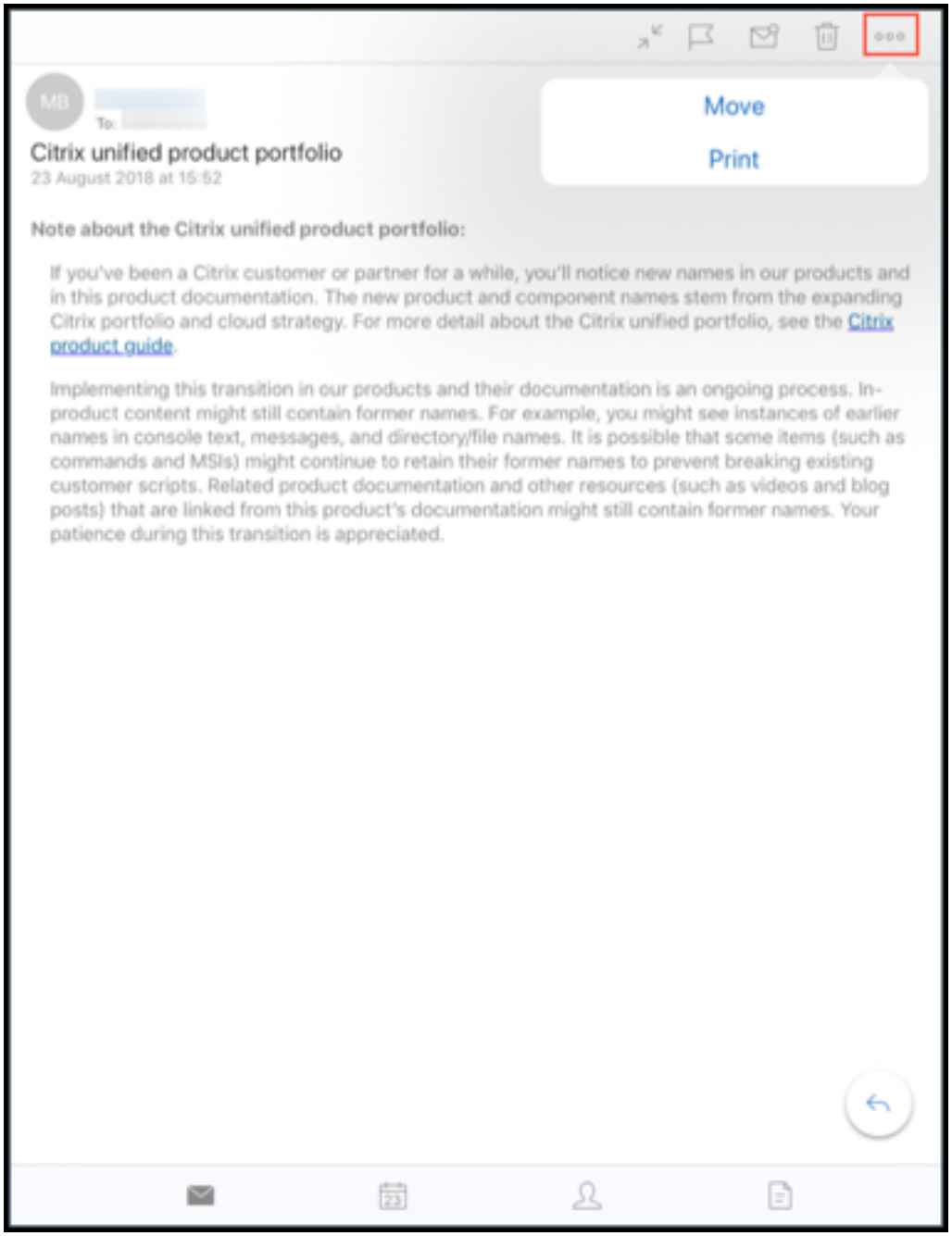
Stellen Sie zunächst sicher, dass die folgenden Anforderungen erfüllt sind:

- Die Option **AirPrint blockieren** ist auf **Aus** gestellt.
- Die Option **Benutzern das Drucken gestatten** ist in IRM deaktiviert.

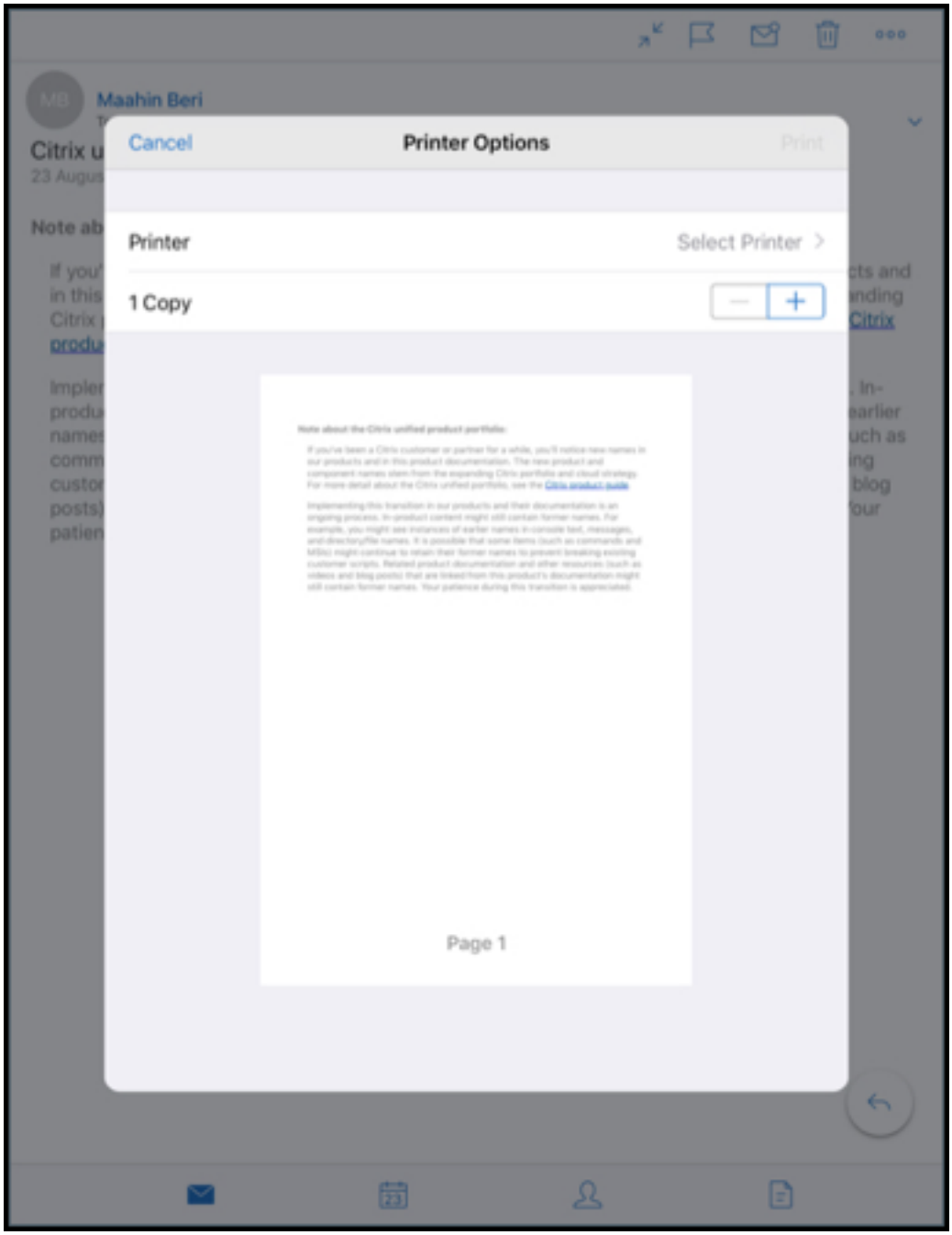
Standardmäßig ist das Drucken in Secure Mail für iOS aktiviert. Die Druckfunktion kann von Ihrem Administrator über Verwaltungsrichtlinien mit Apple AirPrint oder Microsoft Verwaltung von Informationsrechten (IRM) gesteuert werden. In diesen Szenarios funktioniert das Drucken einer E-Mail, eines Kalenderereignisses oder eines eingebetteten Bildes nicht und es wird möglicherweise eine Fehlermeldung angezeigt.

Drucken von E-Mails

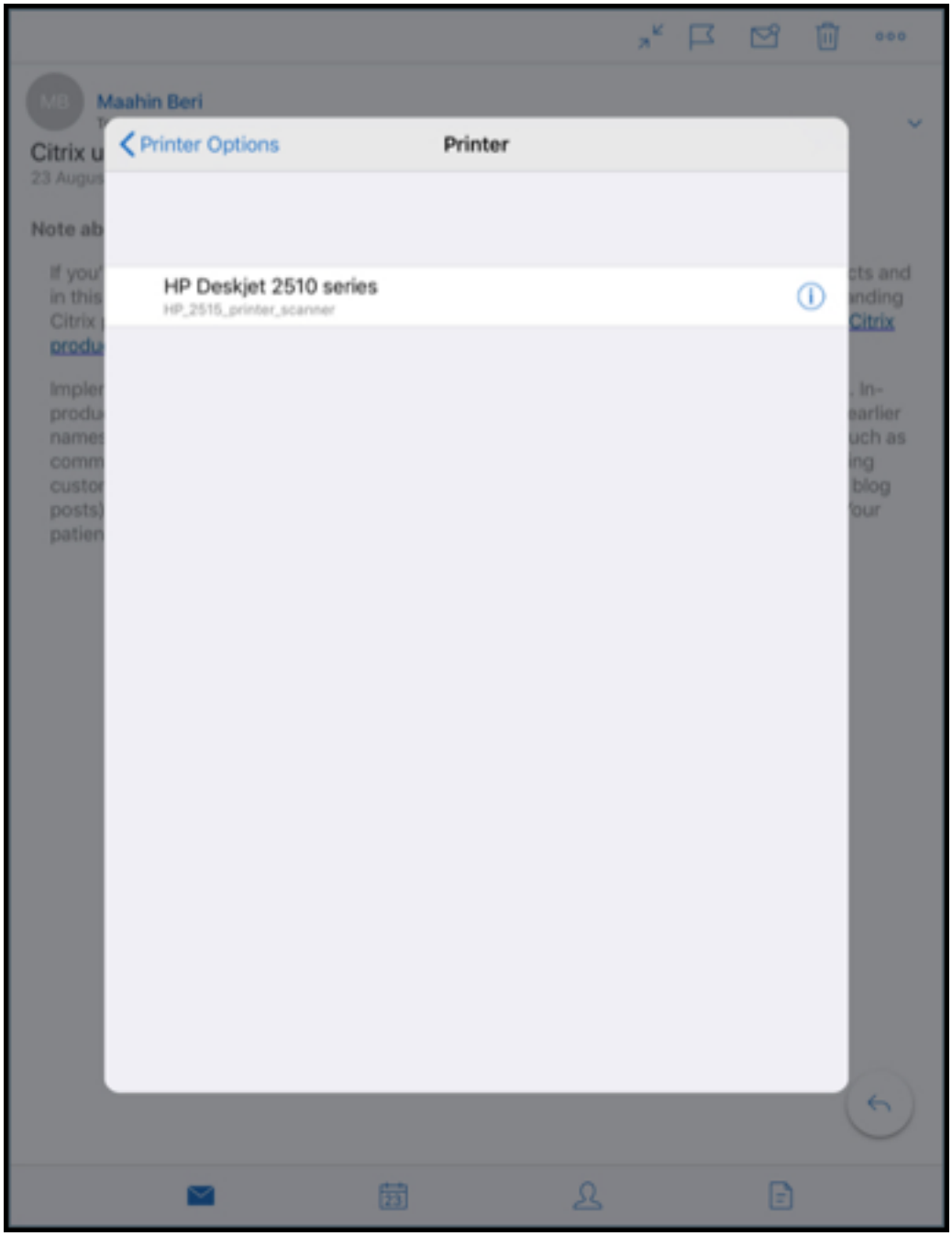
1. Öffnen Sie das E-Mail-Element, das Sie drucken möchten.
2. Tippen Sie auf oben links auf dem Bildschirm auf das Symbol “Mehr”. Die folgenden Optionen werden angezeigt:
    - Verschieben
    - Drucken



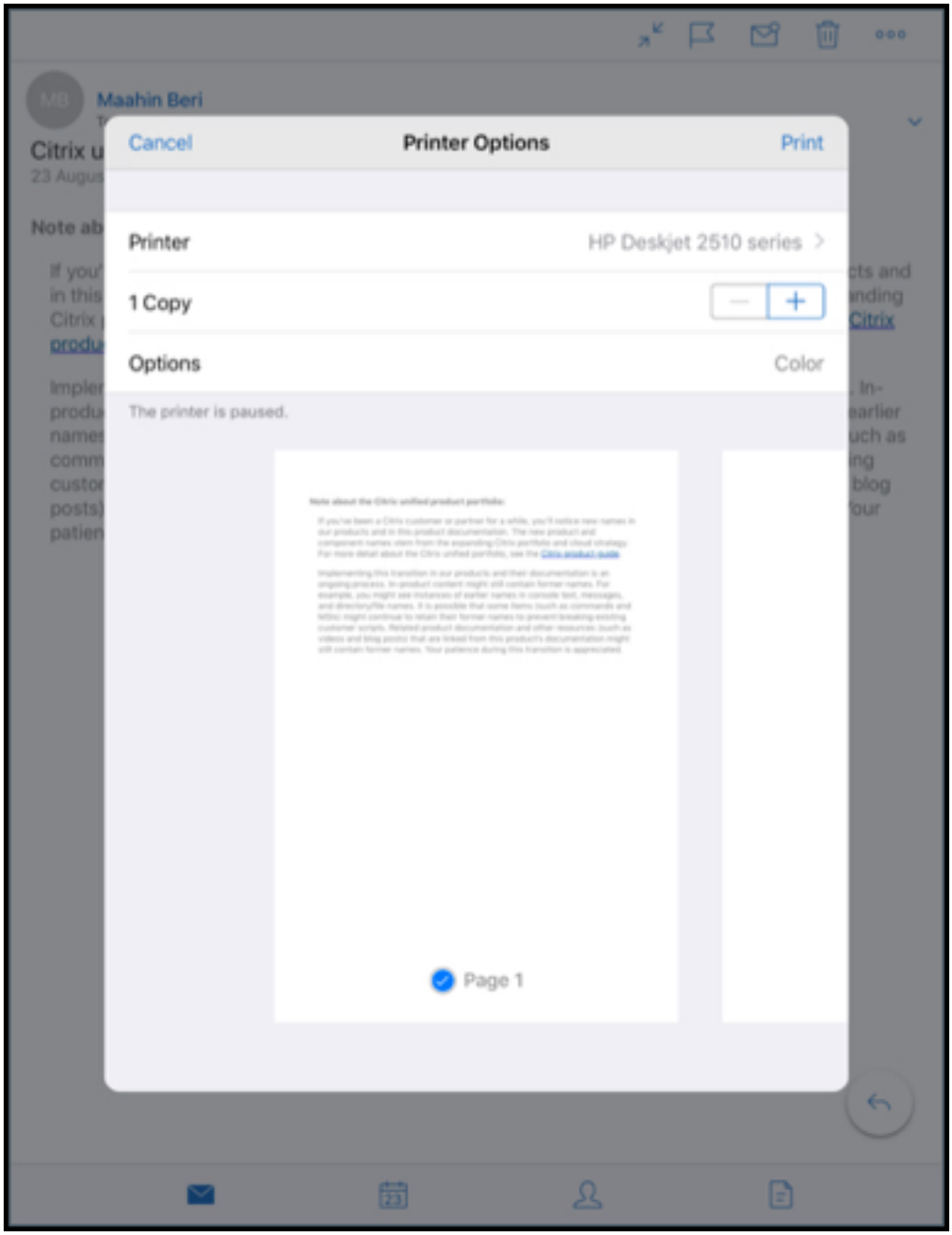
3. Tippen Sie auf **Drucken**.
   Die **Druckeroptionen** werden angezeigt.



4. Wählen Sie einen Drucker, tippen Sie auf **Drucker wählen**.
   Der Bildschirm **Drucker** wird angezeigt.

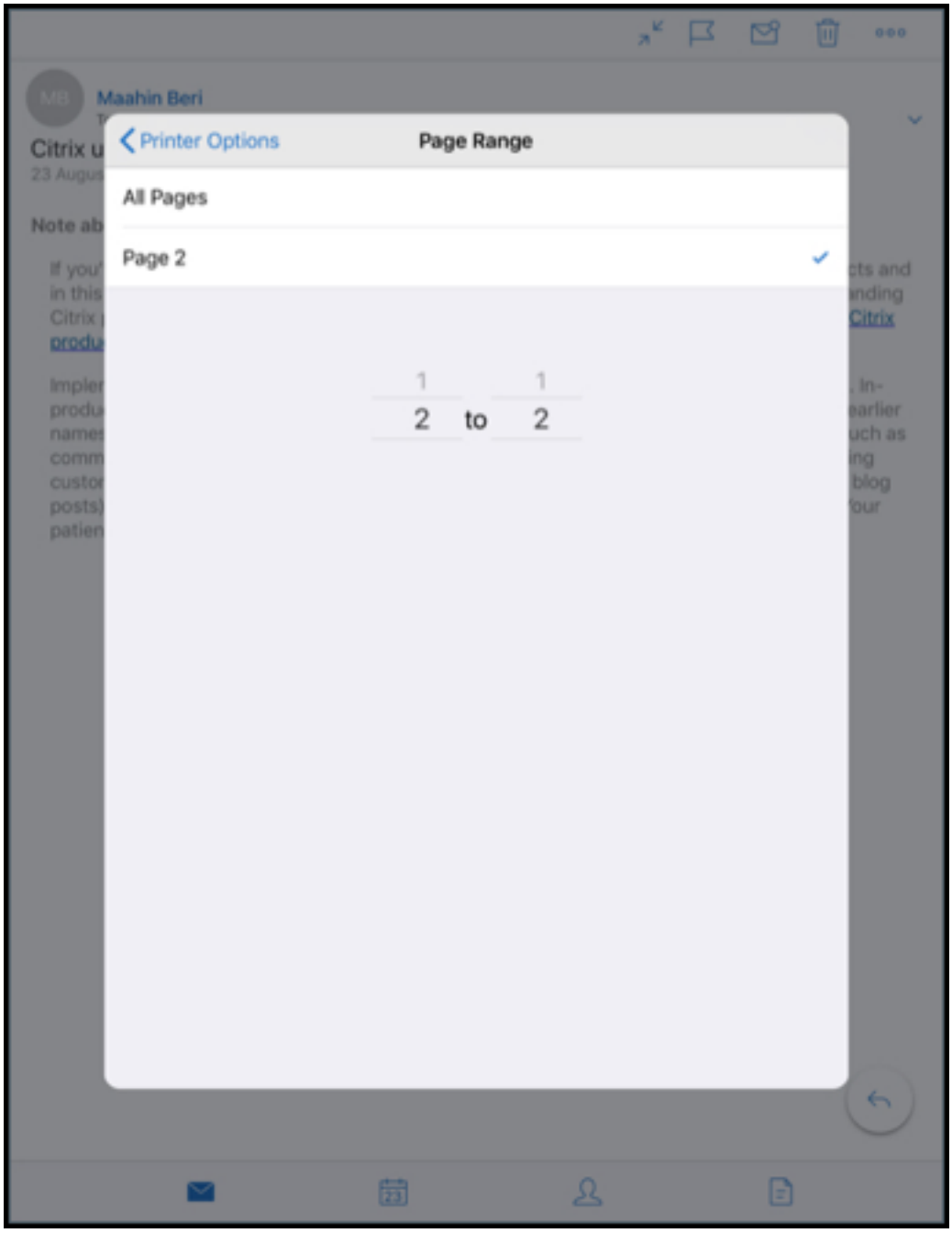


5. Wählen Sie den Drucker, auf dem Sie drucken möchten.

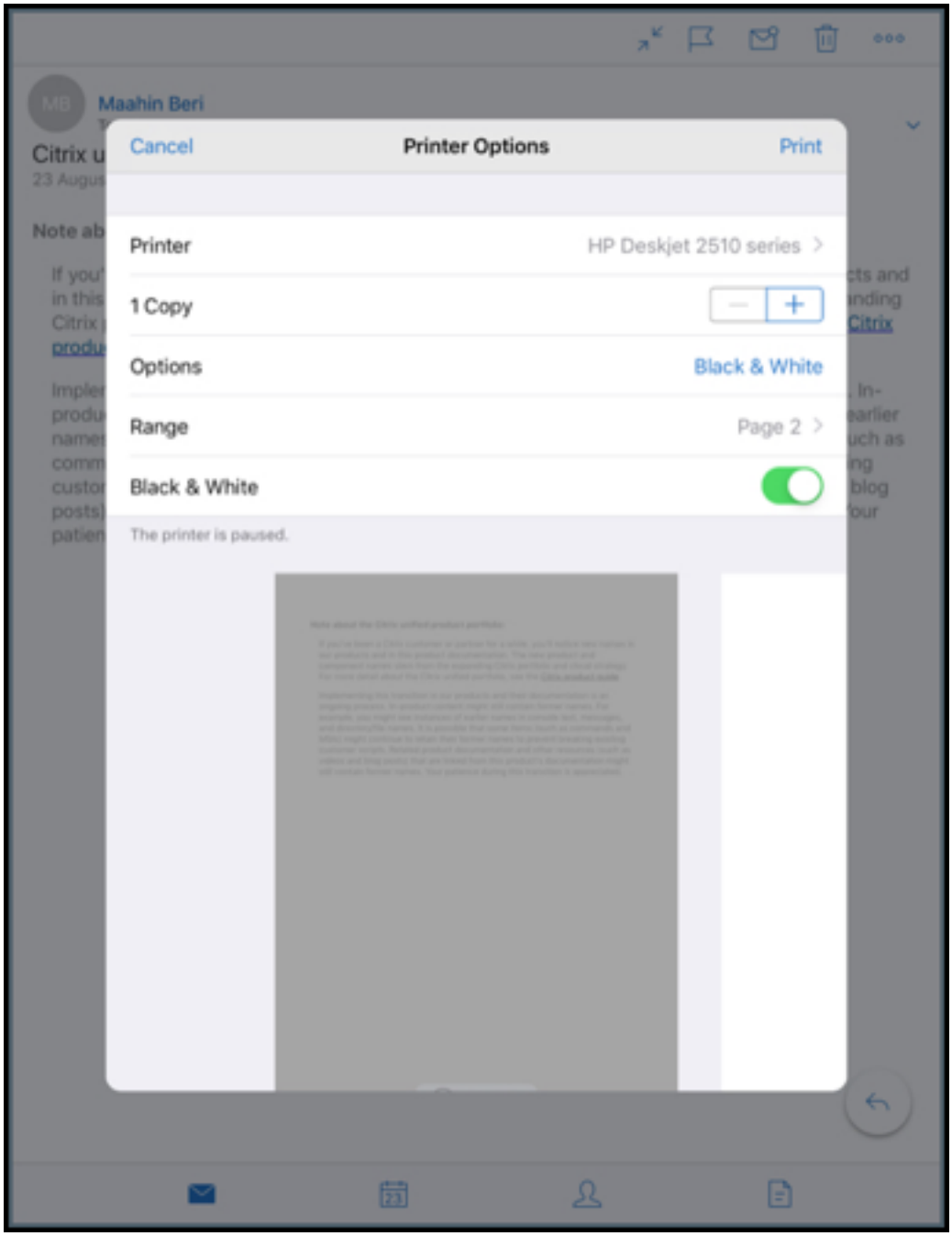


6. Tippen Sie auf **-** oder **+**, um die Anzahl der zu druckenden Kopien zu verringern oder zu erhöhen.
7. Um eine bestimmte Seite oder einen Bereich von Seiten zu drucken, tippen Sie auf **Bereich**. Der Bildschirm **Seitenbereich** wird angezeigt. Standardmäßig ist **Alle Seiten** ausgewählt.

8. Um die Seitenauswahl zu ändern, wischen Sie die Seitennummern nach oben oder unten.



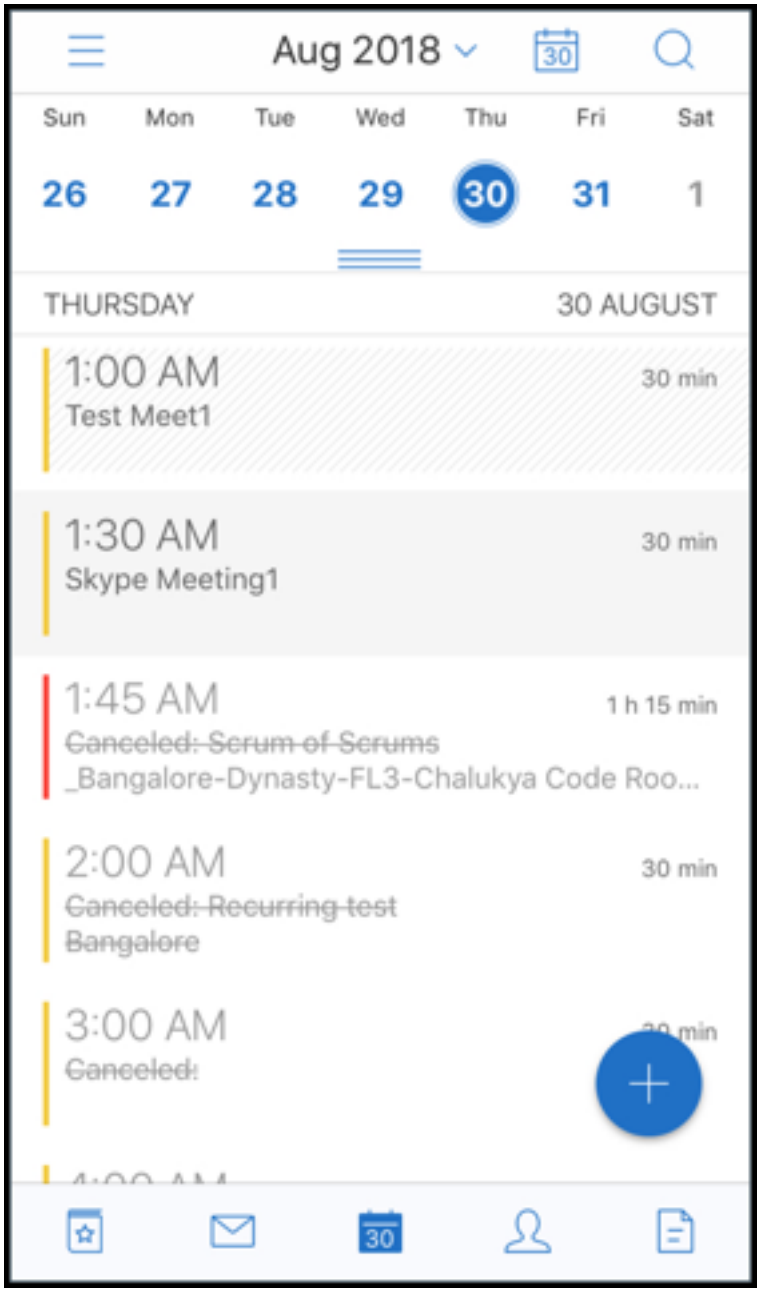
9. Tippen Sie auf **Druckeroptionen**, um zum Bildschirm **Druckeroptionen** zurückzukehren.



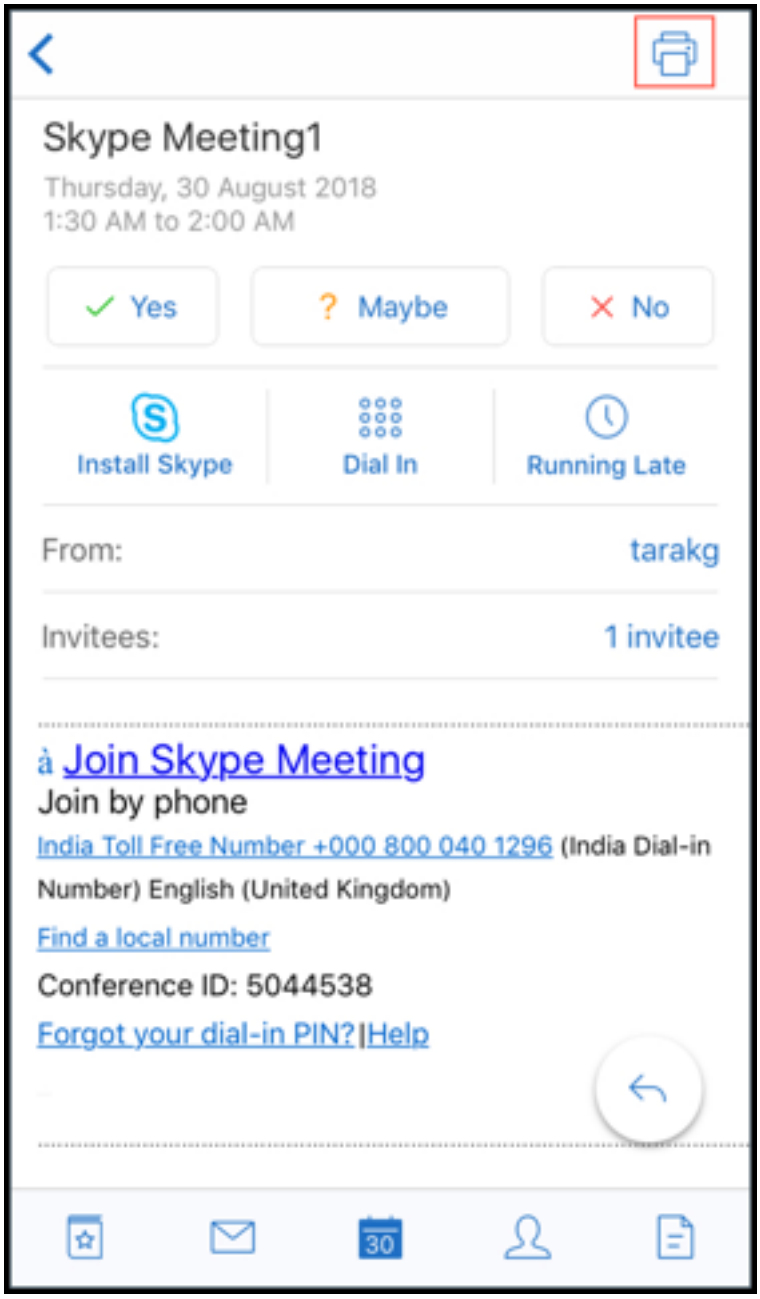
10. Um in Schwarzweiß zu drucken, tippen Sie auf die Schaltfläche **Schwarzweiß**. Standardmäßig druckt Secure Mail in Farbe.
11. Tippen Sie oben rechts auf **Drucken**, um die E-Mail zu drucken.
12. Um den Druckauftrag abzubrechen, tippen Sie oben links auf **Abbrechen**.

Drucken von Kalenderereignissen

1. Navigieren Sie zum Kalender und wählen Sie ein Ereignis aus.

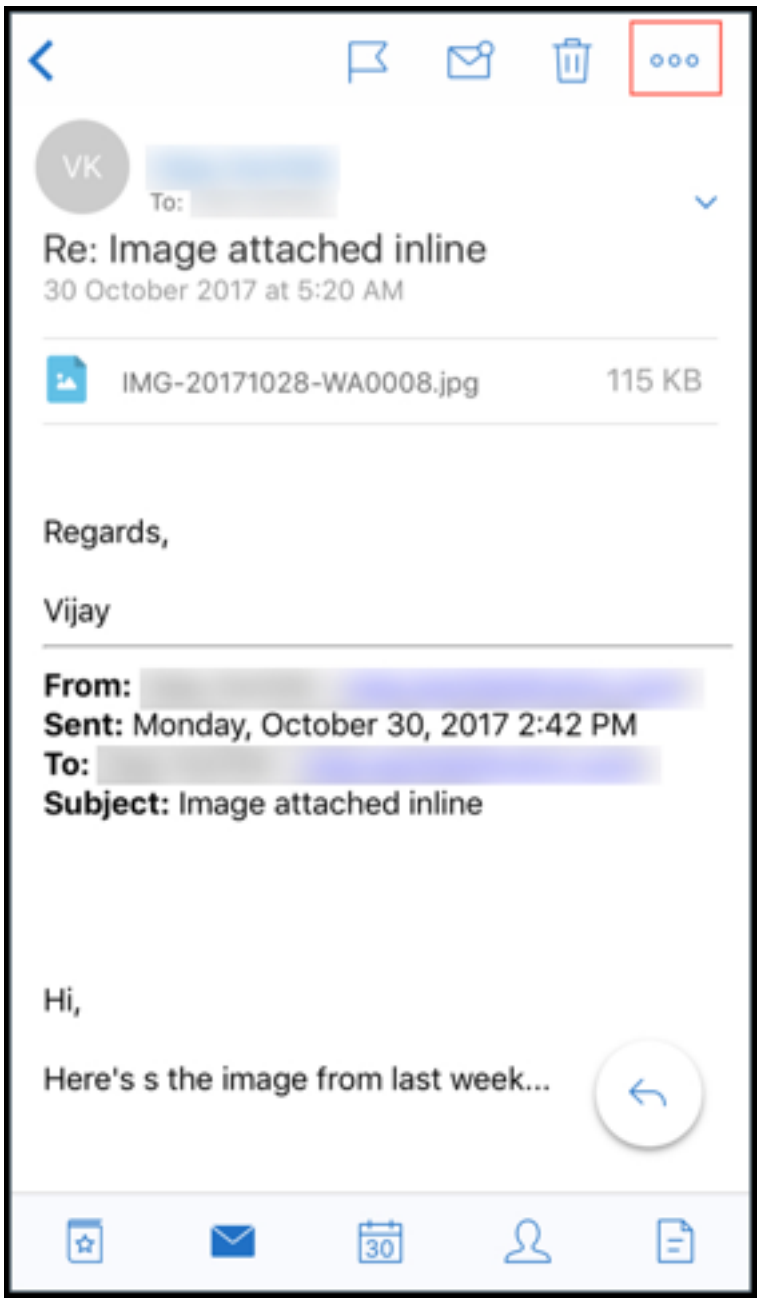


2. Tippen Sie auf das Symbol “Drucken”und folgen Sie den gleichen Anweisungen wie weiter oben im Abschnitt **Drucken von E-Mails**.



Drucken von eingebetteten Bildern:

1. Öffnen Sie das E-Mail-Element mit dem eingebetteten Bild.
2. Tippen Sie auf das Symbol “Mehr”. Die folgenden Optionen werden angezeigt:
    - Verschieben
    - Drucken
    - Abbrechen



3. Tippen Sie auf **Drucken** und folgen Sie den Anweisungen im Abschnitt **Drucken von E-Mails** weiter oben.

Mehrere Konferenzcodes (Einwahl in eine Besprechung)

Secure Mail für iOS unterstützt mehrere Konferenzcodes. Sie können jetzt einen Code aus der Liste verfügbarer Konferenzcodes auswählen, um an einer Besprechung teilzunehmen.

Einwahl in eine Besprechung

1. Öffnen Sie eine Besprechungseinladung und tippen Sie auf **Einwählen**.
2. Wählen Sie aus der Liste der angezeigten Telefonnummern eine Telefonnummer aus.
3. Wählen Sie aus der Liste der angezeigten Konferenzcodes einen Code aus, um an der Besprechung teilzunehmen.
4. Tippen Sie auf **Anrufen**, um an der Besprechung teilzunehmen.

Unterstützung für das Drucken von E-Mail-Anlagen

Secure Mail für iOS unterstützt das Drucken von E-Mail-Anlagen.

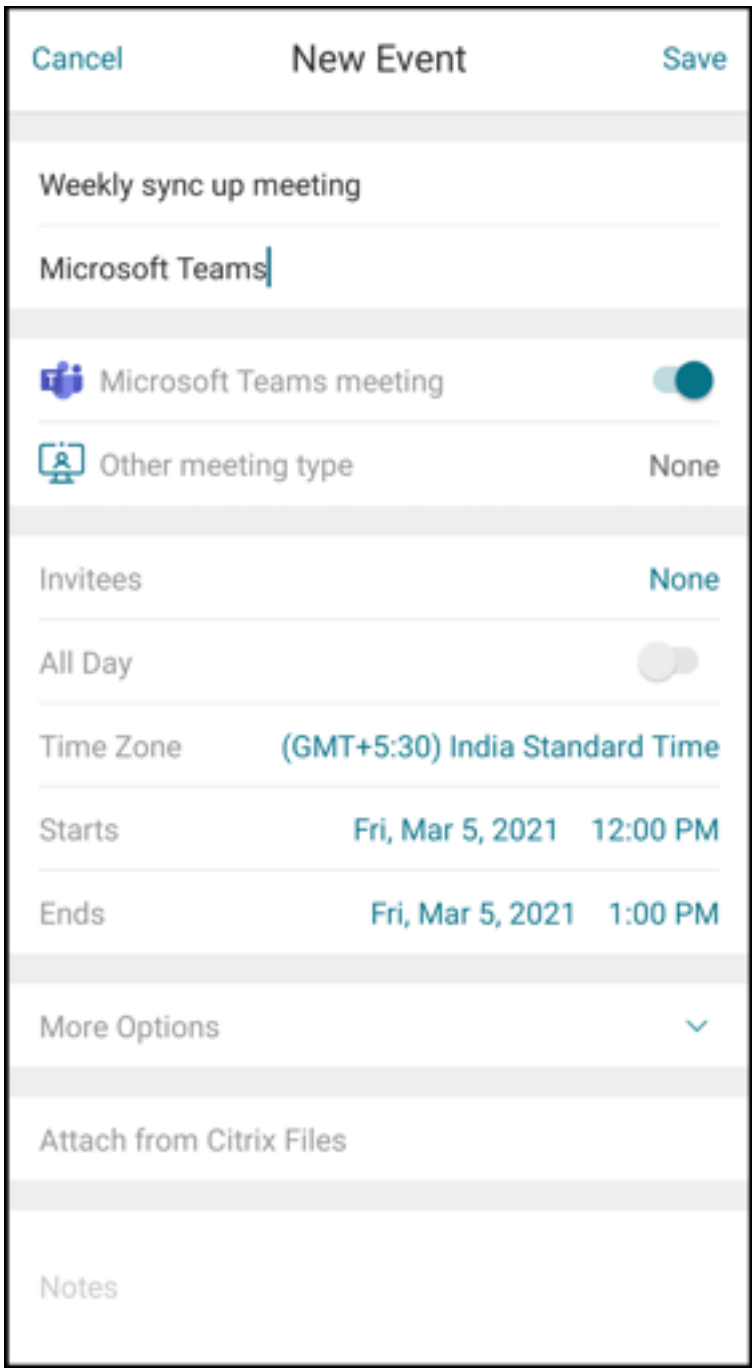
Android-Features

June 6, 2024

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

Erstellen von Microsoft Teams-Besprechungen in Secure Mail-Kalenderereignissen

In Secure Mail für Android können Sie Einladungen für Microsoft Teams-Besprechungen erstellen, während Sie Kalenderereignisse erstellen. Um eine Microsoft Teams-Besprechung zu erstellen, aktivieren Sie die Umschaltfläche **Microsoft Teams-Besprechung**. Der Link zur Besprechungseinladung und die Details werden automatisch mit den Ereignisdetails gesendet.

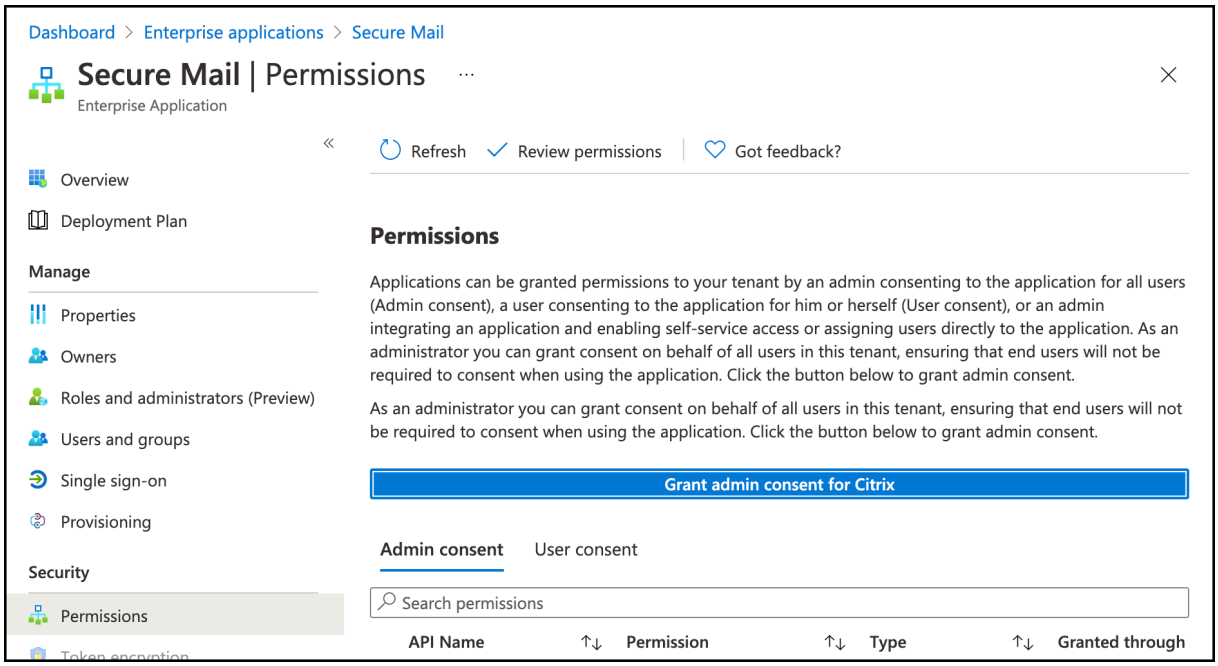


Voraussetzungen:

Stellen Sie sicher, dass der globale Administrator von Azure Active Directory folgende Schritte ausführt:

- Die moderne Authentifizierung (OAuth) aktiviert und sicherstellt, dass ein Exchange Online oder ein Postfachbenutzer mit einer gültigen Microsoft Teams-Lizenz verwendet wird.
- Mandantenweite Admin-Zustimmung für die Secure Mail-App gewährt.
- Das Exchange-Konto in der Secure Mail-App konfiguriert und die App-Berechtigung für alle Be-

nutzer zulässt, die sich anmelden. Sie sehen den folgenden Bildschirm:



- Aktivieren Sie die Microsoft Teams-Integrationsrichtlinie.

Einschränkungen:

Für Meetings, die mit Secure Mail erstellt wurden, hat das Feature derzeit die folgenden Einschränkungen für den Microsoft Outlook-Kalender:

- Die Option **Online teilnehmen** ist nicht verfügbar
- Die Benachrichtigung **Die Besprechung hat begonnen** ist nicht verfügbar

2-Wege-Kontaktsynchronisierung

In Secure Mail für Android können Sie Secure Mail-Kontakte aus Ihrer lokalen Kontaktliste erstellen, bearbeiten und löschen.

Senden von E-Mails rückgängig machen

In Secure Mail für Android können Sie das Senden von E-Mail rückgängig machen. Sobald Sie auf die Schaltfläche **Senden** tippen, erhalten Sie eine Popupmeldung, mit der Sie das Senden rückgängig machen können. Tippen Sie auf **Rückgängig**, um das Senden rückgängig zu machen, die E-Mail oder die E-Mail-Empfänger zu bearbeiten, Anlagen anzuhängen oder zu entfernen oder die E-Mail zu verwerfen.

Anlagen im Ordner Entwürfe synchronisieren

Wenn der Ordner **Entwürfe** in Secure Mail für Android synchronisiert wird, werden die Anlagen auch synchronisiert und sind auf allen Geräten verfügbar. Dieses Feature ist für Geräte verfügbar, in denen Exchange ActiveSync Version 16 oder höher ausgeführt wird.

In-App-Ansicht von PDF-Dateien

In Secure Mail für Android können Sie PDF-Dateien in der App anzeigen, auch Lesezeichen und Anmerkungen. Ebenfalls verfügbar ist die erweiterte Ansicht anderer Microsoft Office-Anlagen.

Richtlinie “Web-SSO zum Tunneln verwenden”für Umgebungen, die moderne Authentifizierung mit Microsoft Office 365 ausführen

In Secure Mail für Android wird eine neue Richtlinie **Web-SSO zum Tunneln verwenden** eingeführt. Mit dieser Richtlinie können Sie OAuth-Datenverkehr über Web-SSO tunneln. Vorgehensweise:

- Legen Sie Richtlinie **Web-SSO zum Tunneln verwenden** auf **Ein** fest.
- Wählen Sie die Option **Tunnel - Web-SSO** für die Netzwerkzugriffsrichtlinie.
- Schließen Sie alle Hostnamen, die mit OAuth in Verbindung stehen, von der Richtlinie für **Hintergrunddienste** aus.

Drag & Drop für Kalendereereignisse

In Secure Mail für Android können Sie die Zeit eines vorhandenen Kalendereereignisses durch Drag & Drop ändern. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Kalendereereigniszeit ändern.

Unterstützung für 64-Bit-Apps für Google Play

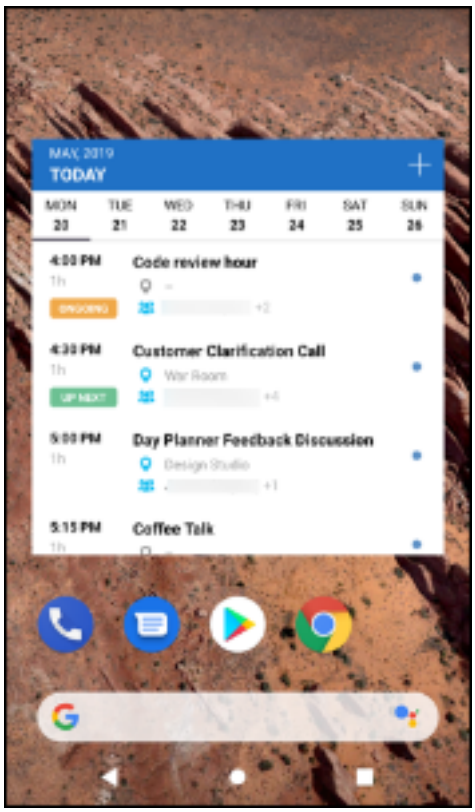
Secure Mail für Android unterstützt 64-Bit-Architekturen.

Verbesserte Funktion “Zum Aktualisieren ziehen”in Secure Mail für Android

In Übereinstimmung mit den Material Design-Richtlinien haben wir kleinere Verbesserungen am Aktualisieren durch Ziehen gemacht. Der Synchronisierungszeitstempel ist unten auf dem Bildschirm verfügbar, wenn Sie auf das Hamburgersymbol tippen.

Widget für Kalenderagenda

In Secure Mail für Android ist die **Kalenderagenda** als Widget verfügbar. Von diesem Widget können Sie die bevorstehenden Ereignisse im **Kalender** für eine Woche anzeigen. Mit diesem Feature können Sie ein **Kalenderereignis** erstellen, ein vorhandenes Ereignis anzeigen und die Details bearbeiten. Die Richtlinie **Screenshot blockieren** gilt nicht für das auf dem Startbildschirm platzierte Widget. Sie können das Widget jedoch mit der Richtlinie **Kalenderwidget zulassen** deaktivieren.



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 parallel über “Tunnel - Web-SSO”und die Secure Ticket Authority (STA) tunneln. Sie können auch Verbindungen mit “Tunnel - Web-SSO”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 unter Hinzufügen einer MDX-App.
2. Klicken Sie für die Netzwerkzugriffsrichtlinie auf die Option **Tunnel - Web-SSO**. Weitere Informationen finden Sie unter App-Netzwerkzugriff

Verbesserungen für Feed-Karten

Die folgenden Verbesserungen wurden am bestehenden Ordner **Feeds** in Secure Mail für Android vorgenommen:

- 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.

Anzeige von Anlagen

Secure Mail für Android ermöglicht die einfache Anzeige von E-Mail- und Kalenderanlagen. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Dateien anzeigen und anhängen.

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".

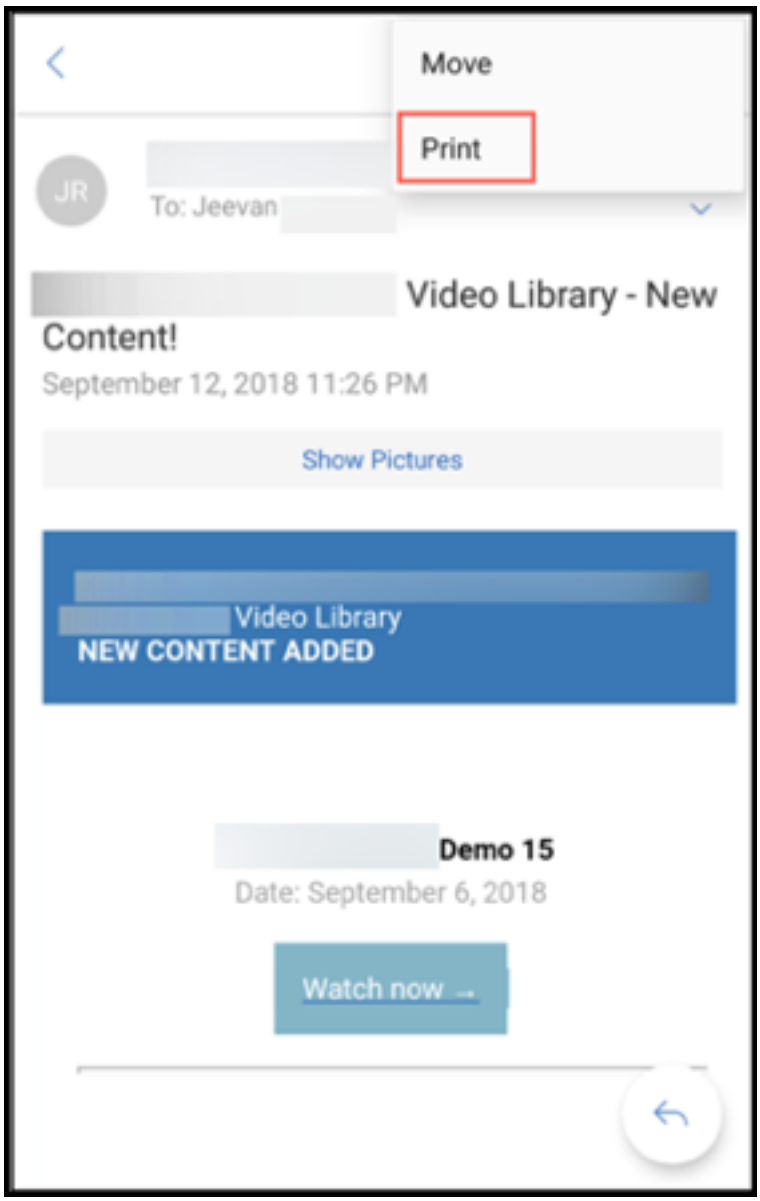
- Wenn eine E-Mail mit IRM geschützt ist, stellen Sie sicher, dass Sie in der E-Mail die Option **Benutzern das Drucken gestatten** aktivieren.

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

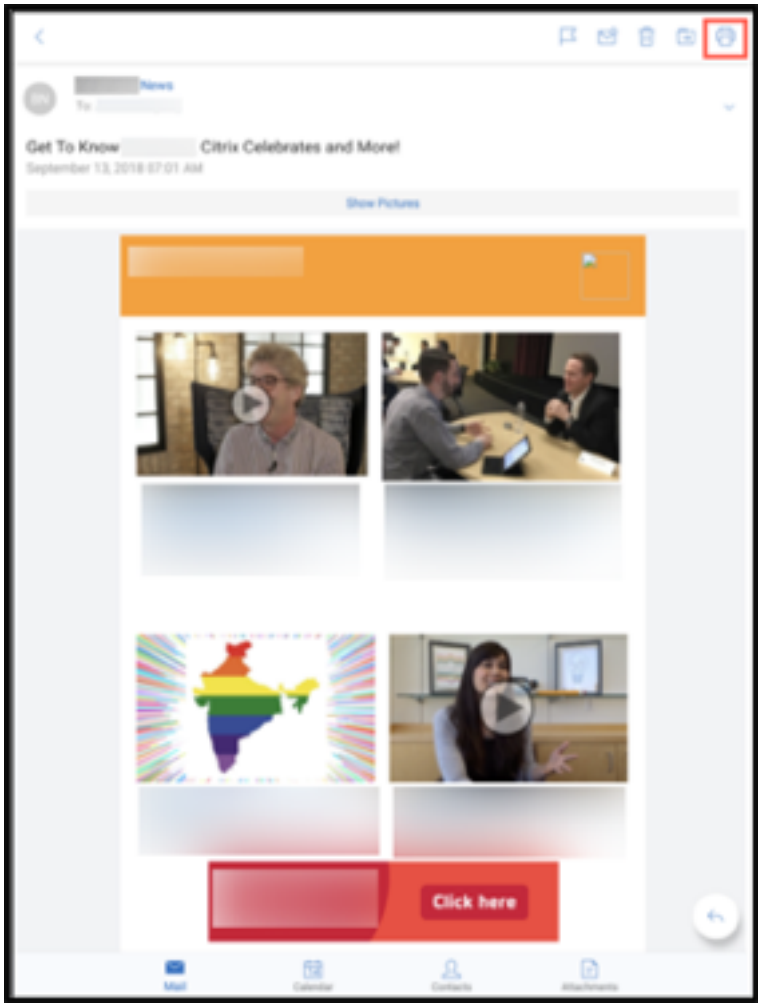
> **Hinweis:**
>
> Für diese Druckfunktion gelten die folgenden bekannten Einschränkungen:
>
> - Inlinebilder werden nur dann gedruckt, wenn sie durch Antippen von **Bilder anzeigen** heruntergeladen wurden. Wenn Sie nicht auf **Bilder anzeigen** tippen, werden nur die Bildplatzhalter gedruckt.
> - In 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



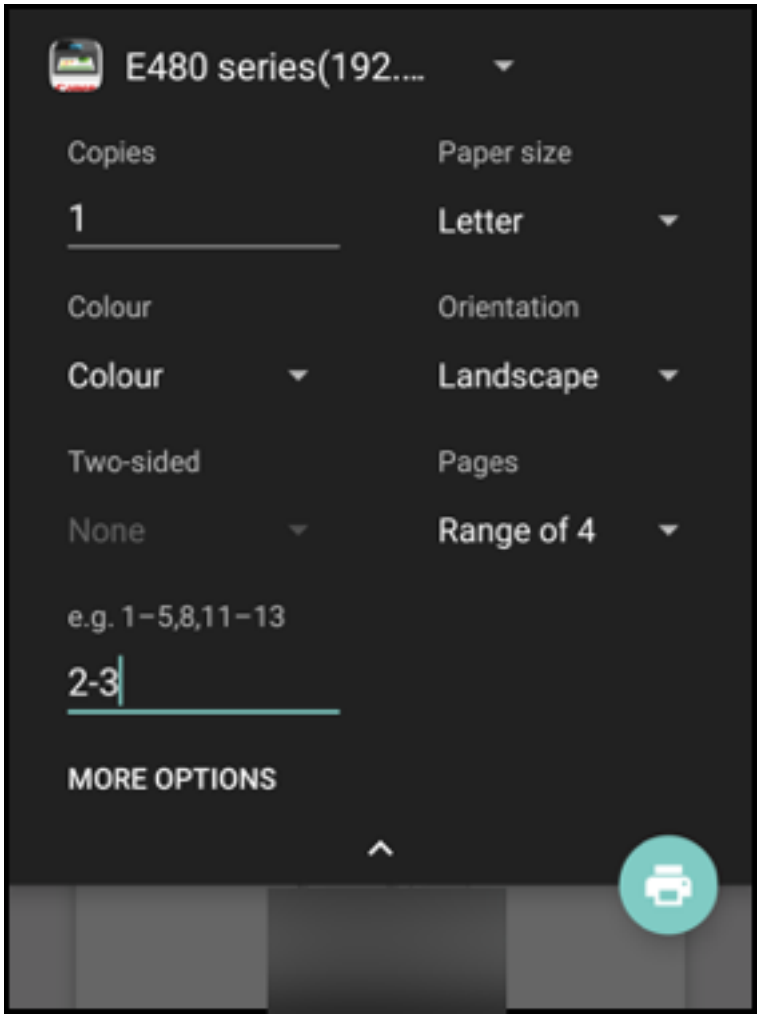
> **Hinweis:**
>
> Auf Tablets können Sie das Drucksymbol oben links auf dem Bildschirm verwenden, um eine E-Mail zu drucken.



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.



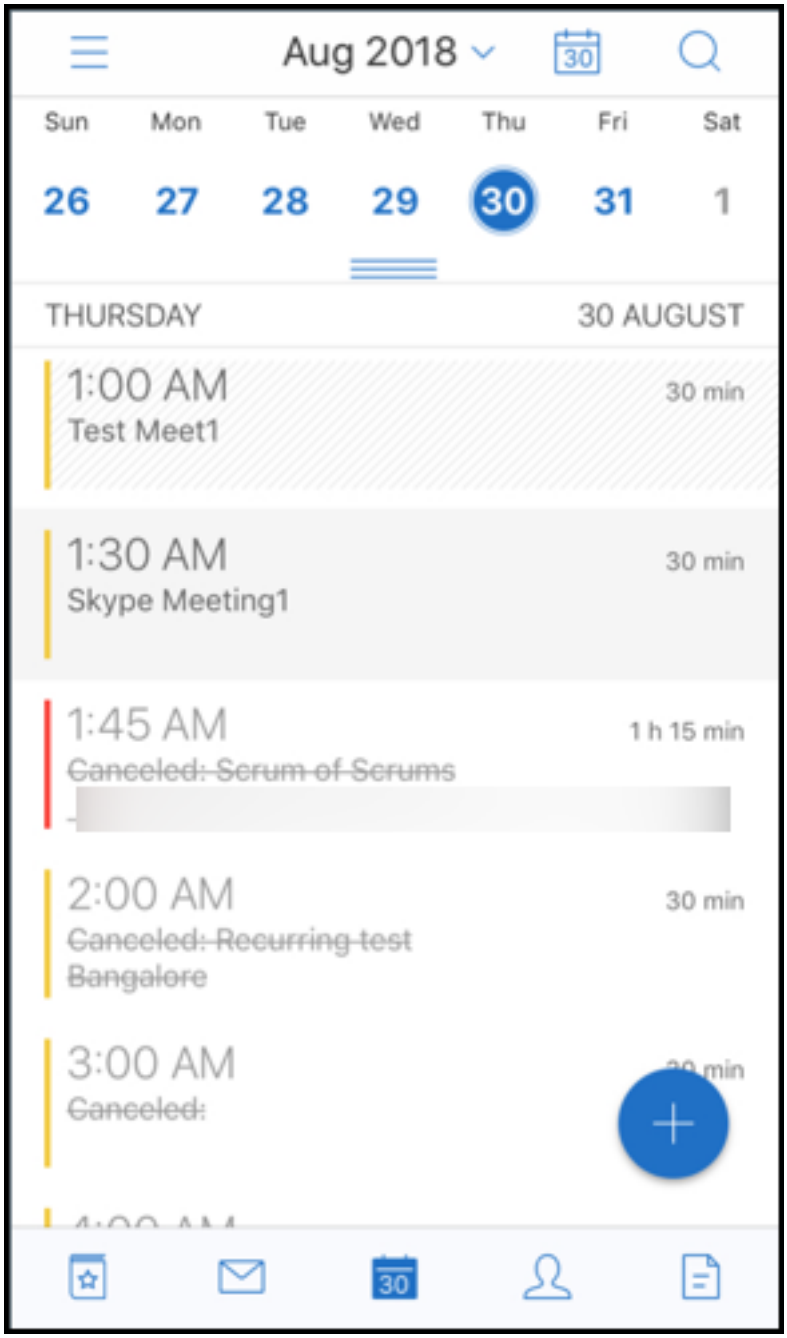
6. Wählen Sie den Drucker, auf dem Sie drucken möchten. Verwenden Sie die folgenden Druckoptionen:
    - Geben Sie die Anzahl der zu druckenden Exemplare ein.
    - Wählen Sie das Papierformat aus der Liste aus.
    - Wählen Sie die Farbe aus der Liste aus.
    - Wählen Sie die Seitenausrichtung.
    - 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

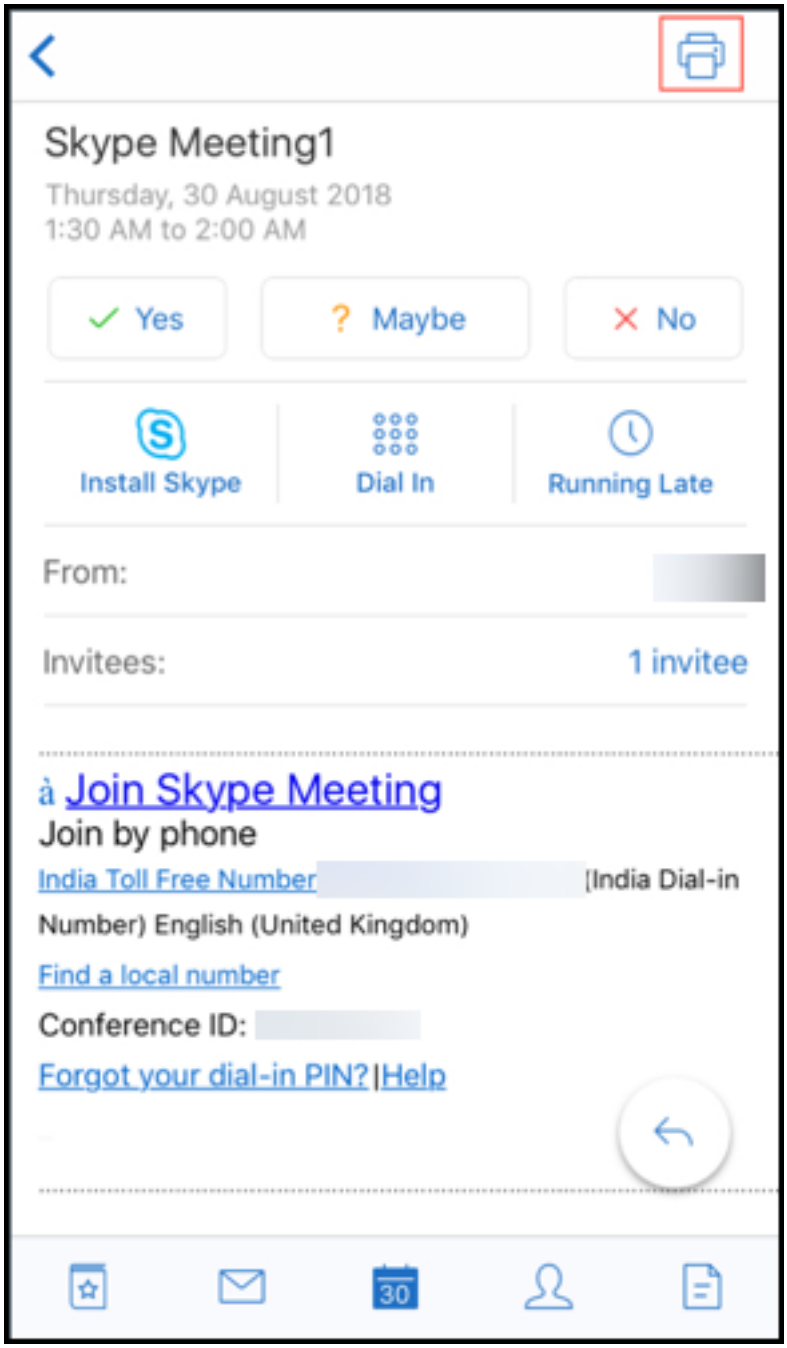
- Tippen Sie in der E-Mail auf **Bilder anzeigen** und folgen Sie den Anweisungen im Abschnitt Drucken von E-Mail oben.

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. Weitere Informationen zum Konfigurieren von MDX-Richtlinien für Secure Mail finden Sie unter MDX-Richtlinien für mobile Produktivitätsapps.

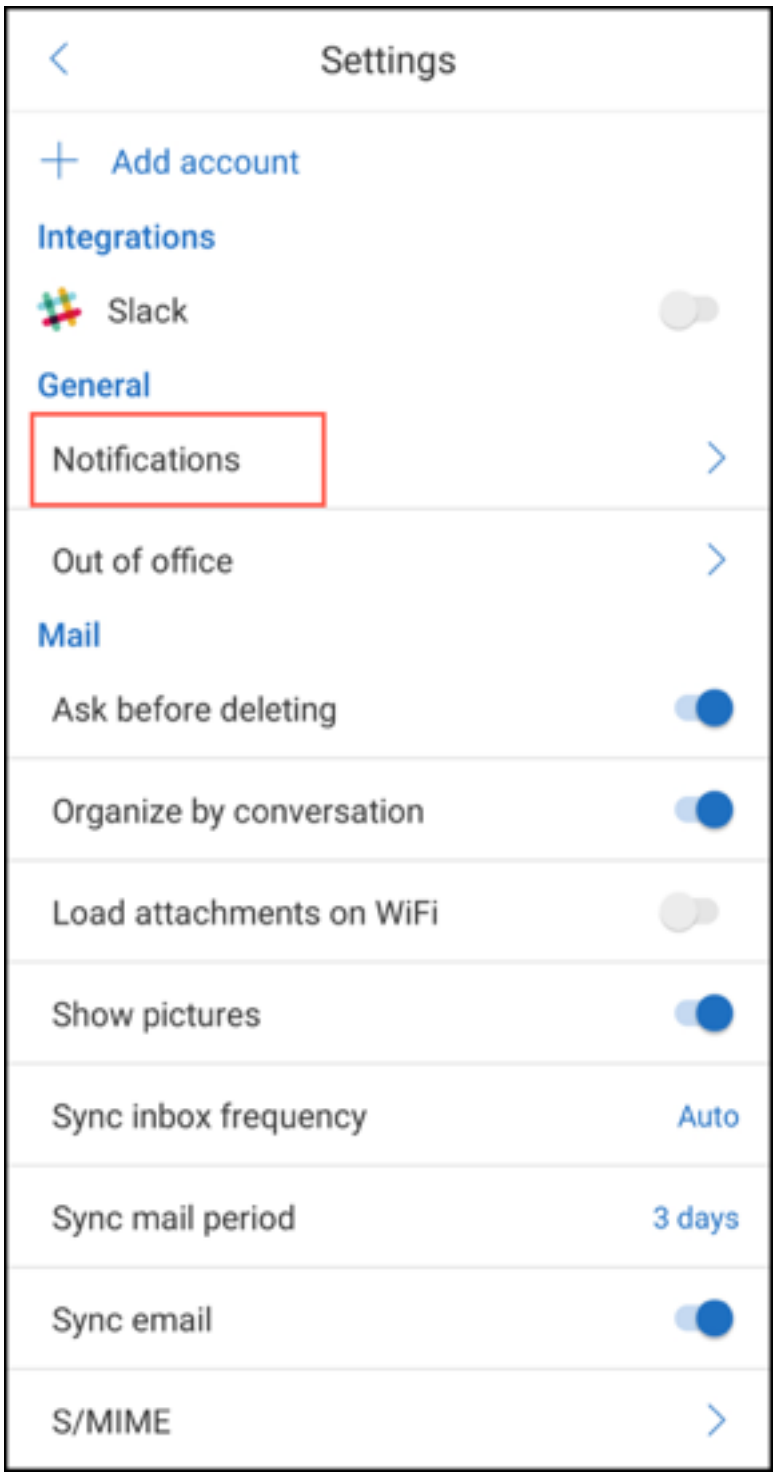
Unterordnerbenachrichtigungen

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

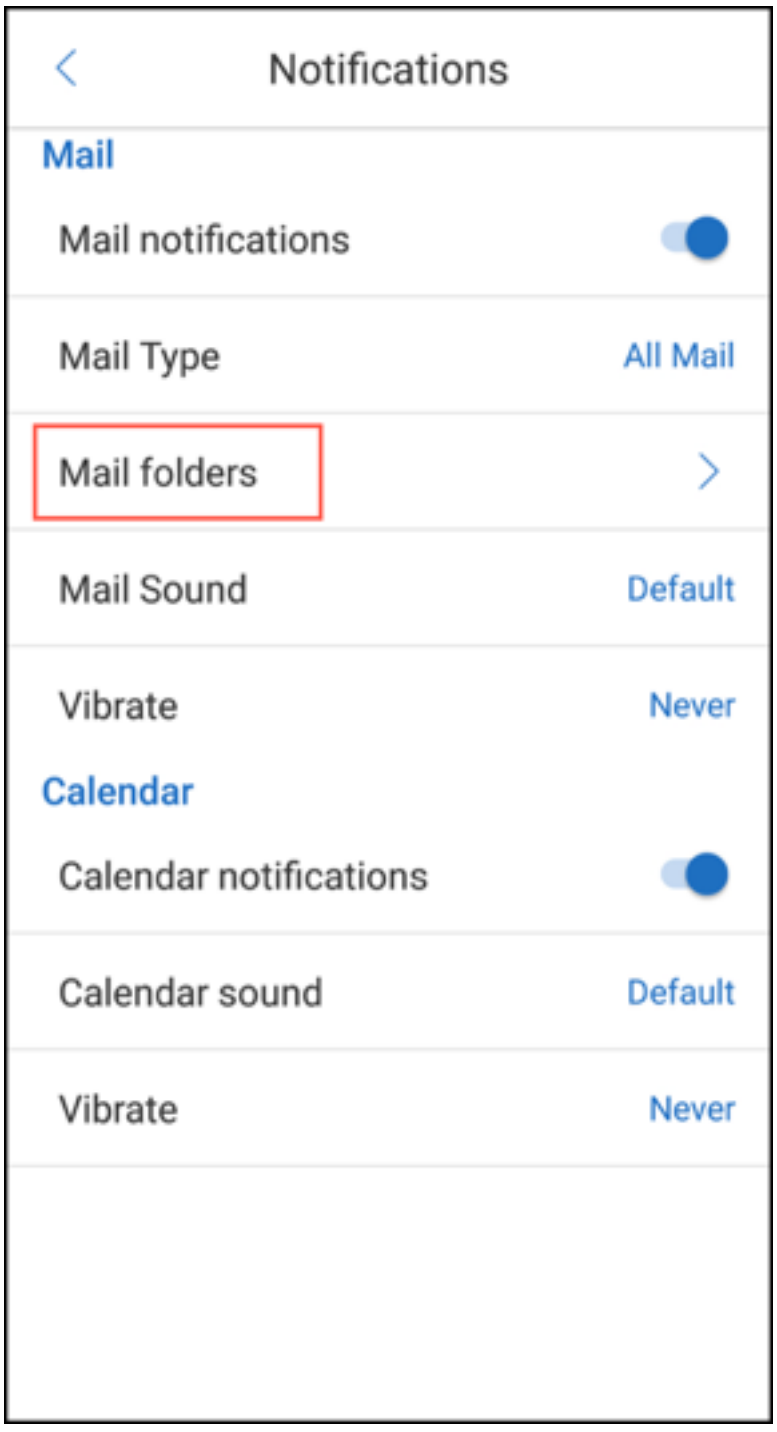
> **Hinweis:**
>
> - Stellen Sie sicher, dass FCM-basierte Pushbenachrichtigungen in der Endpoint Management-Konsole aktiviert sind, um Benachrichtigungen für Unterordner zu erhalten. Schritte zur Konfiguration von FCM-basierten Pushbenachrichtigungen finden Sie unter Pushbenachrichtigung für Secure 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**.



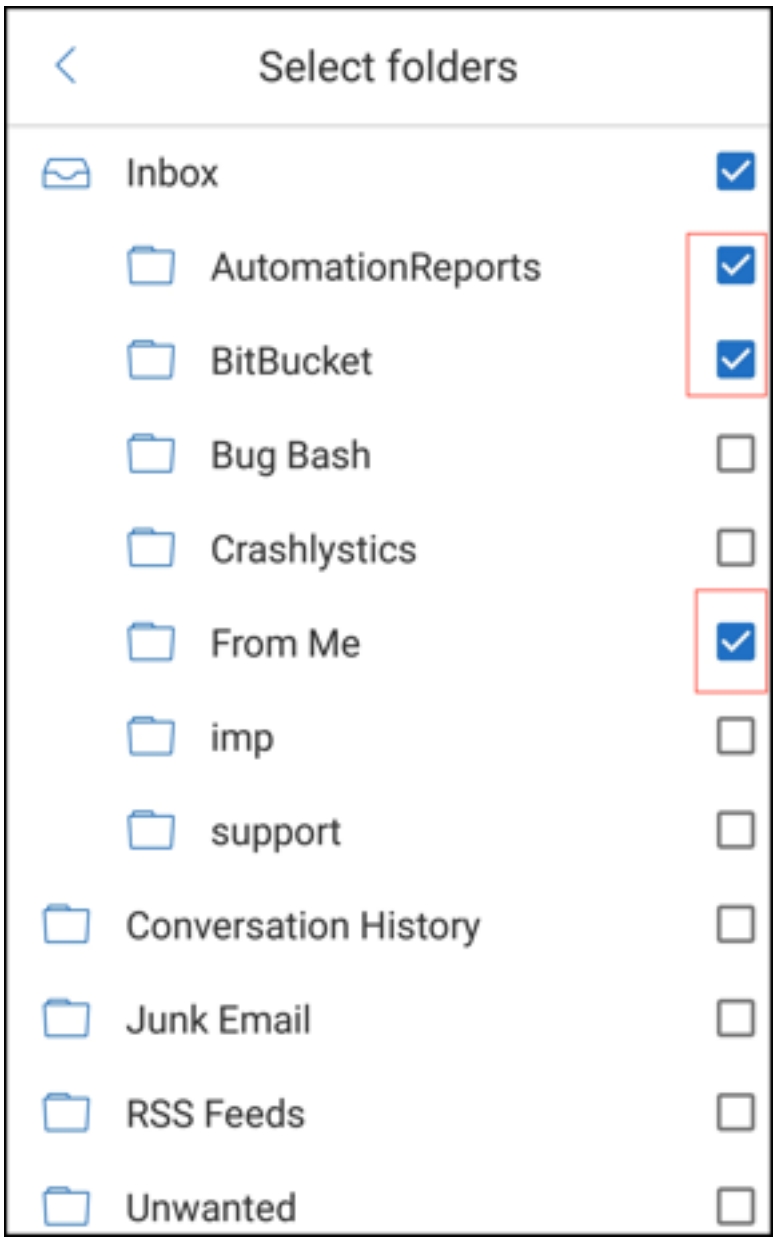
2. Tippen im Bildschirm **Benachrichtigungen** auf **E-Mail-Ordner**. Eine Liste der Unterordner des Posteingangs wird angezeigt.



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 Synchro-

> nisierung aktiviert.

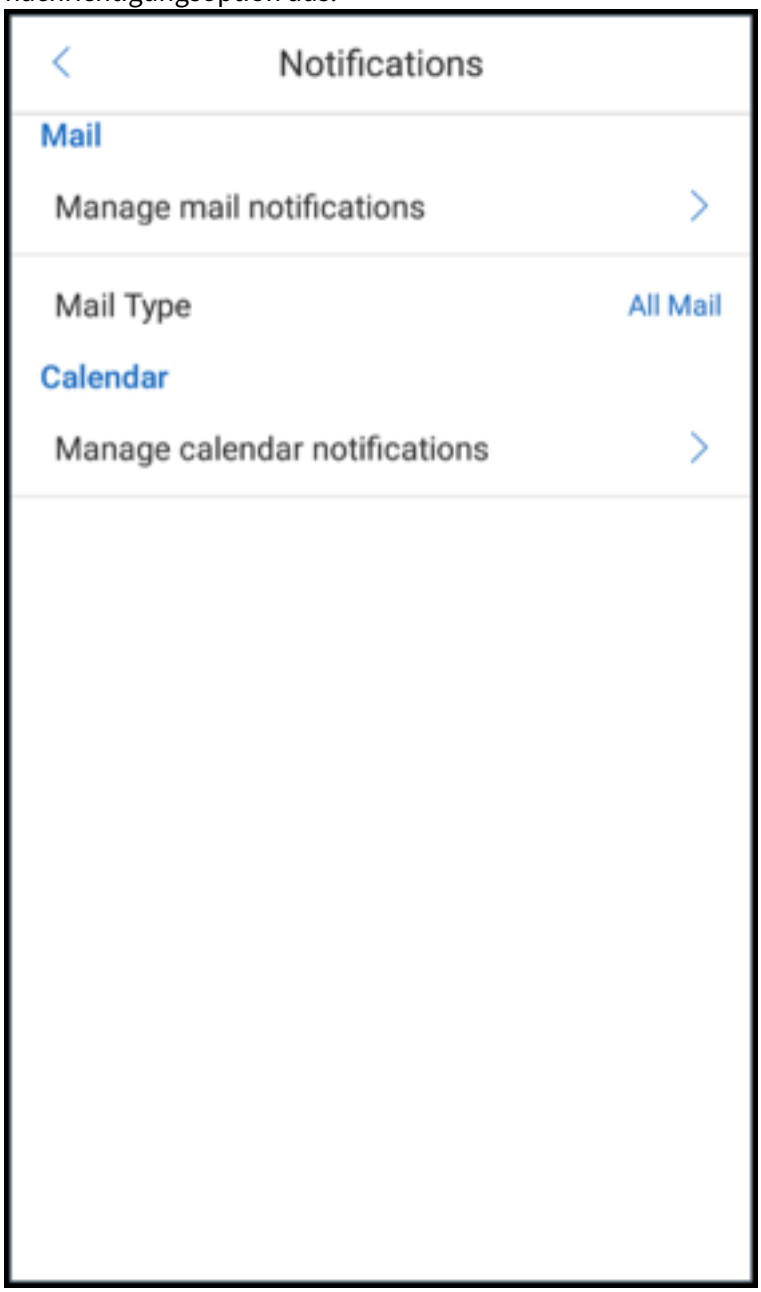


Zum Deaktivieren von Benachrichtigungen für spezifische Unterordner deaktivieren Sie deren Kontrollkästchen.

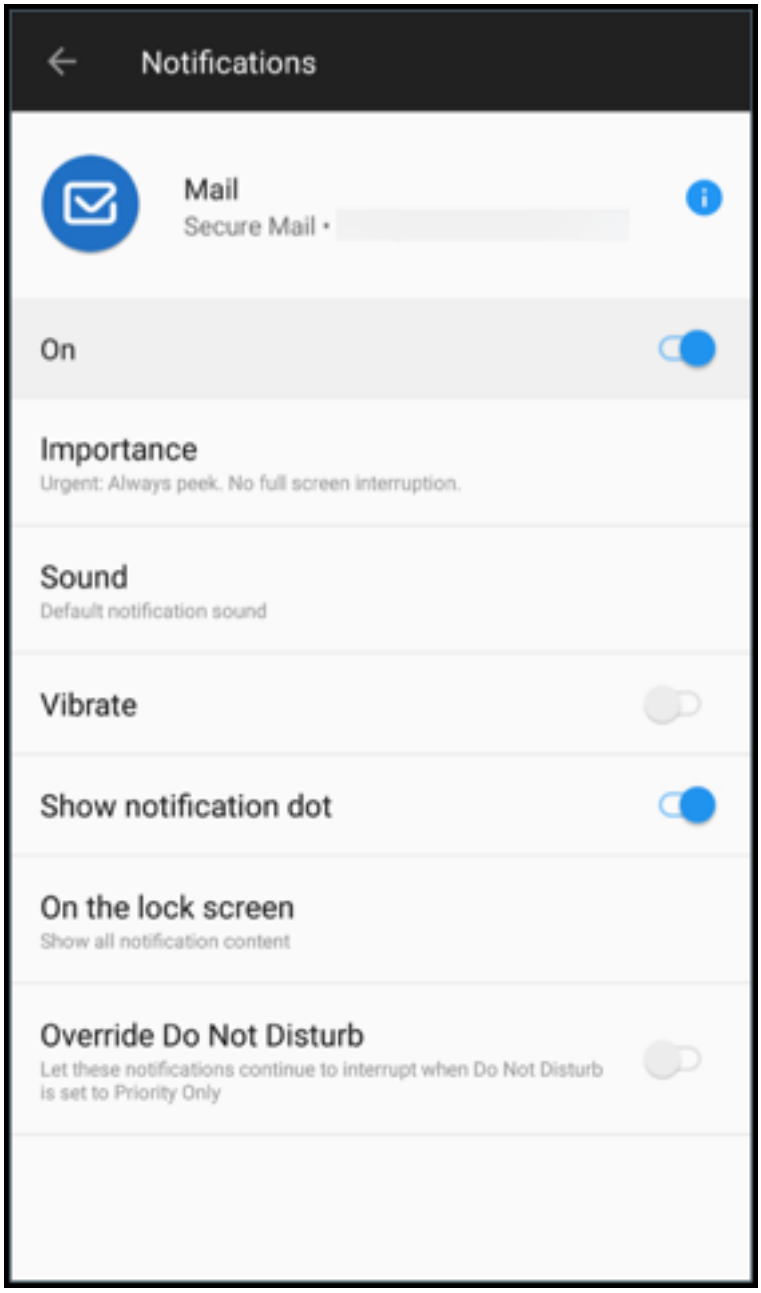
Benachrichtigungskanäle

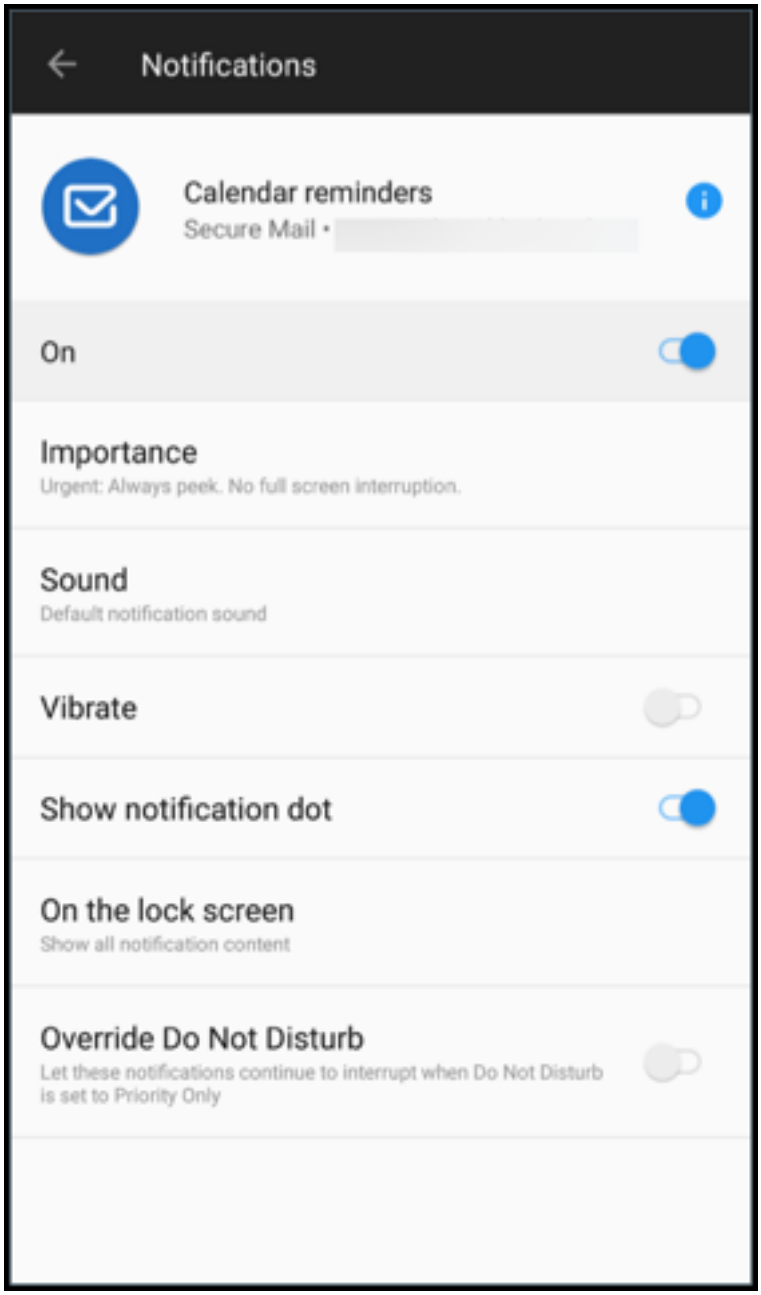
Auf Geräten mit Android O oder höher können Sie über die Einstellungen des Benachrichtigungskanals verwalten, wie Ihre E-Mail- und Kalenderbenachrichtigungen behandelt werden. Mit diesem Feature können Sie Ihre Benachrichtigungen anpassen und verwalten.

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.

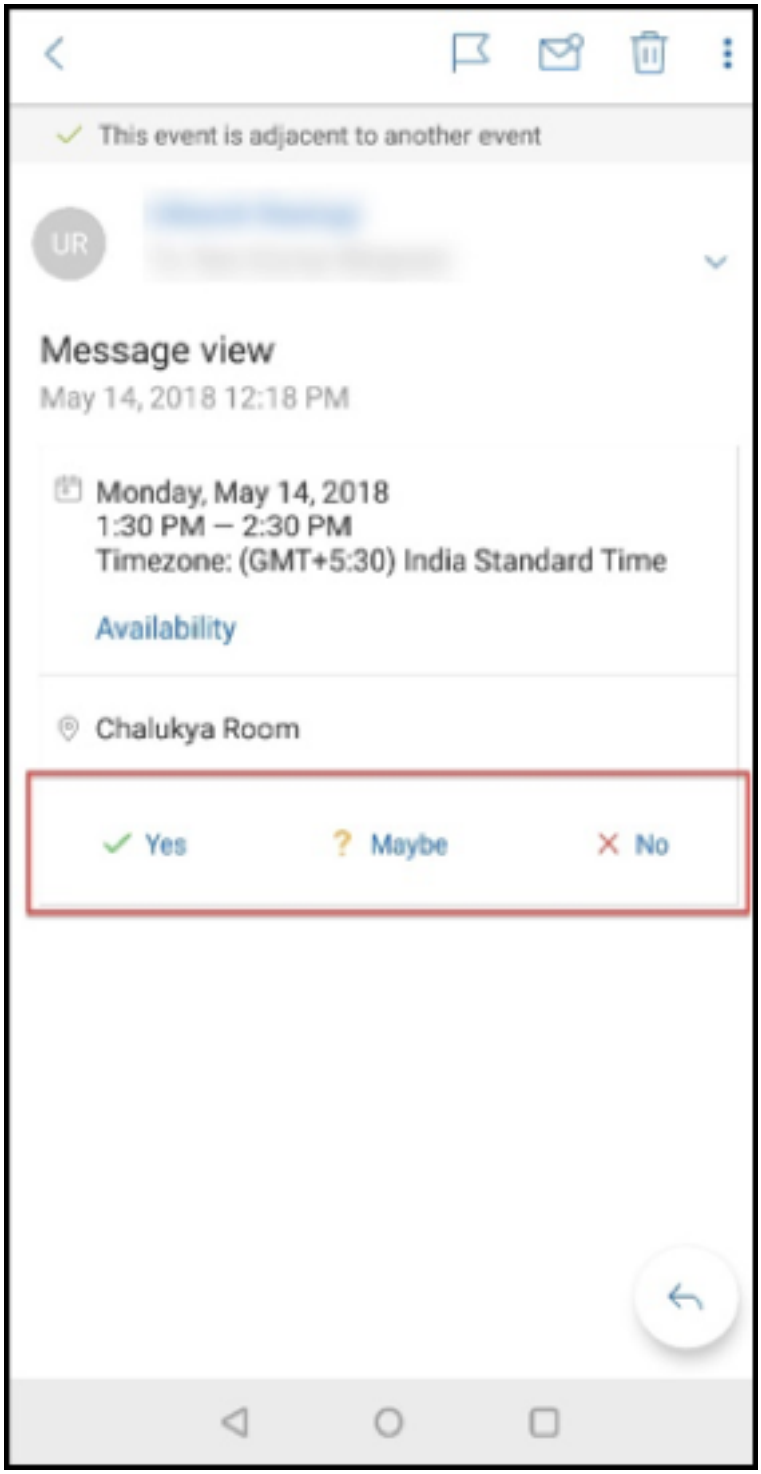
Wenn Ihre Vibrationseinstellung zuvor auf **Nur bei 'Lautlos'** eingestellt war, wechselt sie mit diesem Feature zur Standardeinstellung (**Aus**).

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

E-Mails mit Antwortschaltflächen für Besprechungen

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



Verbesserung für Anlagen

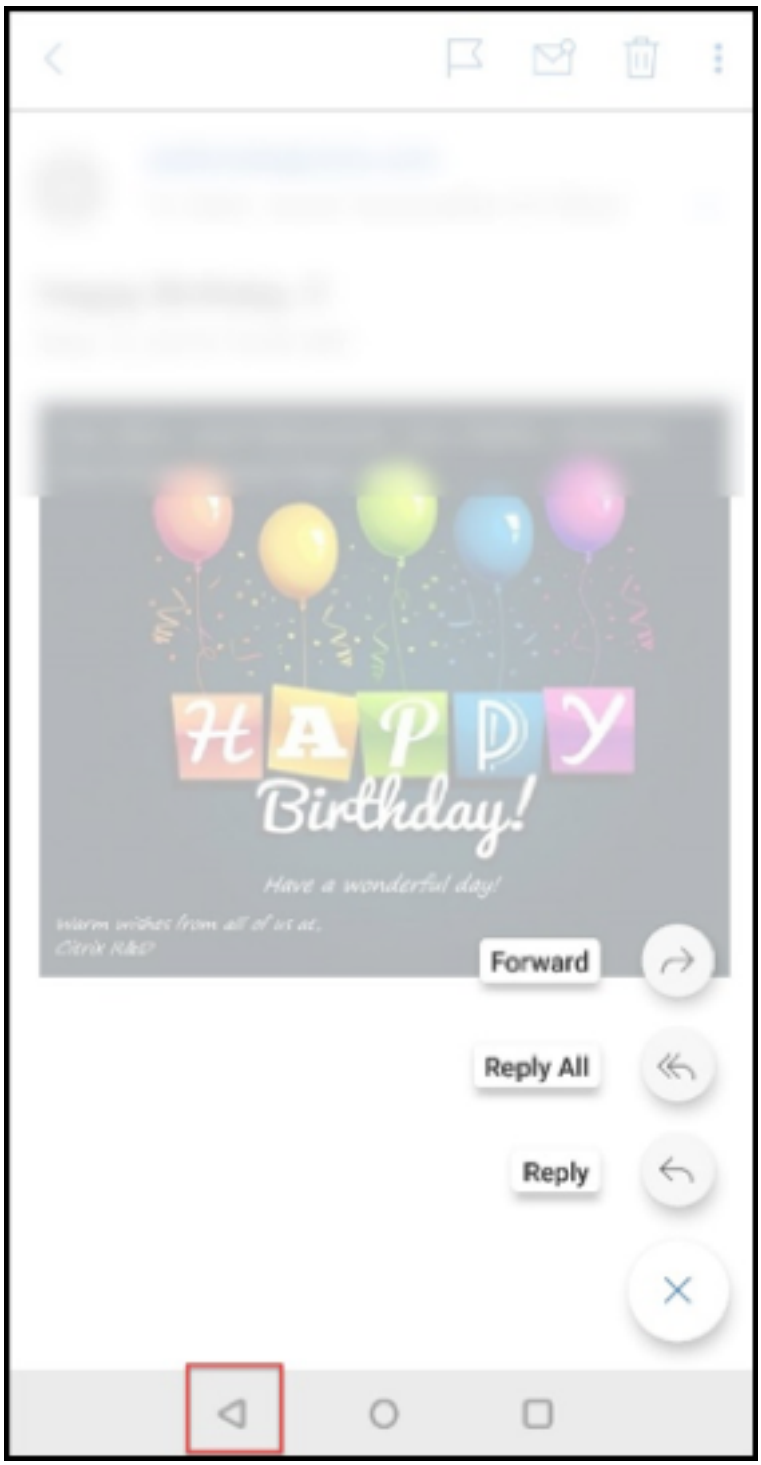
Die Anzeige von Anlagen wurde in Secure Mail für Android vereinfacht. Unwesentliche Schritte wurden zur Verbesserung der Benutzererfahrung entfernt, während vorhandene Optionen aus früheren

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. Wenn die Anlage nicht mit Secure Mail angezeigt werden kann, wird eine Liste der Apps angezeigt. Sie können dann die erforderliche App zur Anzeige der Anlage auswählen. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Dateien anzeigen und anhängen.

Verbesserungen der Zurück-Taste

In Secure Mail für Android können Sie die erweiterten Optionen der **unverankerten Aktionstaste** schließen, indem Sie auf Ihrem Gerät auf die Taste “Zurück”tippen. Durch diese Aktion kehren Sie zur Ansicht der Nachrichten- oder Ereignisdetails zurück.



Schritte für Administratoren zum Aktivieren von Dateianhängen aus der Galerie in Android

In Secure Mail 10.3.5 und höher können Benutzer keine Bilder direkt aus der Galerie-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 Galerie-App anzuhängen, führen Sie die nachfolgenden Schritte in der Endpoint Management-Konsole aus.

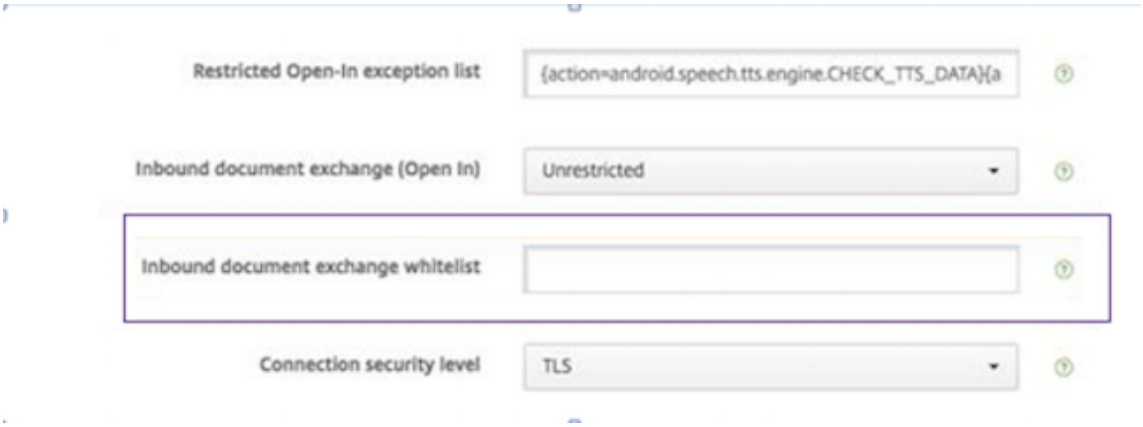
1. Legen Sie **Galerie blockieren** auf **Aus** fest.
2. Rufen Sie die Galerie-Paket-ID für Geräte ab. Beispiele:
    - **LG Nexus 5:**
      com.google.android.gallery3d, com.google.android.apps.photos
    - **Samsung Galaxy Note 3:**
      com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, 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 Galerie-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 ein Bild aus der Galerie-App anhängen. Hilfedokumentation für Benutzer zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Dateien anzeigen und 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

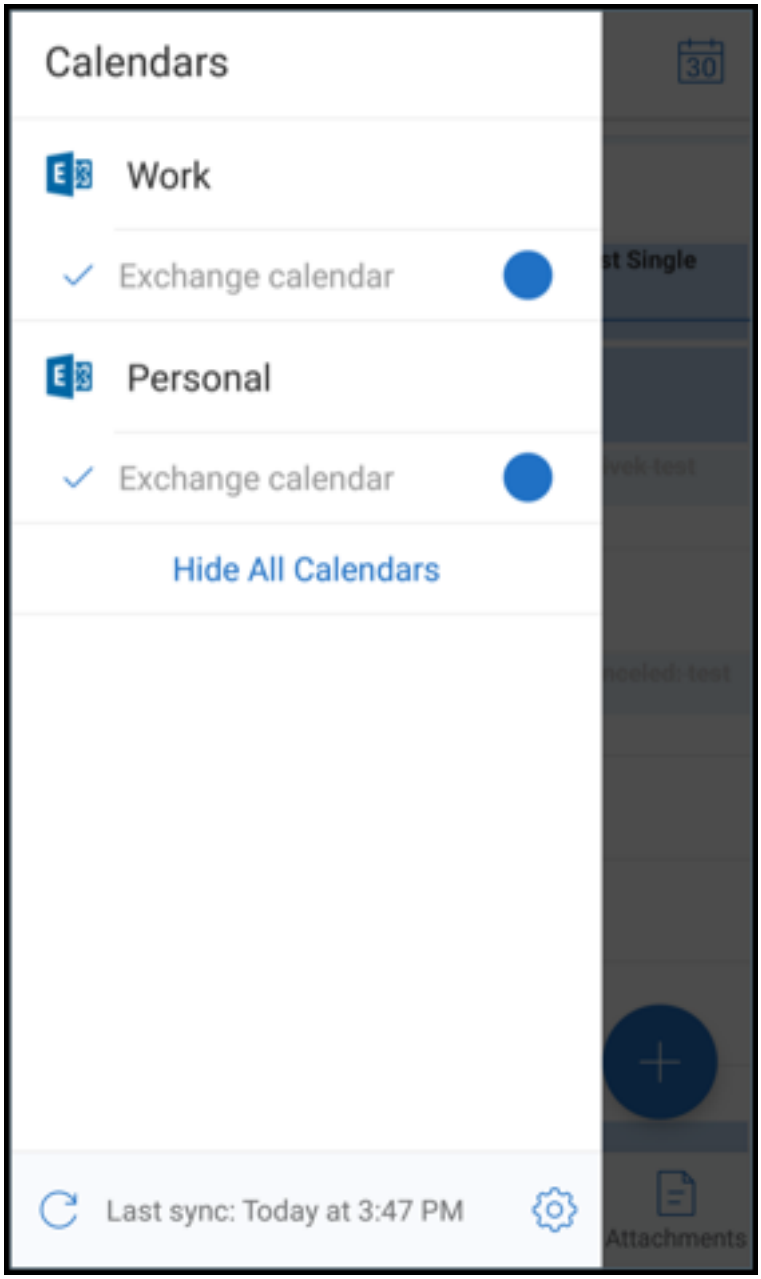
Format	iOS	Android
Video: H.264 AAC codec_mp4	X	X
Video: H.264 Acclc codec_mp4	X	X
GTM recorded_wmv		X
AVI		X
WAV	X	X
MP4	X	X
3GP	X	X
Flac		X
AAC	X	X
M4A	X	X
3GP(AMR-NB)	X	X
MP3	X	X
WAV	X	X
OGG		X
ICO	X	X
JPEG	X	X
PNG	X	X
TIF (einseitig)	X	
BMP	X	X
GIF	X	X
WebP		X
DOT	X	X
DOTX		X
PDF	X	X
PPT	X	X
PPTX	X	X
PPS		X
PPSX		X
DOC	X	X

Format	iOS	Android
DOCX	X	X
XLS	X	X
XLSM	X	X
XLSX	X	X
TXT	X	X
POT	X	X
POTX		X
HTM	X	X
HTML	X	X
ZIP	X	X
EML	X	X

Kalender

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

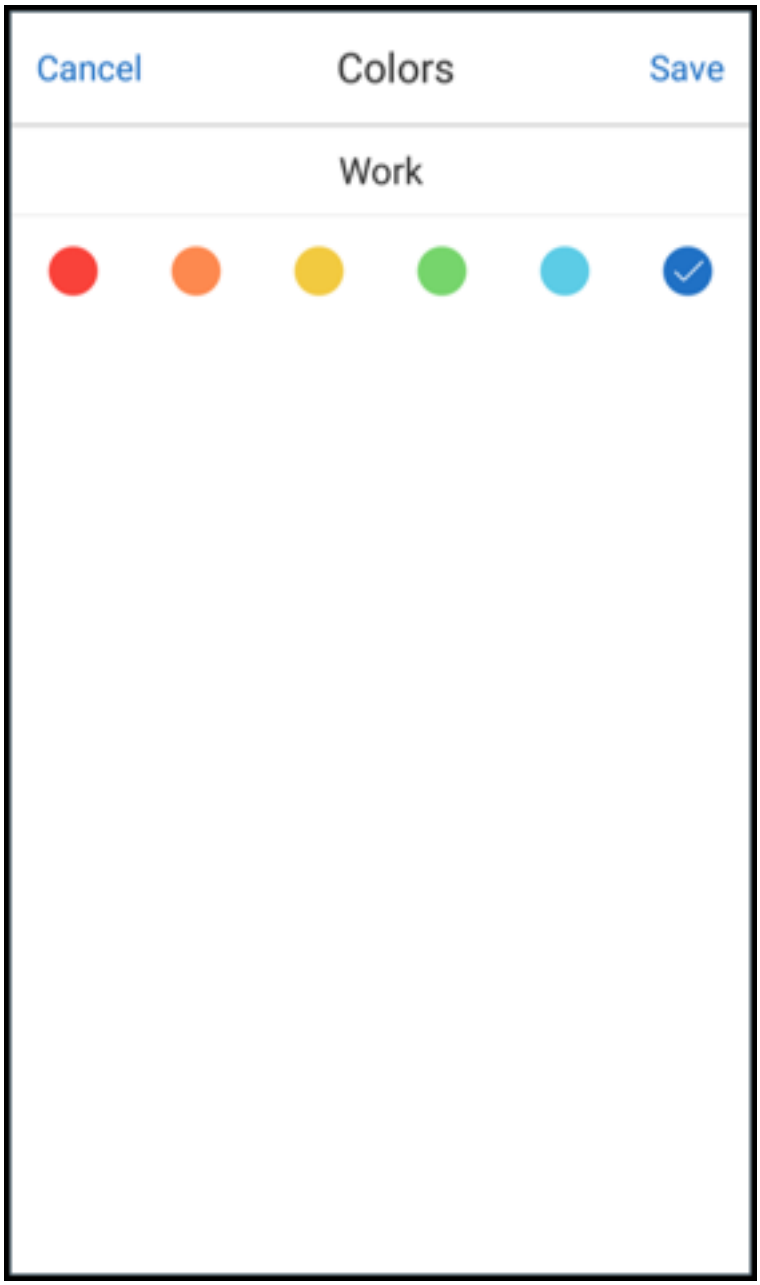
> **Hinweis**
> :
> Der persönliche Kalender ist immer Ihrem primären oder Standardkonto zugeordnet, falls aktiviert.

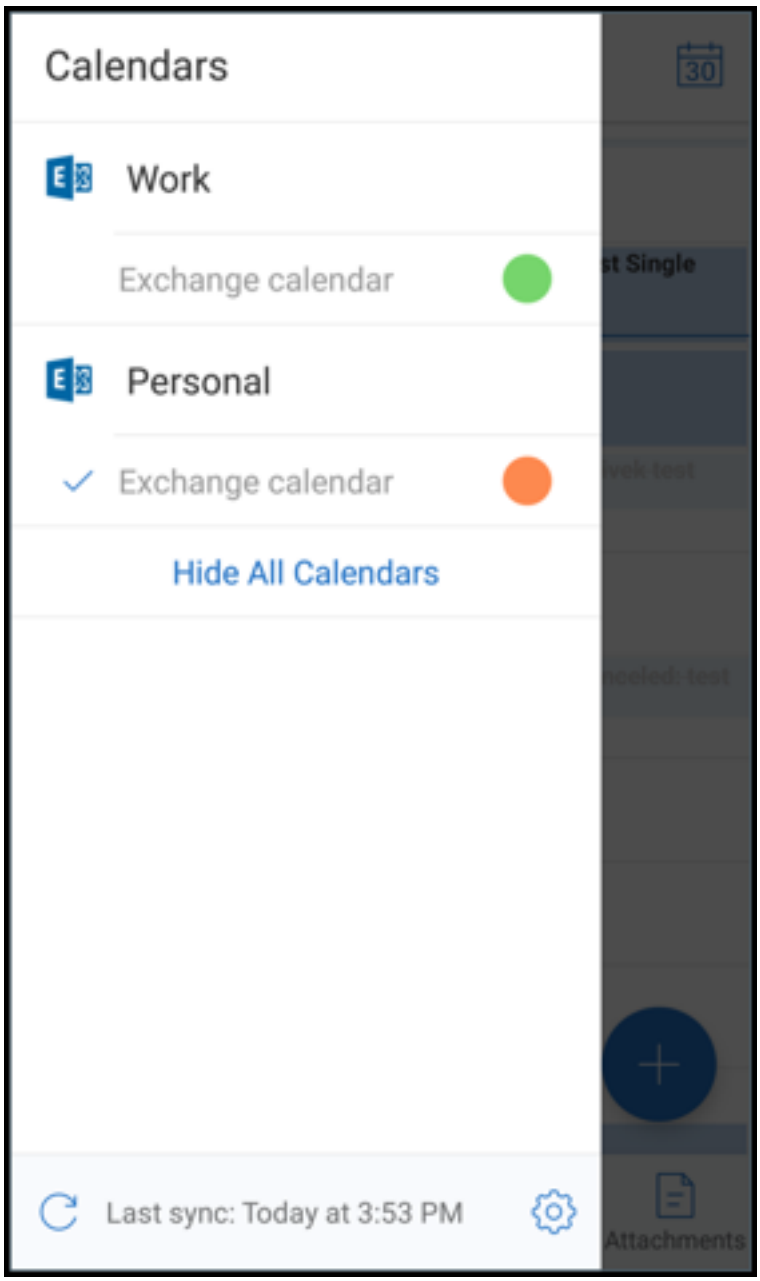


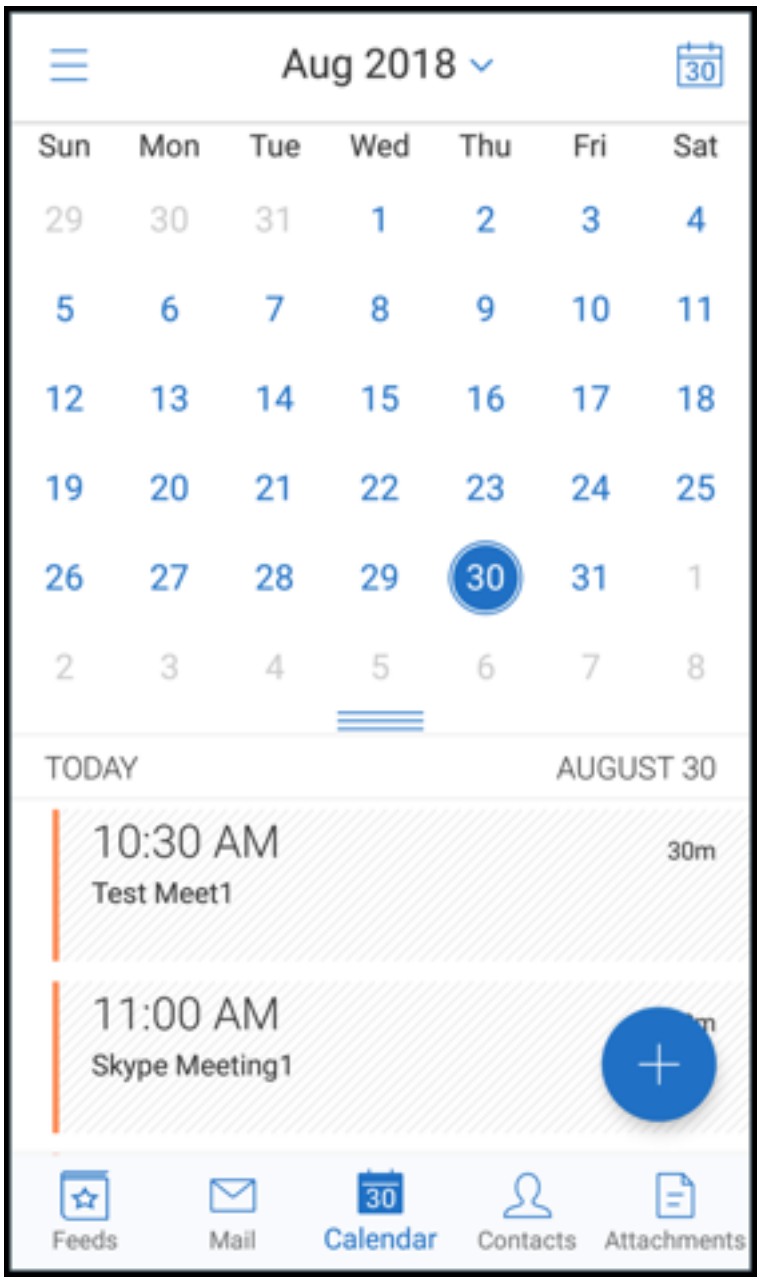
Festlegen von Farben für Kalenderereignisse

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**.

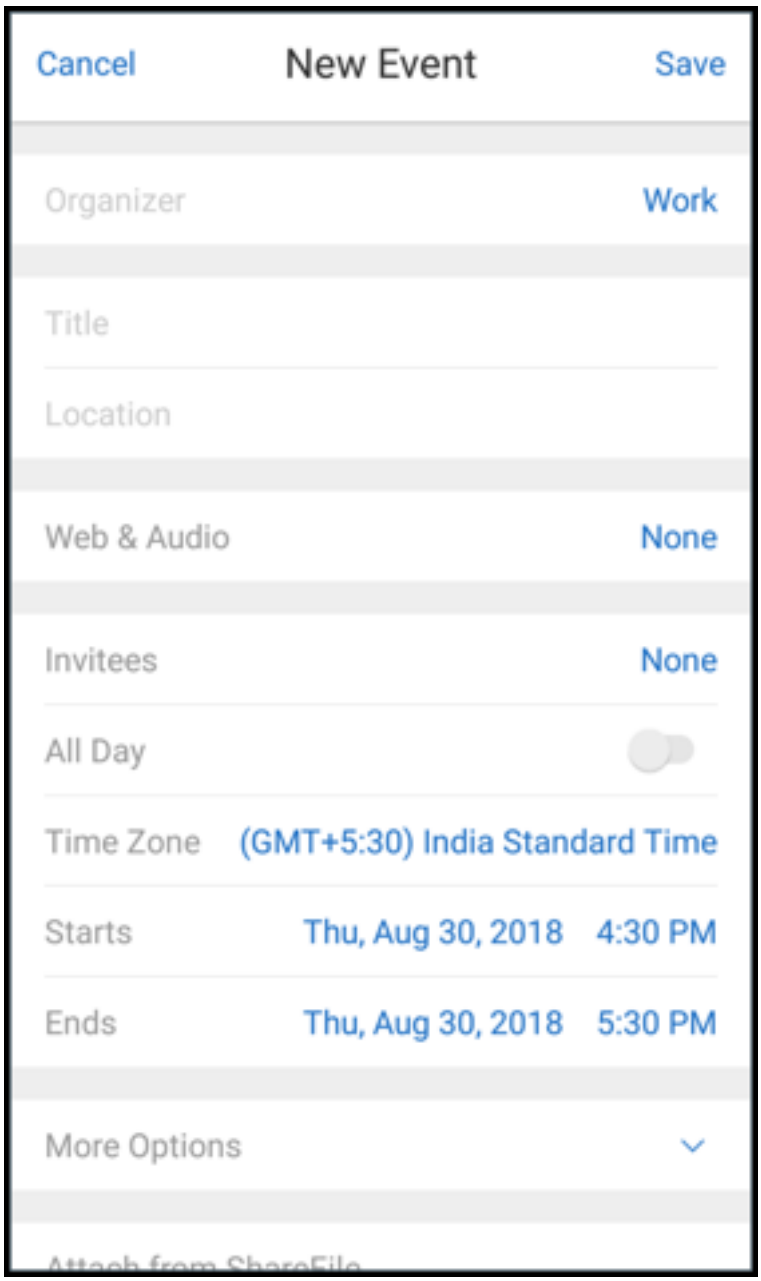
4. Um zum vorigen Bildschirm zurückzukehren, tippen Sie auf **Abbrechen**.
   Die ausgewählte Farbe wird nun auf alle Ereignisse des Exchange-Kontos angewendet.

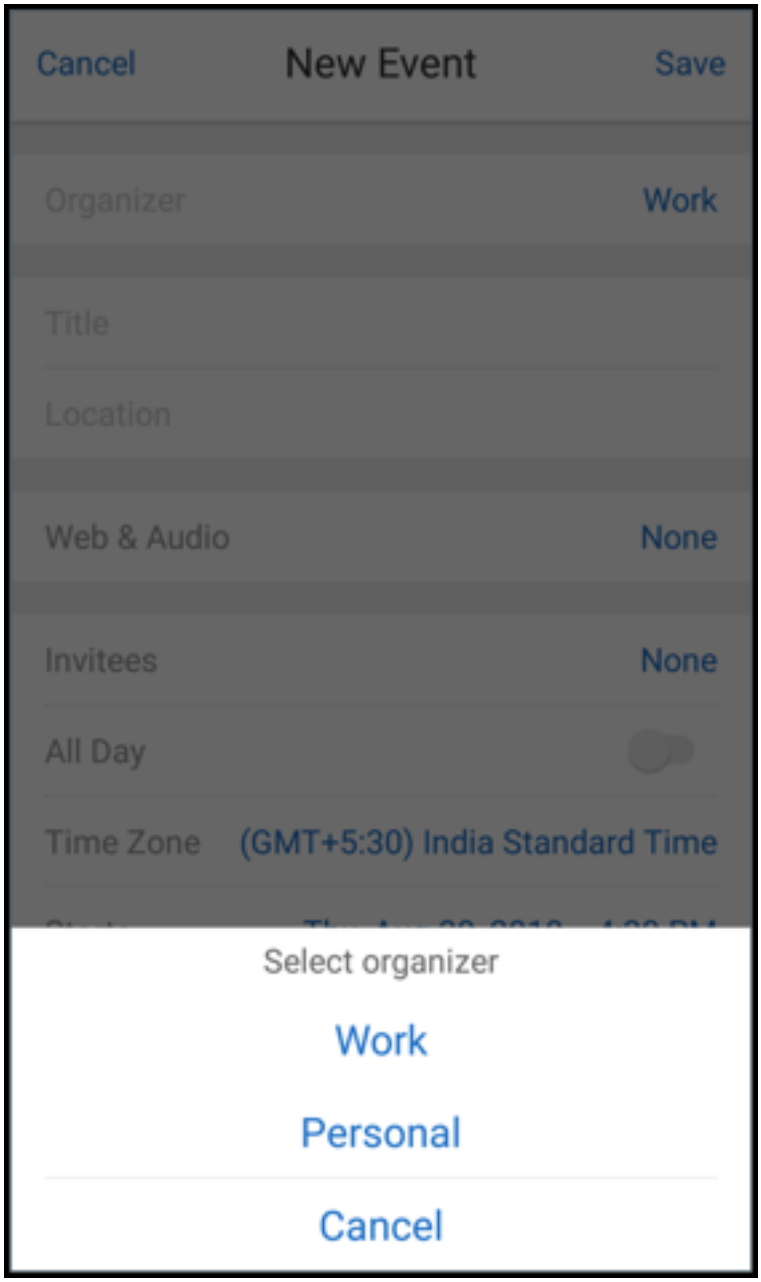






Wenn Sie Kalendereereignisse oder Einladungen erstellen, wird im Feld **Organisator** automatisch die E-Mail-Adresse des Standardkontos eingetragen. Zum Ändern des E-Mail-Kontos tippen Sie auf die E-Mail-Adresse und wählen Sie ein anderes Konto.





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.

Aktualisierung von Hintergrunddiensten

Zur Erfüllung der Google Play-Limits zur Ausführung im Hintergrund auf Geräten mit Android 8.0 (API-Level 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 variiert, 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.

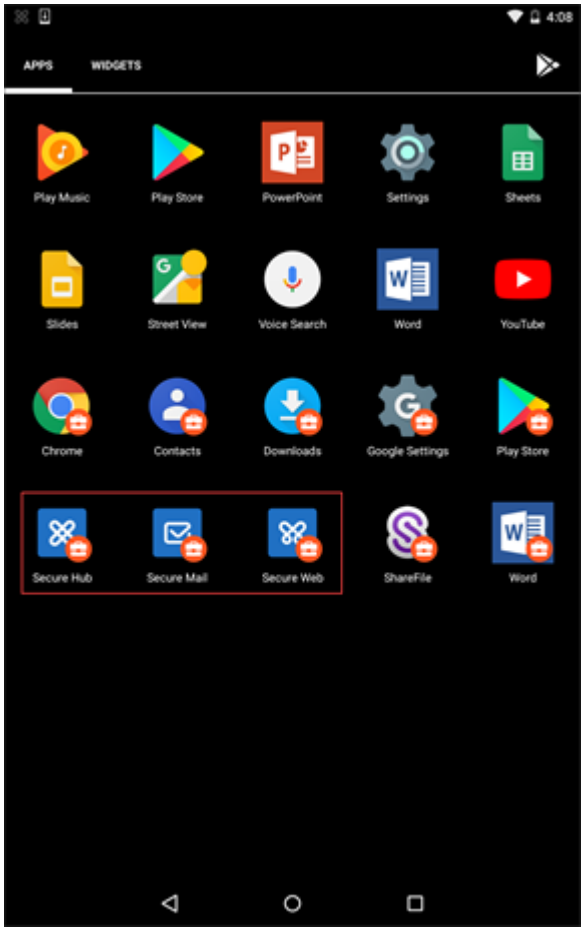
Android Enterprise in Secure Mail

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
E-Mail-Klassifizierung	X

Feature	Support
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
Tunnel —Web-SSO-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 Kalenderex-

port 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.

iOS- und Android-Features für Secure Mail

June 6, 2024

In diesem Artikel werden die iOS- und Android-Features beschrieben, die von Secure Mail unterstützt werden.

Unterstützung für Azure Government Cloud Computing

Secure Mail unterstützt Government Cloud Computing (GCC) High, das moderne Authentifizierung (OAuth) auf dem Azure Active Directory-Mandanten bietet. Secure Mail ist als Endpunkt auf dem GCC High registriert, um die obligatorische Anforderung von Microsoft für den gesamten GCC High Service zu erfüllen. Weitere Informationen finden Sie unter Neuerungen bei Azure Active Directory in Microsoft 365 Government.

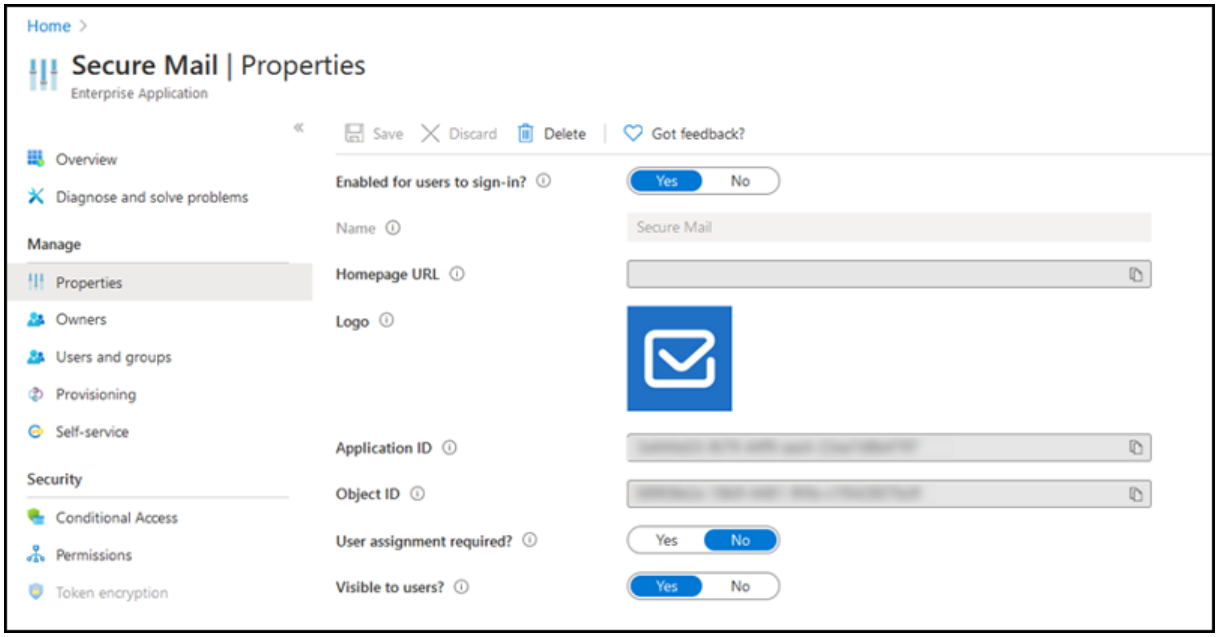
Sie werden nun zur Authentifizierung an GCC High auf dem Azure Active Directory-Mandanten weitergeleitet. Der Administrator muss Berechtigungen für Secure Mail auf dem Azure Active Directory-Mandanten zulassen.

Voraussetzungen

Stellen Sie sicher, dass der globale Administrator von Azure Active Directory folgende Schritte ausführt:

- Download der aktuellen Version von Secure Mail auf Ihr Gerät.
- Konfigurieren Ihres Exchange-Kontos in der Secure Mail-App und Zulassen der App-Berechtigung in Azure Active Directory für alle Benutzer, die sich anmelden. Weitere Informationen bietet der folgende Bildschirm.

> **Hinweis:**
>
> Diese Schritte sind von globalen Administratoren auszuführen und nur einmal erforderlich. Sobald der App der Zugriff gewährt wurde, können Sie einfach ein Upgrade über den App Store ausführen.



Nach dem Upgrade

Nach einem Upgrade werden Sie nach Ablauf des Aktualisierungstokens zur erneuten Autorisierung aufgefordert und zu GCC High in Azure AD umgeleitet. Überprüfen Sie den vorherigen Workflow, um sicherzustellen, dass die Autorisierungsanforderung an GCC High in Azure AD gesendet wird.

Es gibt zwei Möglichkeiten zur Überprüfung des Workflows:

- Secure Mail mit dem App-Namen **Secure Mail-GCC High** wird auf der Anmeldeseite im Azure Active Directory-Mandanten angezeigt.
- Überprüfen Sie in den Secure Mail-Protokollen, ob die Weiterleitungen nach der Neuauthentifizierung über https://login.microsoftonline.us erfolgen.

Unterstützung für ICS-Dateien

In Secure Mail können Sie angehängte ICS-Dateien anzeigen und als Ereignis in Ihren Kalender importieren.

Kontaktbild in Secure Mail

Zeigen Sie in Secure Mail ein Bild des Kontakts an, wenn Sie Empfänger in E-Mails oder Besprechungseinladungen hinzufügen. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Bilder Ihrer Kontakte anzeigen.

Feeds verwalten

In Secure Mail können Sie Ihre **Feed**-Karte entsprechend Ihren Anforderungen organisieren. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter E-Mails organisieren.

Definieren der Office 365-Serveradresse mit der Richtlinie für Office 365 Exchange Server

In Secure Mail wurde im Abschnitt "OAuth-Unterstützung für Office 365"die Richtlinie **Office 365 Exchange Server** hinzugefügt. Mit dieser Richtlinie können Sie in Cloud den Hostnamen für das Office 365-Postfach definieren. Die Richtlinie unterstützt auch Office 365 für Behörden. Der Hostname ist ein einzelner Wert, z. B. *outlook.office365.com*. Der Standardwert ist *outlook.office365.com*.

Unterstützung für die Verschlüsselungsverwaltung

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

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

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

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

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

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

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

Geräte mit iOS

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

- iOS 10: Die Betriebssystemversion der App ist größer oder gleich der angegebenen Version.
- Debuggerzugriff: Debugging ist für die App nicht aktiviert.
- Gerät mit Jailbreak: Auf Geräten mit Jailbreak wird die App nicht ausgeführt.
- Gerätepasscode: Der Gerätepasscode ist **aktiviert**.
- Datenfreigabe: Die Datenfreigabe ist für die App nicht aktiviert.

Geräte mit Android

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

- Android SDK 24 (Android 7 Nougat) - Die App führt Betriebssystemversion aus, die größer oder gleich der angegebenen Version ist.
- Debuggerzugriff: Debugging ist für die App nicht aktiviert.
- Gerät mit Rooting: Auf Geräten mit Rooting wird die App nicht ausgeführt.
- Gerätesperre: Der Gerätepasscode ist **aktiviert**.
- Gerät verschlüsselt: App wird auf einem verschlüsselten Gerät ausgeführt.

Unterstützung für dynamische E-Mails

Secure Mail wurde optimiert, um dynamische E-Mails zu liefern. Bisher wurden E-Mail-Inhalte mit großen Tabellen oder Bildern falsch gerendert. Dieses Feature biete E-Mail-Inhalte, die auf allen unterstützten Geräten unabhängig von E-Mail-Format und Größe besser lesbar sind.

Drag & Drop für Kalenderereignisse

In Secure Mail können Sie die Zeit eines vorhandenen Kalenderereignisses durch Drag & Drop ändern. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Kalenderereigniszeit ändern.

Feeds verwalten

In Secure Mail können Sie Ihre **Feed**-Karte entsprechend Ihren Anforderungen organisieren. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter E-Mails organisieren.

Automatisch weiter

Wenn Sie in Secure Mail eine Nachricht in den **Unterhaltungen** löschen, können Sie auswählen, zu welcher Nachricht Sie zurückkehren. Um diese Funktion zu verwenden, navigieren Sie zu **Einstellungen > Autom. weiterleiten**. Wählen Sie dann die gewünschte Option aus. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter E-Mail in Unterhaltung löschen und automatisch andere E-Mail anzeigen.

Automatische Synchronisierung des Ordners “Entwürfe”

Der Ordner “Entwürfe”wird 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.

Die Hilfedokumentation zu diesem Feature, einschließlich eines Videos, finden Sie in der Citrix-Benutzerhilfe unter Automatische Synchronisierung des Ordners “Entwürfe”.

Unterstützung für Single Sign-On bei der Verwendung von Microsoft Intune im MDM + MAM-Modus

Für iOS-Geräte:

Um diese Feature zu verwenden, muss die Microsoft Authenticator-App auf Ihrem Gerät installiert sein. Weitere Informationen zum Installieren der Microsoft Authenticator-App finden Sie unter **Microsoft Authenticator App herunterladen und installieren** in docs.microsoft.com.

Android-Geräte:

Um diese Feature zu verwenden, muss das Intune-Unternehmensportal auf Ihrem Gerät installiert sein. Sobald Sie sich am Intune-Unternehmensportal angemeldet haben, können Sie SSO im MDM + MAM-Modus verwenden und müssen sich nicht in Secure Mail neu authentifizieren.

Verbesserungen für Kontakte

Wenn Sie in Secure Mail 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 Kalenderereignis erstellen. Die Angaben aus **Vorgesetzte(r)**, **Direkte Mitarbeiter** oder **Kollegen** werden automatisch in das Feld **An:** der E-Mail oder des
Kalenderereignisses 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:**
>
> Dieses Feature wird von IBM Lotus Notes-Servern nicht unterstützt.

Export von Zeit und Ort einer Besprechung in den nativen Kalender

In Secure Mail 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.

Mehrere Exchange-Konten

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. Die Administratorvoraussetzungen sind wie folgt:

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

Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Exchange-Konten hinzufügen.

Kontakte

Die Hilfedokumentation für Kontakte finden Sie in der Citrix-Benutzerhilfe unter Kontakte anzeigen und synchronisieren.

Festlegen von Farben in Kalendern

Zu diesem Kalenderfeature finden Sie Hilfedokumentation in der Citrix-Benutzerhilfe unter Farben für synchronisierte Secure Mail-Kalender festlegen.

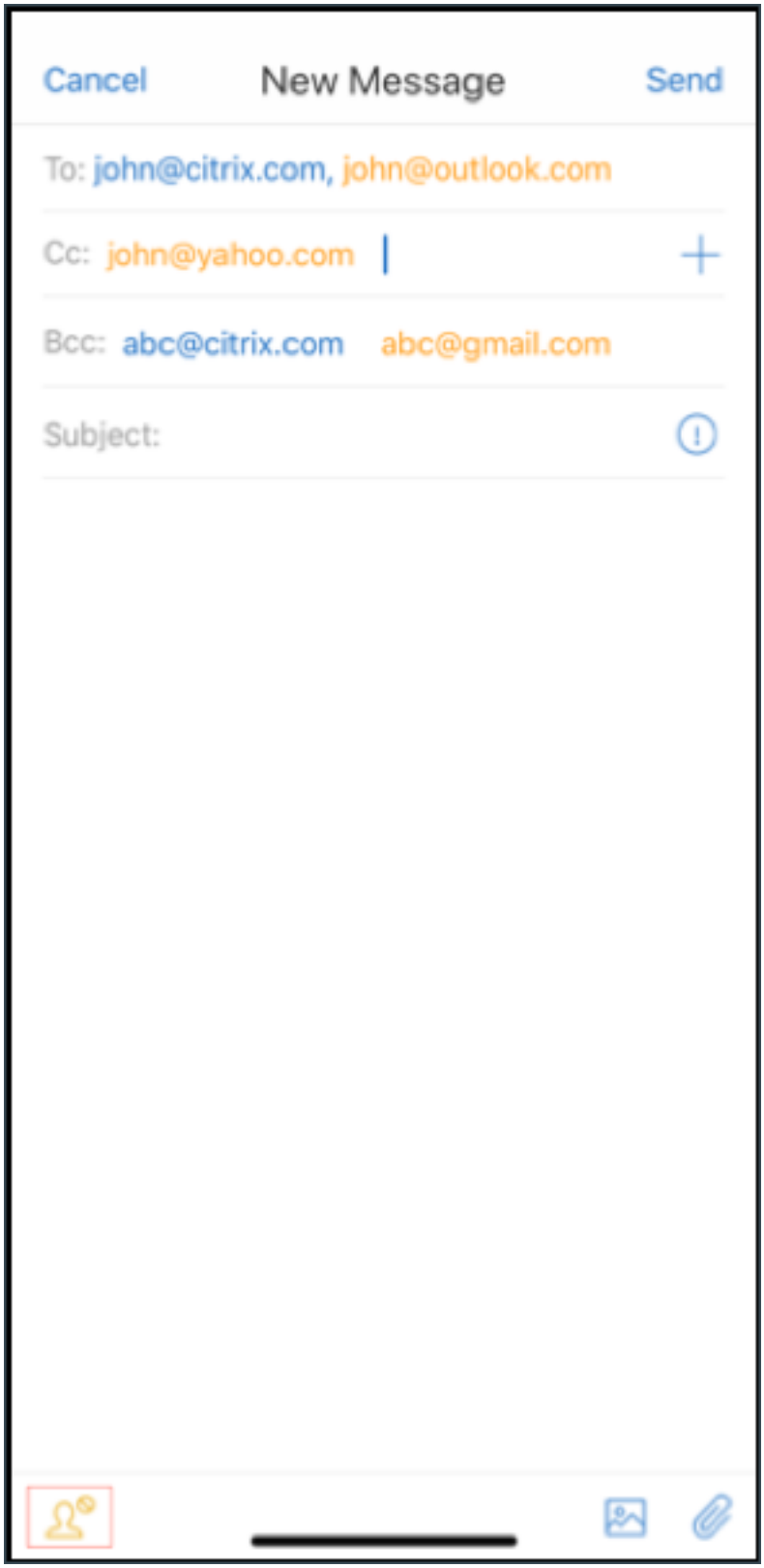
Interne Domänen

Sie können E-Mail-Empfänger identifizieren und bearbeiten, die zu externen Organisationen gehören.

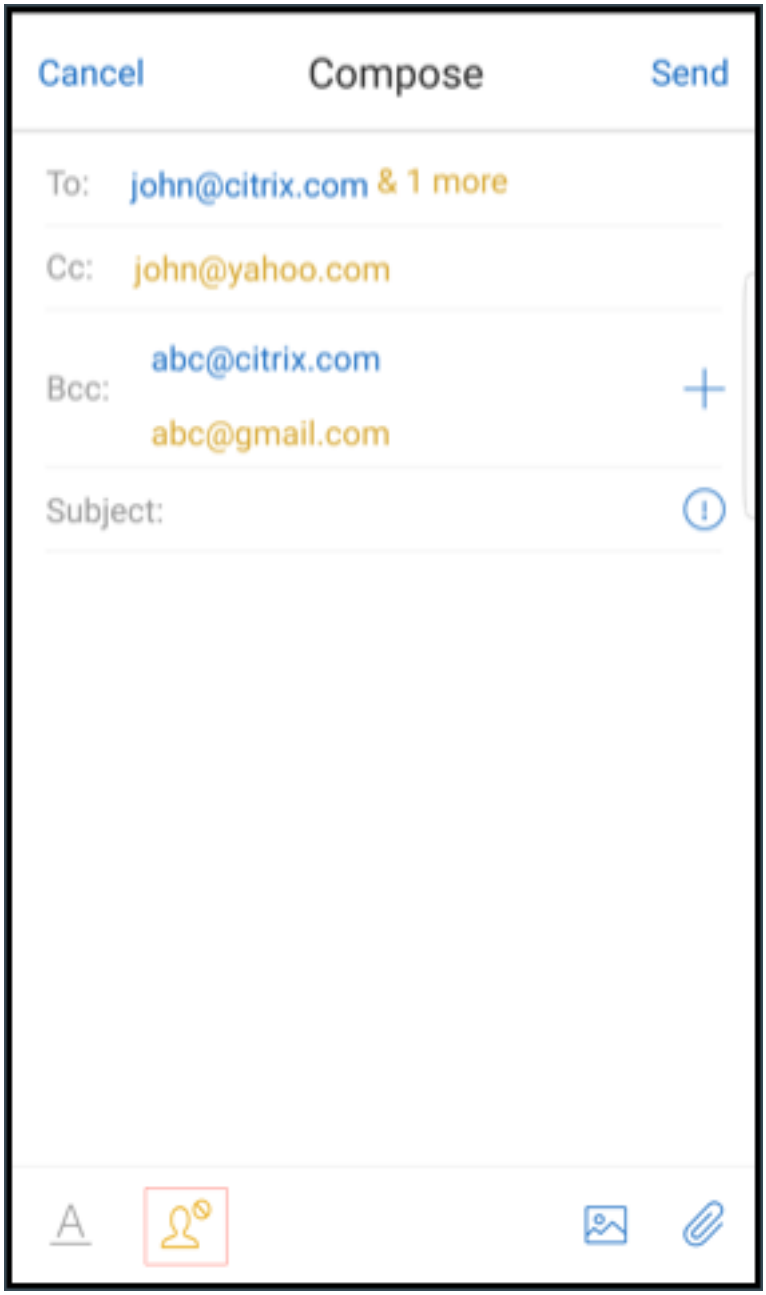
Voraussetzungen: Stellen Sie sicher, dass Sie die Richtlinie **Interne Domänen** in Citrix Endpoint Management aktiviert und die Anwendung neu gestartet haben.

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.

Auf Geräten mit iOS:

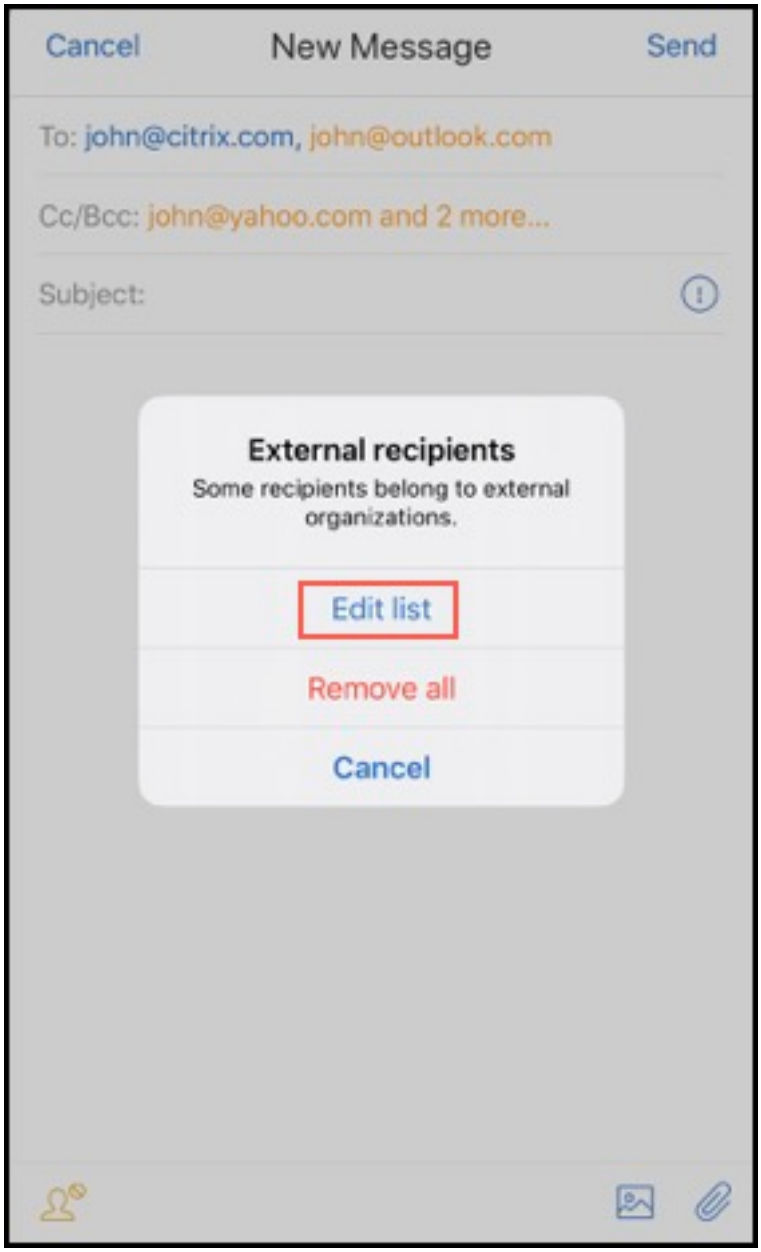


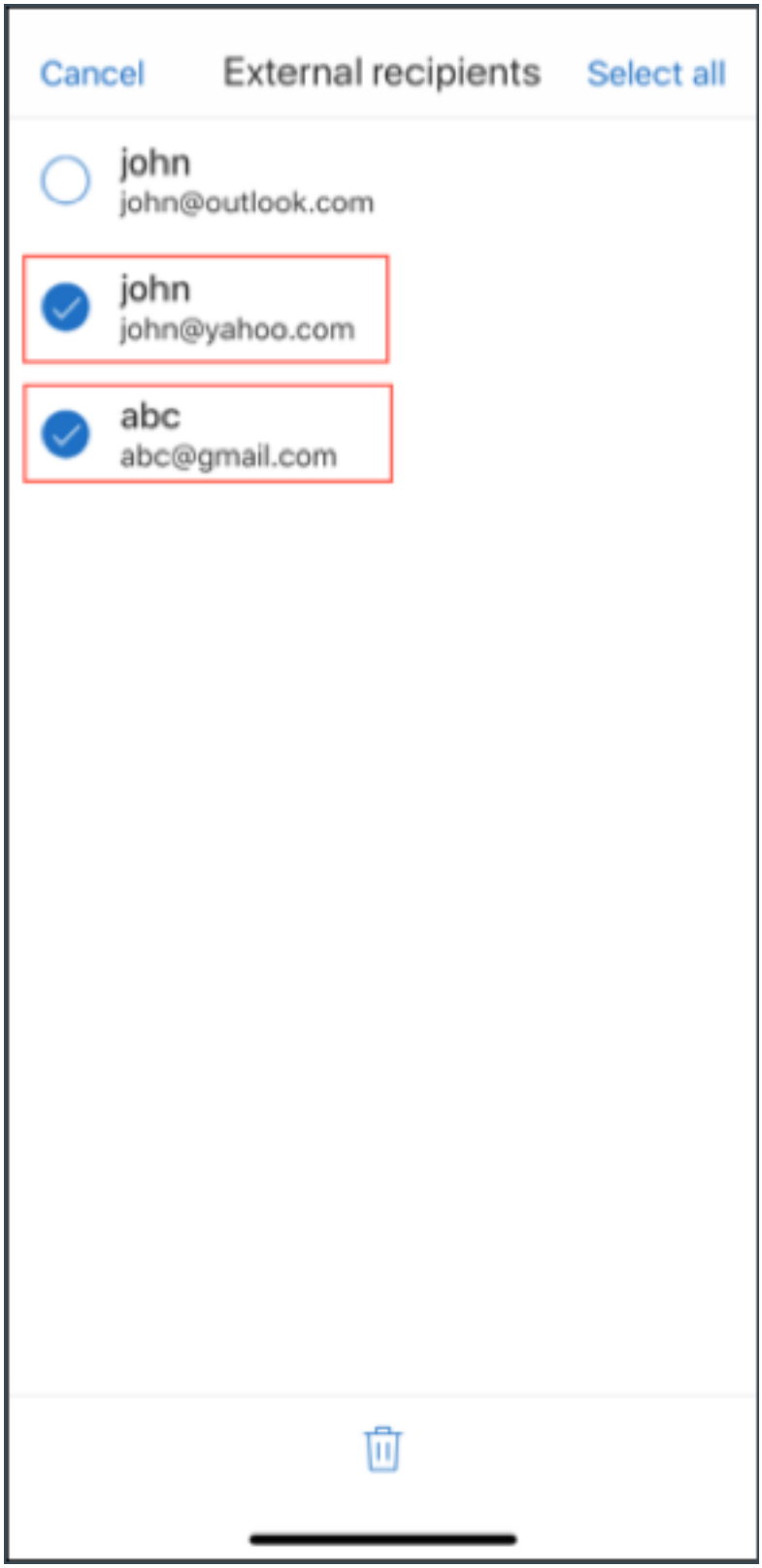
Auf Geräten mit Android:



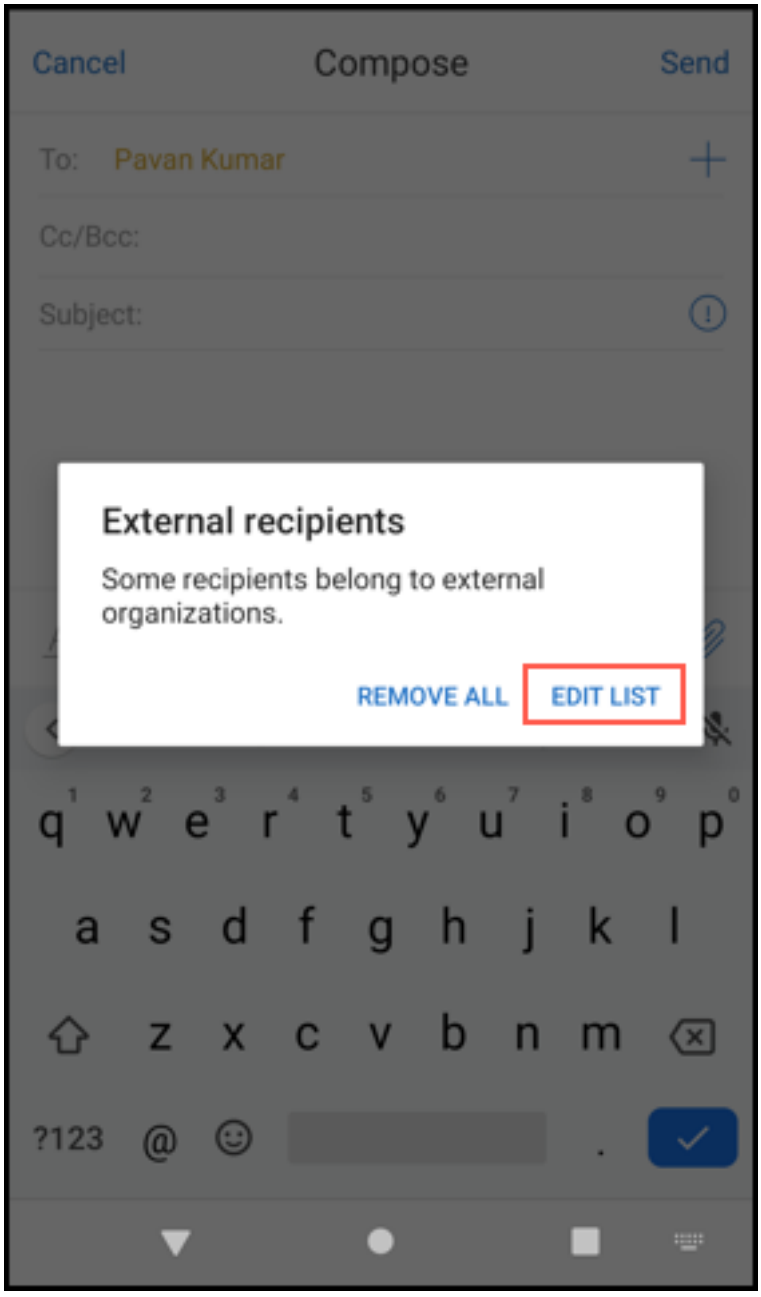
Wenn Sie auf das Symbol **Kontakte** tippen, wird ein Popupfenster mit Optionen zum Bearbeiten der Liste oder Entfernen aller Elemente angezeigt. Tippen Sie auf **Liste bearbeiten**, um die Empfänger auszuwählen, die Sie entfernen möchten. Tippen Sie nach der Auswahl der Empfänger auf den **Papierkorb**.

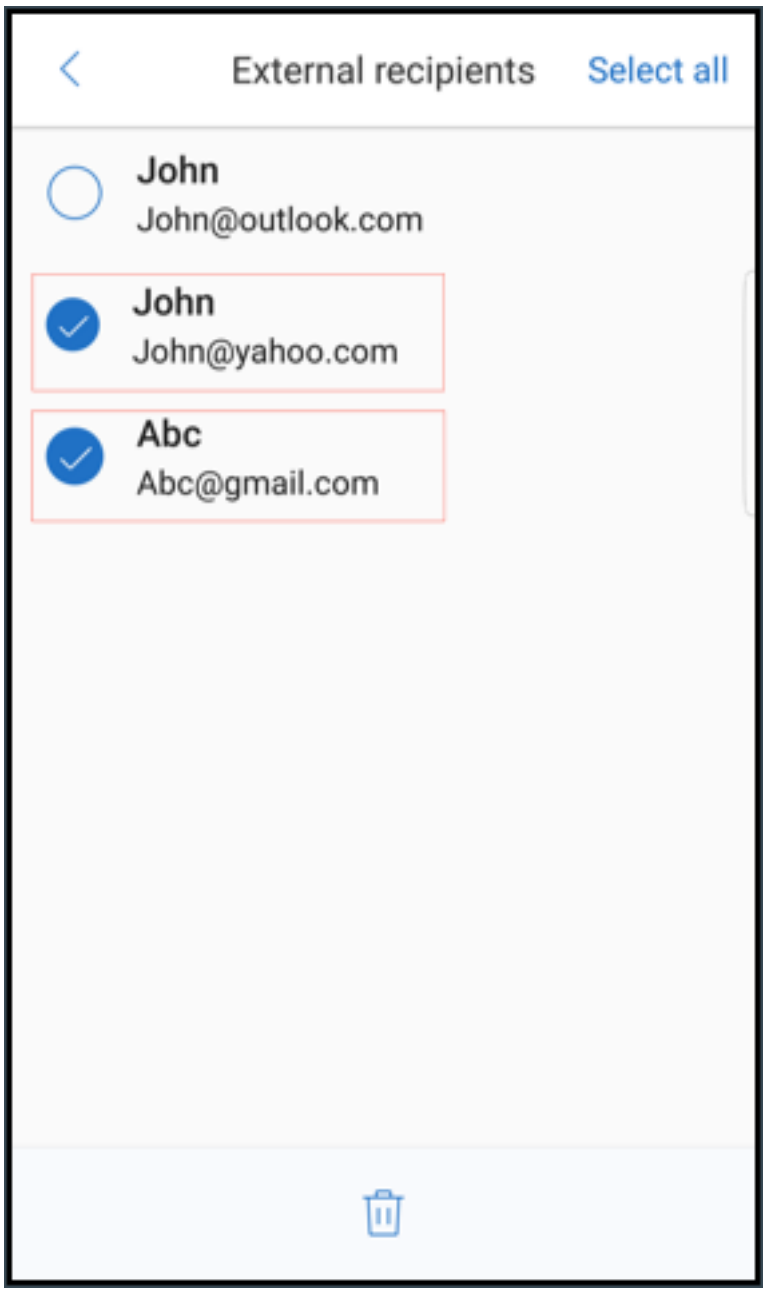
Auf Geräten mit iOS:





Auf Geräten mit Android:



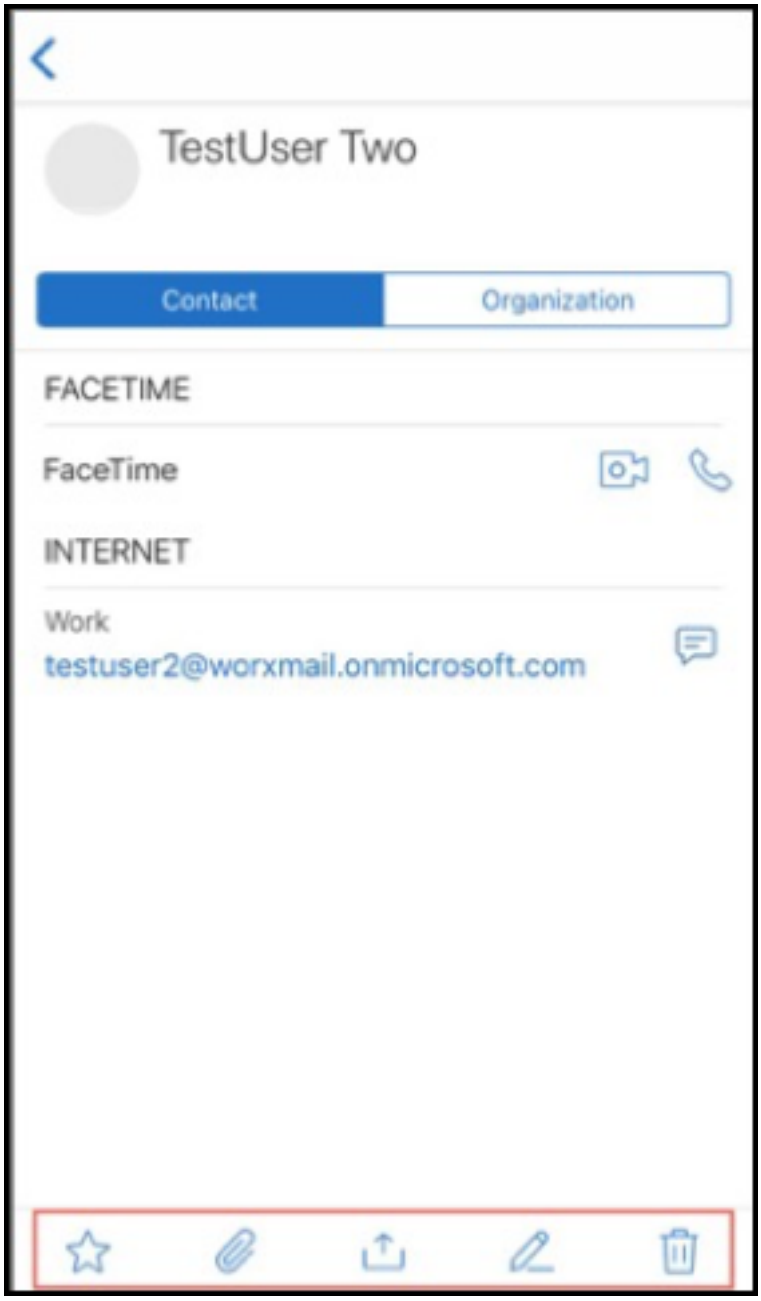


Ergonomische Verbesserungen

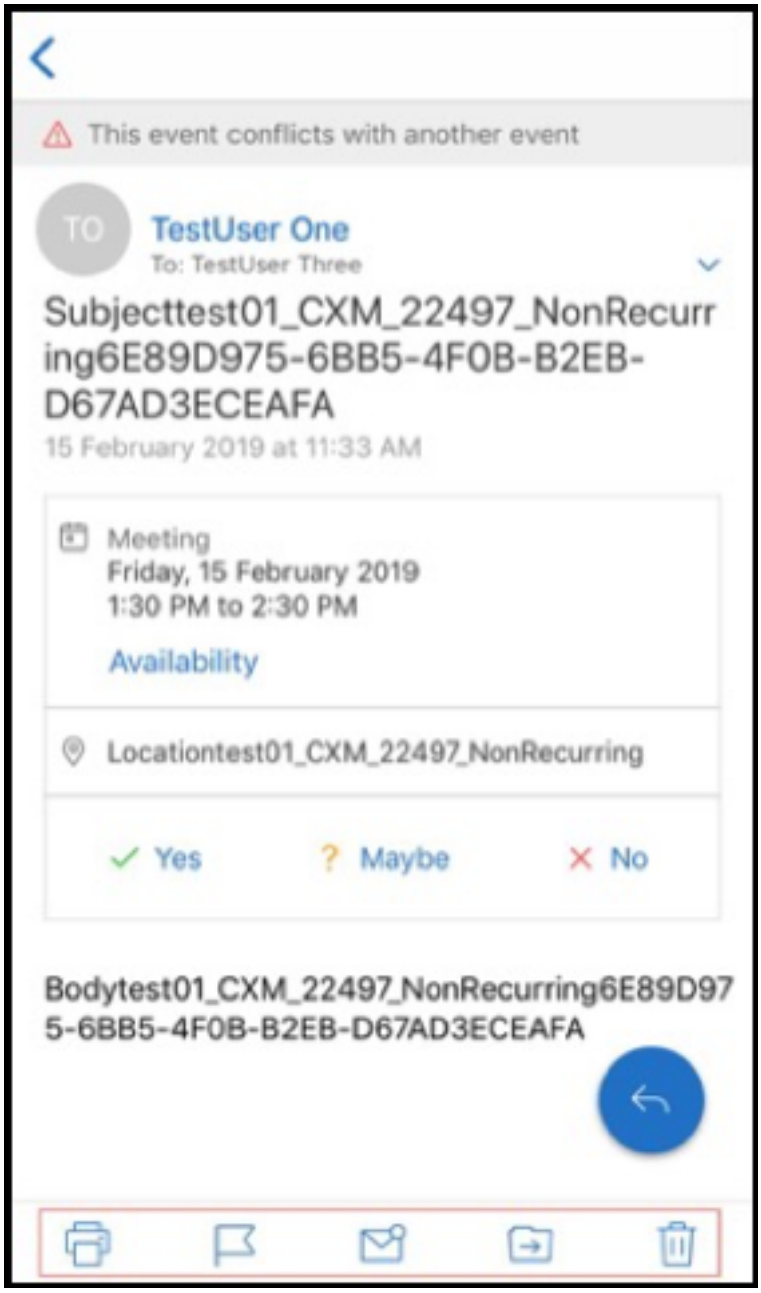
Die Aktionstasten wurden vom oberen Bildschirmrand nach unten verschoben, um den Zugriff zu erleichtern. Diese Änderung betrifft die Bildschirme **Posteingang**, **Kalender** und **Kontakte**.

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

Auf Geräten mit iOS



Auf Geräten mit Android



Die unverankerte Aktionstaste **Antworten** wurde an Stil und Branding von Citrix angepasst.

Es ist mit dieser Version nicht mehr möglich, aus einer geöffneten E-Mail heraus auf Schaltflächen im Hauptfenster des Posteingangs zuzugreifen. Sie müssen die geöffnete E-Mail schließen, um auf Elemente wie **Feeds**, **Kalender**, **Kontakte**und **Anlagen** zugreifen.

Die Optionen in der Fußzeilenleiste von iOS wurden geändert, um das Aussehen in iOS und Android einheitlicher zu gestalten.

Secure Mail-Integration in Slack (Preview)

Sie können eine E-Mail-Unterhaltung jetzt auf Geräten mit iOS oder Android in die App Slack übertragen. Weitere Informationen finden Sie unter Secure Mail-Integration in Slack (Vorschau).

Melden von Phishing-E-Mail (als Weiterleitung)

In Secure Mail können Sie mit dem Feature "Als Phishing melden"verdächtige E-Mails (als Weiterleitung) melden. 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 **Phishingberichtmethode** auf **Durch Weiterleiten melden** festlegen. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Phishing-E-Mail melden.

Phishing-E-Mail melden

Sie können eine Phishing-E-Mail basierend auf der von einem Administrator konfigurierten Richtlinie melden. Die Hilfedokumentation zu diesem Feature sowie Angaben zu den Administratoreinstellungen finden Sie in der Citrix-Benutzerhilfe unter Phishing-E-Mail melden.

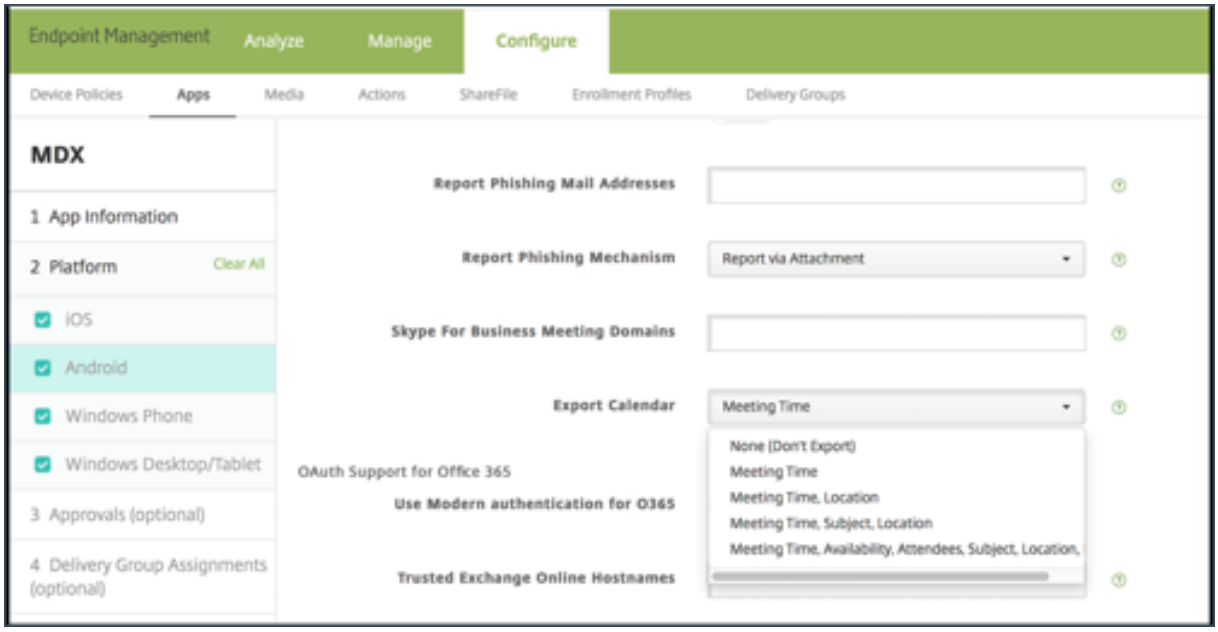
Secure Mail-Kalenderereignisse exportieren

Mit Secure Mail für iOS und Android können Sie Secure Mail-Kalenderereignisse in die native Kalender-App Ihres Geräts exportieren. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Secure Mail-Kalenderereignisse exportieren.

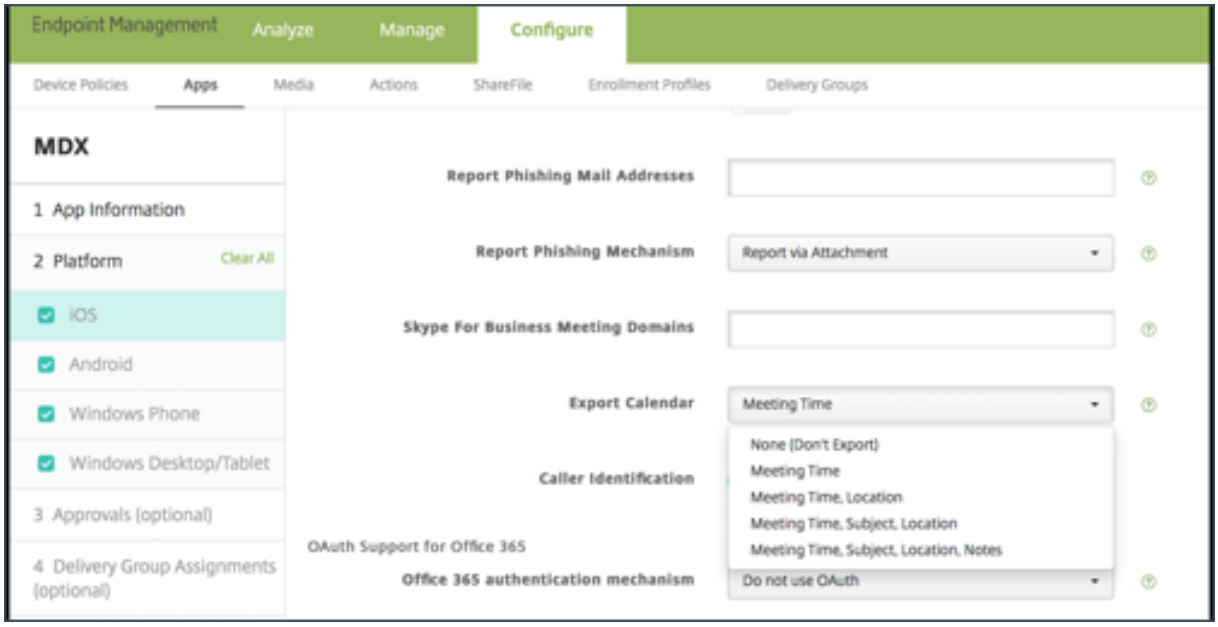
Die folgenden MDX-Richtlinienwerte sind für die Kalenderereignisfelder verfügbar, die in Ihrem persönlichen Kalender erscheinen:

- Keine (nicht exportieren)
- Besprechungszeit
- Besprechungszeit, Ort
- Zeit, Ort und Betreff der Besprechung
- **(Für Android)** Besprechungszeit, Verfügbarkeit, Teilnehmer, Betreff, Ort, Notizen
- **(Für iOS)** Besprechungszeit, Betreff, Ort, Notizen

Android-Optionen:



iOS-Optionen:



Für iOS

Obwohl aus Secure Mail exportierte Kalenderereignisse **gelesen/geschrieben** werden, sind Änderungen an Ereignissen außerhalb von Secure Mail nicht möglich.

Wichtig:

- Dieses Feature ist sichtbar, aber in Secure Mail deaktiviert, wenn eine der folgenden Bedingungen erfüllt ist:

  - Die Richtlinie für den Export des Kalenders ist auf **AUS** festgelegt.
  - Ihre MDX-Version enthält die Richtlinie nicht

- Dieses Feature funktioniert nicht, wenn E-Mail-Konten bereits in Ihrer persönlichen Kalender-App konfiguriert sind und Ihr iCloud-Konto deaktiviert ist. Dieses Feature funktioniert, wenn in Ihrer persönlichen Kalender-App kein anderes Konto eingerichtet ist.
- Um die URL zu starten und die Secure Mail-Kalenderereignisse aus Ihrem persönlichen Kalender zu bearbeiten, stellen Sie sicher, dass der Wert **"ctxevent:"in** der MDX-Richtlinie „App-URL-Schemas"enthalten ist.

Für Android

Kalenderereignisse, die aus Secure Mail exportiert werden, sind schreibgeschützt. Um Secure Mail-Ereignisse zu bearbeiten, tippen Sie in Ihrem Kalenderereignis auf den Link **Secure Mail-Ereignis**.

Wichtig:

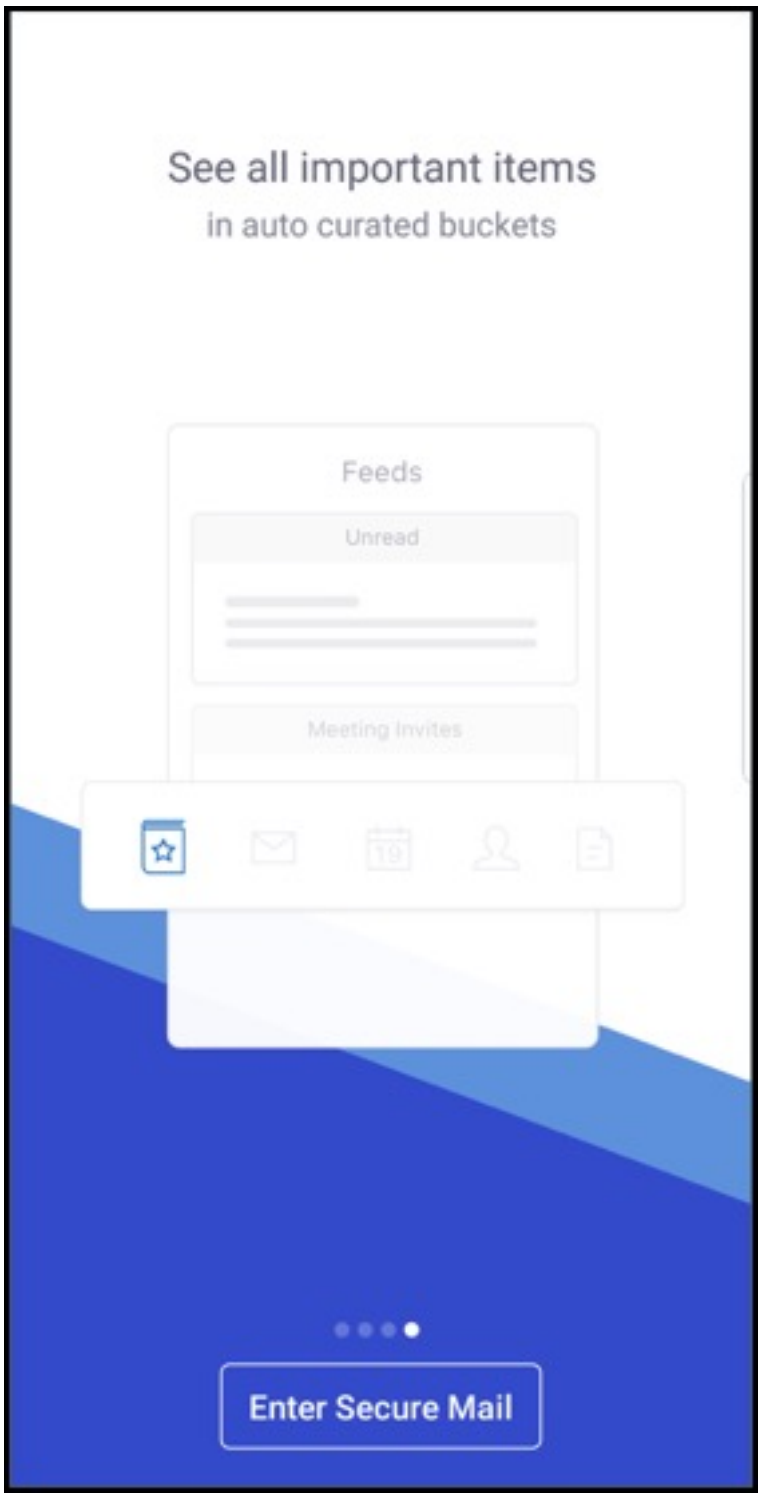
- Dieses Feature ist sichtbar, aber in Secure Mail deaktiviert, wenn eine der folgenden Bedingungen erfüllt ist:
  - Die Richtlinie für den Export des Kalenders ist auf **AUS** festgelegt.
  - Ihre MDX-Version enthält die Richtlinie nicht
- Vergewissern Sie sich, dass die MDX-Richtlinie „ Eingehender Dokumentaustausch"auf **Uneingeschränkt** festgelegt ist.
- Der Link „Secure Mail-Ereignis"ist auf Samsung- und Huawei-Geräten nicht verfügbar.

Feed-Ordner

Der Ordner **Feeds** von Secure Mail enthält alle ungelesenen E-Mails und Besprechungseinladungen sowie anstehende Besprechungen.

Anzeigen von Feed-Karten

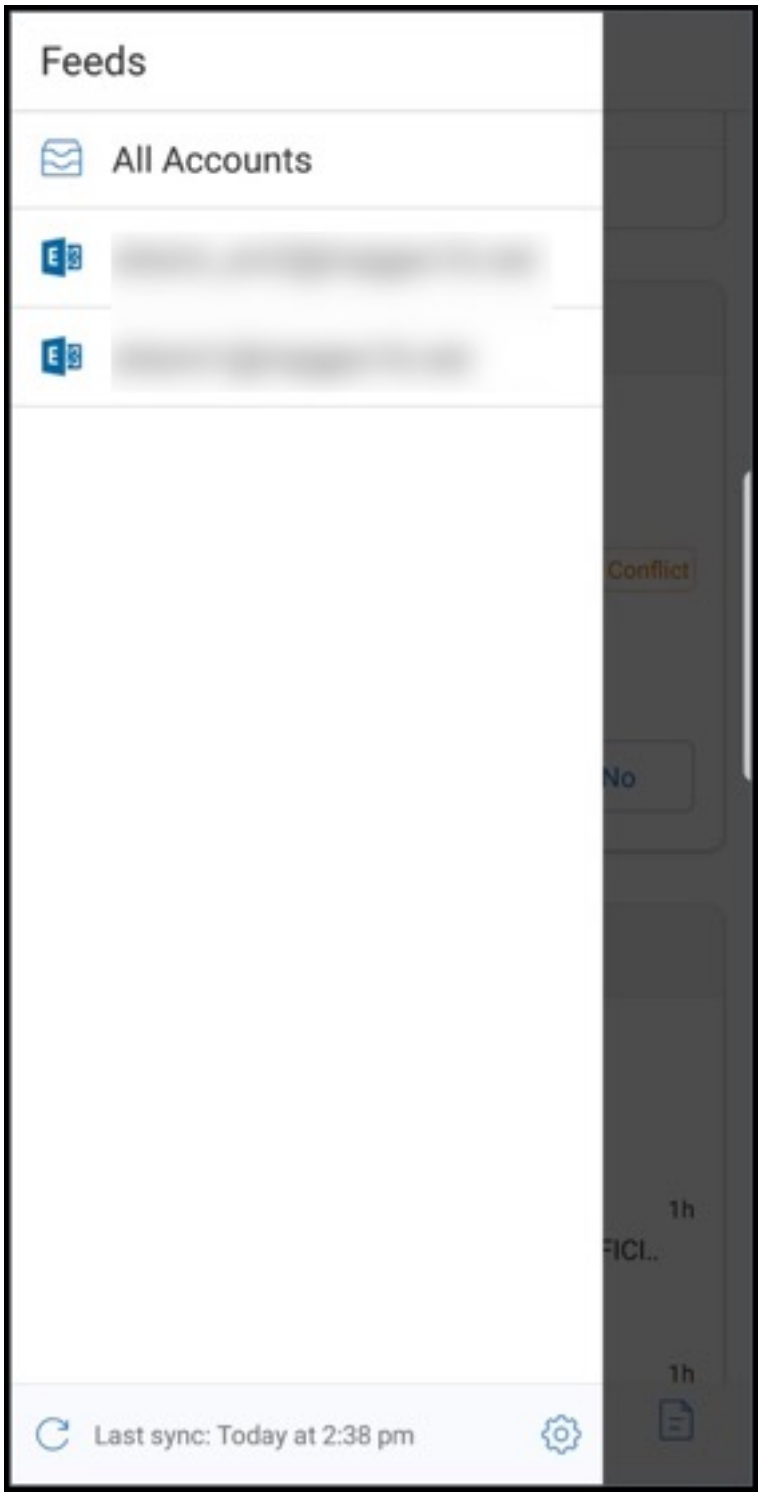
Tippen Sie auf das Symbol **Feeds** unten rechts auf der Tastenleiste.



Die folgenden Feeds-Karten erscheinen:

- Ungelesen
- Besprechungseinladungen
- Anstehende Besprechungen

Standardmäßig zeigt Secure Mail nur Feeds für Ihr primäres Konto an. Wenn Sie mehrere Konten haben, können Sie Feeds für ein anderes Konto anzeigen. Um Feeds für ein anderes Konto anzuzeigen, tippen Sie auf **Feeds**, tippen Sie auf das Hamburgersymbol und wählen Sie das Konto aus.



Die Reihenfolge der Anzeige von Feeds basiert auf dem Zeitstempel. Es gelten folgende Obergren-

zen:

- Fünf ungelesene E-Mails
- Zwei Besprechungseinladungen
- Drei anstehende Besprechungen

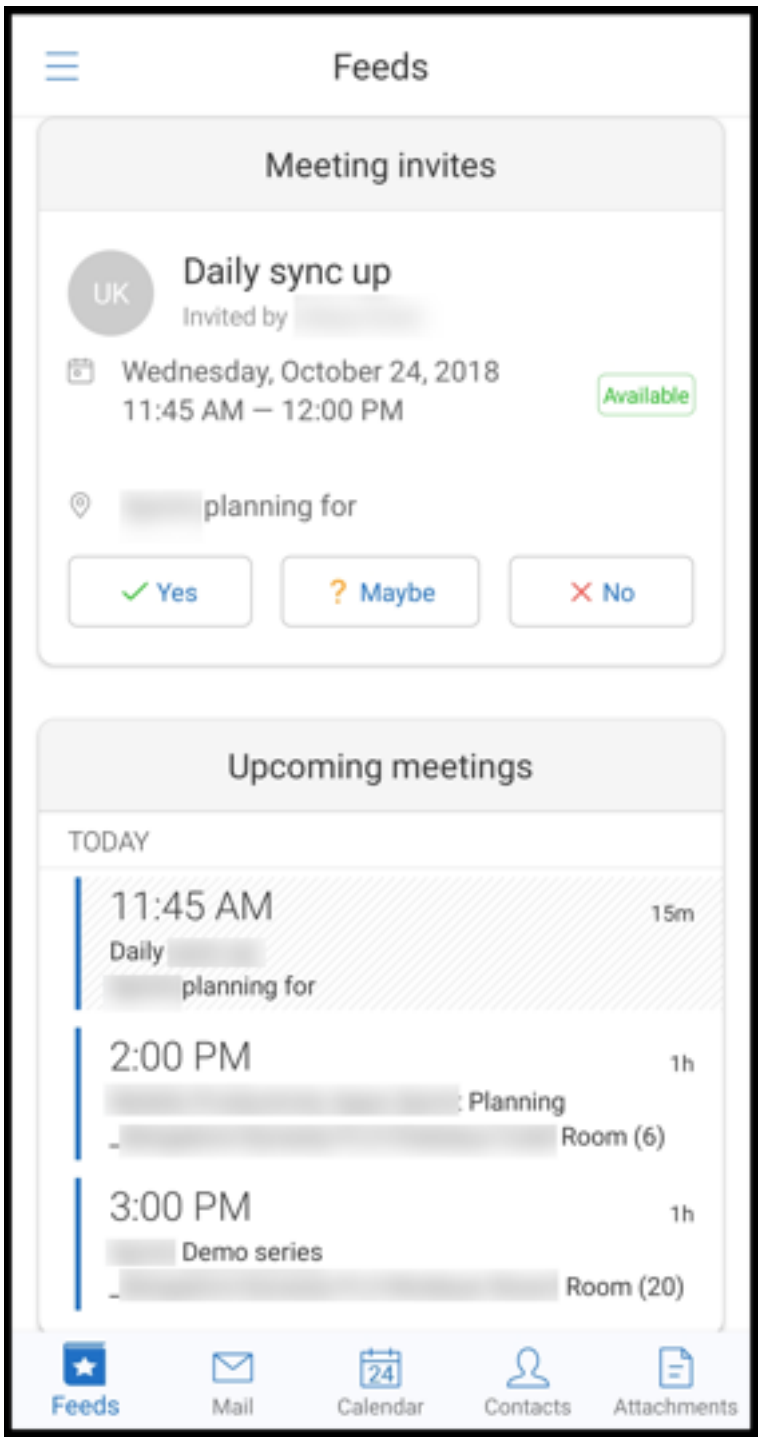
Tippen Sie auf **Alle anzeigen**, um alle Elemente in einer Feeds-Karte anzuzeigen.

> **Hinweis:**
>
> Die Anzahl der auf den einzelnen Karten angezeigten Feeds hängt vom Synchronisierungszeitraum ab, den Sie auf Ihrem Gerät festgelegt haben.

Verbesserungen am Ordner Feeds

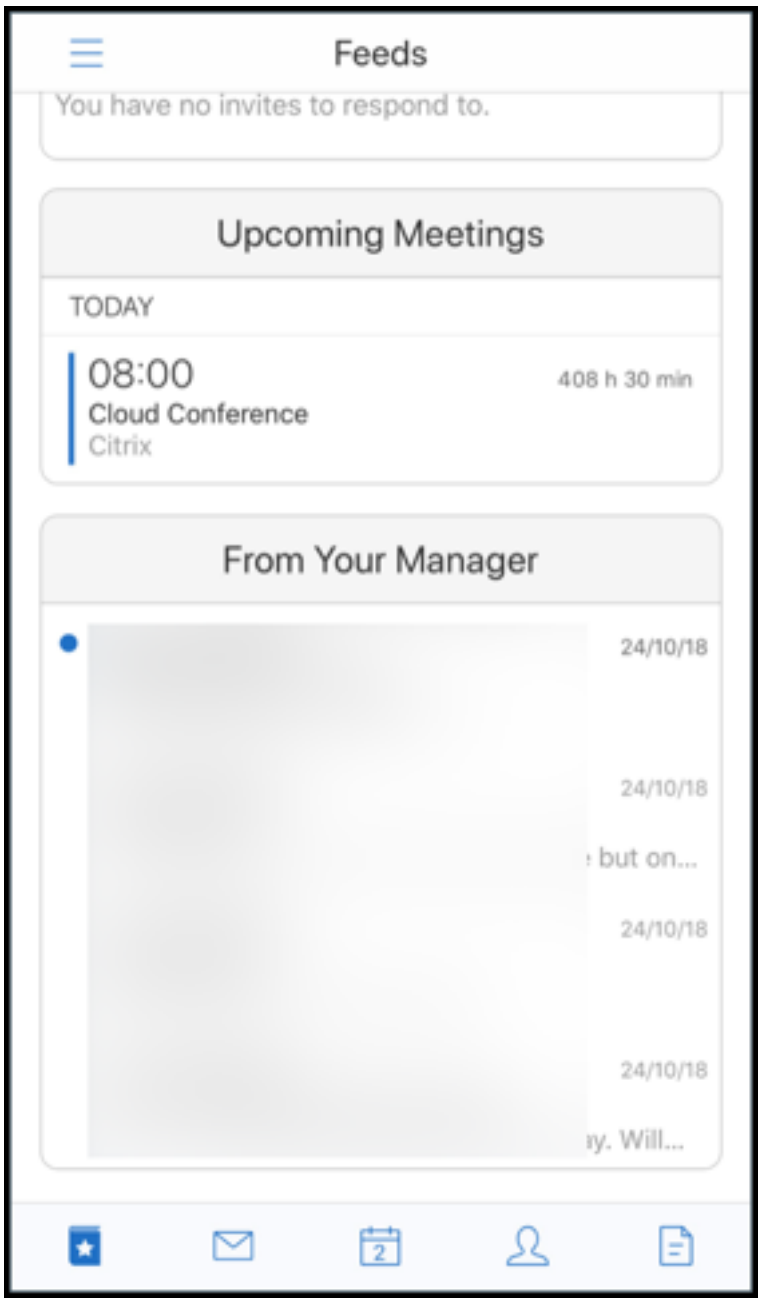
Nachfolgend sind die Verbesserungen am Ordner **Feeds** aufgeführt:

- 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.
- Anstehende Besprechungen für die nächsten 24 Stunden werden in der Feeds-Karte im Abschnitt **Heute** und **Morgen** angezeigt.



Feeds von Ihrem Manager

In Secure Mail 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:**
>
> Dieses Feature wird von IBM Lotus Notes-Servern nicht unterstützt.

Teilnehmen an Besprechungen vom Kalender aus

In Secure Mail können Benutzer direkt von Einladungen im Kalender aus an Besprechungen teilnehmen. Die folgende Tabelle enthält die unterstützten Besprechungstypen und Telefonnummernformate sowie die jeweiligen Einwahlbedingungen.

Unterstützte Besprechungstypen

Besprechungstyp	Identifizierungsanforderungen	Aktion nach Tippen auf "An Besprechung teilnehmen"
Microsoft Teams		Wenn die Microsoft Teams-App installiert ist, wird die App geöffnet und der Benutzer nimmt an der Besprechung teil. Wenn die App nicht installiert ist, sieht der Benutzer eine Option zum Installieren von Microsoft Teams aus dem App Store.
GoToMeeting (GTM)	Eine der folgenden Optionen im Besprechungsinhalt: 1. Dieser URL-Typ: `https://www1.gotomeeting.com/join/1234567892`. 2. GTM-Zugangscode in einem der folgenden Formate: GTM: 123456789, GTM –123456789, G2M –123456789, G2M: 123456789	Wenn die GTM-App installiert ist, wird die App geöffnet und der Benutzer nimmt an der Besprechung teil. Wenn die App nicht installiert ist, wird dem Benutzer die Option angezeigt, zum App-Store zu gehen und GTM zu installieren. Bei GTMs im Format gotomeet.me/benutzername wird die App geöffnet und der Benutzer kann an der Besprechung teilnehmen.

Besprechungstyp	Identifizierungsanforderungen	Aktion nach Tippen auf “An Besprechung teilnehmen”
WebEx		Citrix Secure Web wird geöffnet und öffnet die nicht umschlossene WebEx-App, wenn sie auf dem Gerät installiert ist. WebEx muss für Android der Secure Web-Richtlinie “Ausnahmeliste für eingeschränktes Öffnen” und für iOS der Richtlinie “Zulässige URLs”als Ausnahme hinzugefügt werden.
Skype for Business		Benutzer können auf einen Link klicken, der Secure Web öffnet. Daraufhin wird die nicht umschlossene Skype for Business-App geöffnet, wenn sie auf dem Gerät installiert ist. Fügen Sie unter Android die Skype for Business-App als Ausnahme der Richtlinie “Ausnahmeliste für eingeschränktes Öffnen”in Secure Web hinzu. Fügen Sie die Ausnahme unter iOS der Richtlinie “Zulässige URLs” hinzu.

Durch Konfigurieren der Richtlinien in folgender Liste können Benutzer auf einen Besprechungslink tippen, um die entsprechende App zu öffnen.

Microsoft Teams-App

- **iOS —Richtlinie “Allow URLs”: ^mteams:
- **Android —Richtlinie “Open-in Exclusions”: {action=android.intent.action.VIEW scheme=mteams package=com.microsoft.teams}

Zoom-App

- **iOS - Richtlinie "Allow URLs":** +^zoomus:
- **Android - Richtlinie "Open-in Exclusions":**{action=android.intent.action.VIEW scheme=zoomus package=us.zoom.videomeetings}

Webex (nicht umschlossene App)

- **iOS - "Allow URLs"Policy":** +^wbx: z. B. Richtlinienzeichenfolge: ^http:,^https:,^mailto:=ctxmail:,+^citrixre g2m-2:,+^col-g2w-2:,+^wbx:,+^maps:ios_addr:
- **Android - Richtlinie "Open-in Exclusions":** {action=android.intent.action.VIEW scheme=wbx package=com.cisco.webex.meetings}

Skype for Business

- **iOS - Richtlinie "Allow URLs":** +^lync:
- **Android - Richtlinie "Open-in Exclusions":**{action=android.intent.action.VIEW scheme=lync package=com.microsoft.office.lync15}

Skype

- **iOS - Richtlinie "Allow URLs":** +^skype:
- **Android - Richtlinie "Open-in Exclusions":** {action=android.intent.action.VIEW scheme=skype package=com.skype.raider}

Einwahlbedingungen

In der folgenden Liste sind der Besprechungstyp und das jeweils unterstützte Telefonnummern- und Konferenzcodeformat aufgeführt.

GoToMeeting (GTM):

Unterstützte Telefonnummernformate:

- Alle Telefonnummern in GTM-Formaten. Beispiele:
  - Indien (gebührenfrei): 000 800 100 7855
  - USA (gebührenfrei): 1 877 309 2073
- Alle Telefonnummern, die den Formatstandards in RFC 3966 entsprechen. Einzelheiten finden Sie im Dokument Internet standards track protocol.

Unterstützte Konferenzcodeformate:

Der Konferenzcode wird aus einem der folgenden Formate im Besprechungstext aufgenommen:

- URL (*.gotomeeting.com/join/123456789)

- URL (Format `gotomeet.me/username`)
- GTM-Formate wie "GTM:123456789"
- G2M-Formate wie "G2M:123456789"
- Formate wie "Zugangsscode: 123456789"

WebEx:

Unterstützte Telefonnummernformate:

- Alle Telefonnummern im WebEx-Einwählformat. Beispiele (Verizon und USA):
  - 1-866-652-5088
  - 1-517-466-3109
- Alle Telefonnummern im WebEx-Audioverbindungsformat. Beispiel:
  - 1-650-479-3207 (US-Toll)
- Alle Telefonnummern, die den Formatstandards in RFC 3966 entsprechen.

Unterstützte Konferenzcodeformate:

Der Besprechungsinhalt muss eines der folgenden Formate enthalten:

- Besprechungsnummer: 123 456 789
- Zugriffscode: 123 456 789

> **Hinweis:**
>
> Bei Konferenzcodes mit bis zu neun Ziffern wird automatisch das #-Zeichen zum Einwählen in die Besprechung hinzugefügt.

Skype for Business

Unterstützte Telefonnummernformate:

- Alle Telefonnummern, die den Formatstandards in RFC 3966 entsprechen. Einzelheiten finden Sie im Dokument Internet standards track protocol.

Unterstützte Konferenzcodeformate:

Der Besprechungstext enthält Folgendes: "Konferenzkennung: 123456789"

> **Hinweis:**
>
> Das #-Zeichen wird automatisch für Skype for Business-Besprechungen hinzugefügt.

Allgemeine Audiokonferenzinformationen

Unterstützte Telefonnummernformate:

- Alle Telefonnummern, die den Formatstandards in RFC 3966 entsprechen Einzelheiten finden Sie im Dokument Internet standards track protocol. Beispiele:
  - 5555555555
  - (555) 555-5555
  - 555-555-5555
  - 555-555-555-5555 (bei einer Landesvorwahl)
  - 1-555-555-5555
  - +1-555-555-5555

> **Hinweis:**
>
> Verwenden Sie ein einzelnes Trennzeichen zwischen den Ziffern der Telefonnummer. Beispiel: Bei “) –”wird die Nummer nicht erkannt.

Unterstützte Konferenzcodeformate:

Empfohlenes Format: “(Telefonnummer)”,”(Code)”

Sie können bei Bedarf bis zu vier Kommas und das #-Zeichen angeben. In der Tabelle weiter unten in diesem Dokument finden Sie eine Liste der unterstützten Formate.

Für eine Audiokonferenz können Benutzer bei folgenden Formaten auf die **Einwähltaste** tippen. Wenn sie stattdessen auf die Telefonnummer im Text der Besprechung im Kalender tippen, können sie sich in die Besprechung einwählen. Sie müssen die Konferenzcodes dann manuell eingeben. Die folgenden Formate für Telefonnummern und Konferenzcodes werden unterstützt.

Unterstützte Telefonnummernformate	Trennzeichen für Konferenzcode	Beispiel
Alle Telefonnummern, die den Formatstandards in RFC 3966 entsprechen. Beispiele: 5555555555; (555) 555-5555; 555-555-5555; 555-555-555-5555 (bei vorhandenem Ländercode); 1-555-555-5555;+1-555-555-5555	Teilnehmercode	1-888-999-9999 Teilnehmercode: 9999999
	Teilnehmer-PIN	1-888-999-9999 Teilnehmer-PIN: 99999999

Unterstützte Telefonnummernformate	Trennzeichen für Konferenzcode	Beispiel
	Gastcode	1-888-999-9999 Gastcode: 99999999
	Gast-PIN	1-888-999-9999 Gast-PIN: 99999999
	Teilnehmer-/Gastcode	1-888-999-9999 Teilnehmer-/Gastcode: 99999999
	Vorsitzcode	1-888-999-9999 Vorsitzcode: 99999999
	Vorsitz-PIN	1-888-999-9999 Vorsitz-PIN: 99999999
	Leitungscode	1-888-999-9999 Leitungscode: 99999999
	Leitungs-PIN	1-888-999-9999 Leitungs-PIN: 99999999
	Host-PIN	1-888-999-9999 Host-PIN: 99999999
	PIN	1-888-999-9999 PIN: 99999999
	Zugangscode	1-888-999-9999 Zugangscode: 99999999
	Code	1-888-999-9999 Code: 99999999
	Konferenzcode	1-888-999-9999 Konferenzcode: 99999999
	Konferenzkennung	1-888-999-9999 Konferenzkennung: 99999999
	,	+1 (631) 992-3240,958209234#
	„	+1 (631) 992-3240„958209234#
	„,	+1 (631) 992-3240„,958209234#
	„„	+1 (631) 992-3240„„958209234#
	Passcode	+1 (631) 992-3240 Passcode 958209234#
	ext	+1 (631) 992-3240 pc 958209234#
	ext.	+1 (631) 992-3240 pc 958209234#

Unterstützte Telefonnummernformate	Trennzeichen für Konferenzcode	Beispiel
	;ext=	+1 (631) 992-3240; pc 958209234#
	extn	+1 (631) 992-3240 pc 958209234#
	HC	+1 (631) 992-3240 HC 958209234#
	xtn	+1 (631) 992-3240 pc 958209234#
	xt	+1 (631) 992-3240 pc 958209234#
	x	+1 (631) 992-3240 x 958209234#
	PC	+1 (631) 992-3240 PC 958209234#
	pc	+1 (631) 992-3240 pc 958209234#

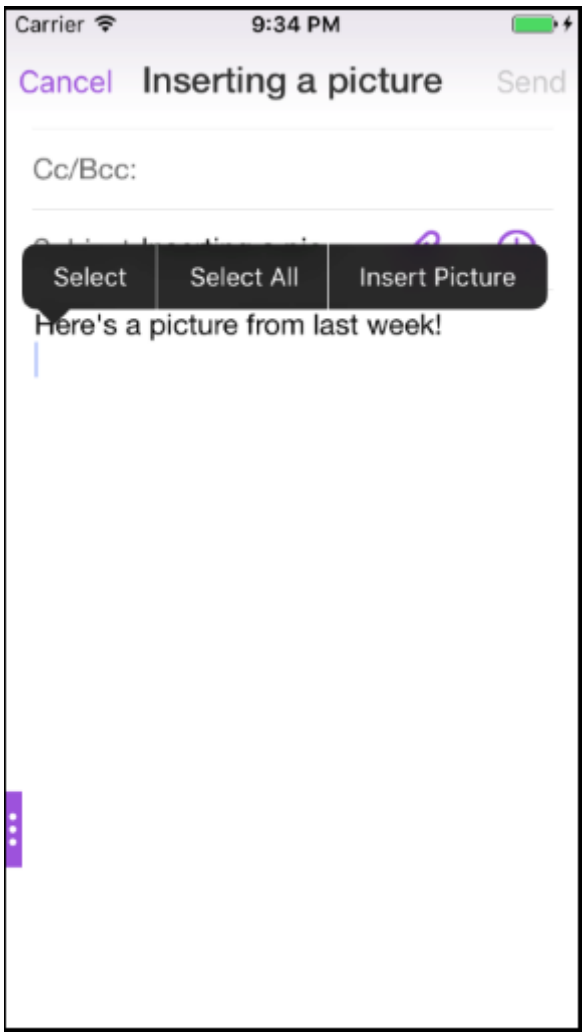
Persönliche Kalenderüberlagerung

Auf iOS- und Android-Geräten können Sie Ihren persönlichen Kalender aus der nativen Kalender-App importieren und persönliche Ereignisse in Secure Mail anzeigen. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Ereignisse in persönlichem Kalender anzeigen.

Einfügen eines Inlinebilds

Im Folgenden wird beschrieben, wie Sie ein Inline-Bild einfügen.

1. Durch langen Fingertipp in den Nachrichtentext einer E-Mail können Sie ein Inlinebild an Ihre E-Mail anhängen. Tippen Sie in den angezeigten Optionen auf **Bild einfügen**.



2. Secure Mail fordert Sie gegebenenfalls auf, den Zugriff auf Ihre Fotos zu bestätigen. Die Fotogalerie wird angezeigt. Navigieren Sie zur Galerie und tippen Sie auf das Bild, das Sie einfügen möchten.

3. Die E-Mail enthält nun das ausgewählte Bild.

Wischaktionen

Auf iOS- und Android-Geräten können Sie Aktionen durch Streichen einer E-Mail nach links oder rechts ausführen. Die Hilfedokumentation zu diesem Feature finden Sie in der Citrix-Benutzerhilfe unter Wischaktionen verwenden.

Teilnahme an Skype for Business-Besprechungen unter iOS und Android

Sie können nahtlos über Secure Mail aus an Skype for Business-Besprechungen teilnehmen. Für dieses Feature muss die Skype for Business-App auf Ihrem Gerät installiert sein.

Teilnahme an einer Skype for Business-Besprechung

1. Tippen Sie auf die Erinnerung oder auf das Kalendereregnis für die Skype for Business-Besprechung.
2. Tippen Sie im Bildschirm **Ereignisdetails** auf die Skype-Schaltfläche **Meeting beitreten**. Die Skype for Business-Besprechung wird in einem neuen Fenster gestartet.

   Wenn Skype for Business nicht auf dem Gerät installiert ist, tippen Sie auf **Skype installieren**.

In-App-Vorschau von Anlagen und andere Verbesserungen für Anlagen

Sie können nun Anlagen (MS Office und Bilder) in der Secure Mail-App anzeigen, anstatt sie mit Anwendungen von Drittanbietern wie QuickEdit öffnen zu müssen.

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.
- Wählen Sie eine neue Nachricht, an die Sie die Datei anfügen möchten.
- Speichern Sie die Datei für den Offlinezugriff.
- Löschen Sie die Anlage aus den Offlinedateien.
- Öffnen Sie die Anlage mit einer anderen Anwendung.
- Zeigen Sie die Quell-E-Mail oder das Kalendereregnis der Anlage an.

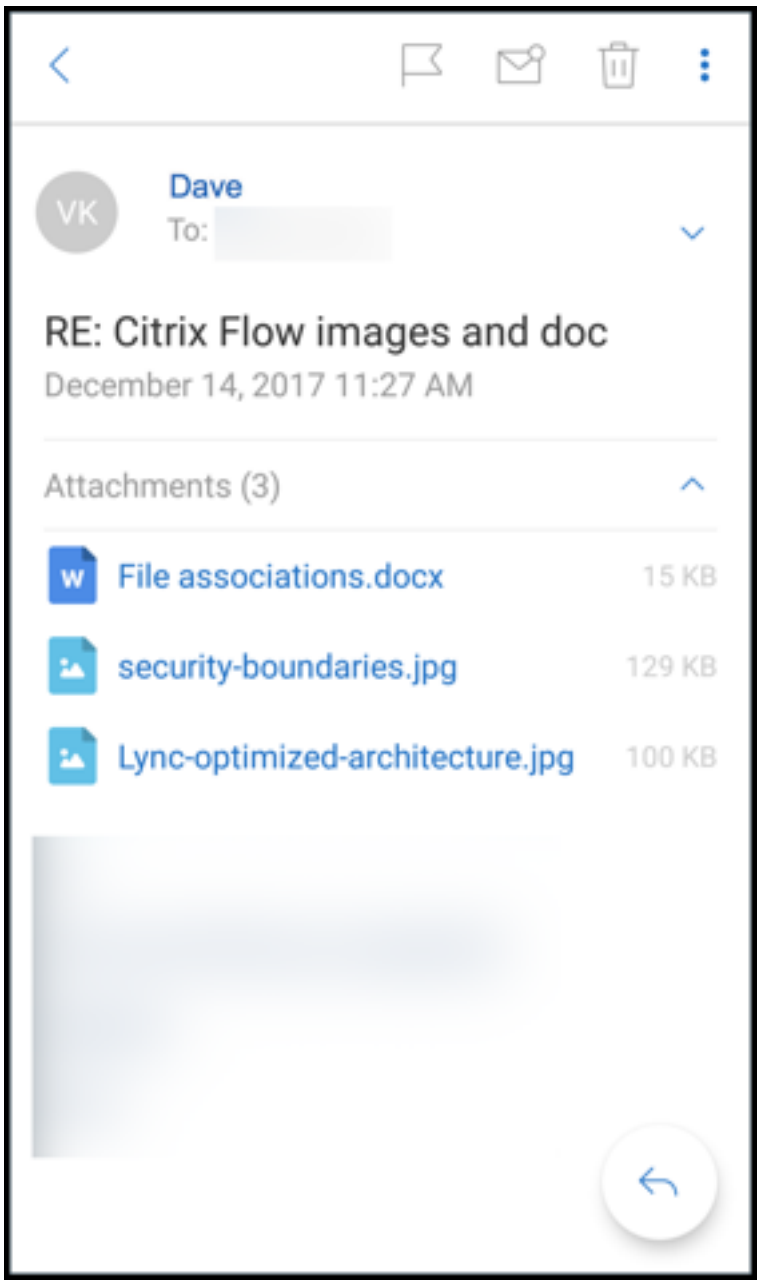
> **Hinweis:**
>
> Sie können die Quell-E-Mail oder das Kalendereregnis nur anzeigen, wenn Sie Anlagen im **Anlagenrepository** anzeigen.

Außerdem können Sie in den folgenden Fällen eine Vorschau der Anlagen anzeigen:

- Anzeigen einer Nachricht
- Verfassen einer neuen Nachricht
- Anlagenordner
- Kalendereregnisse

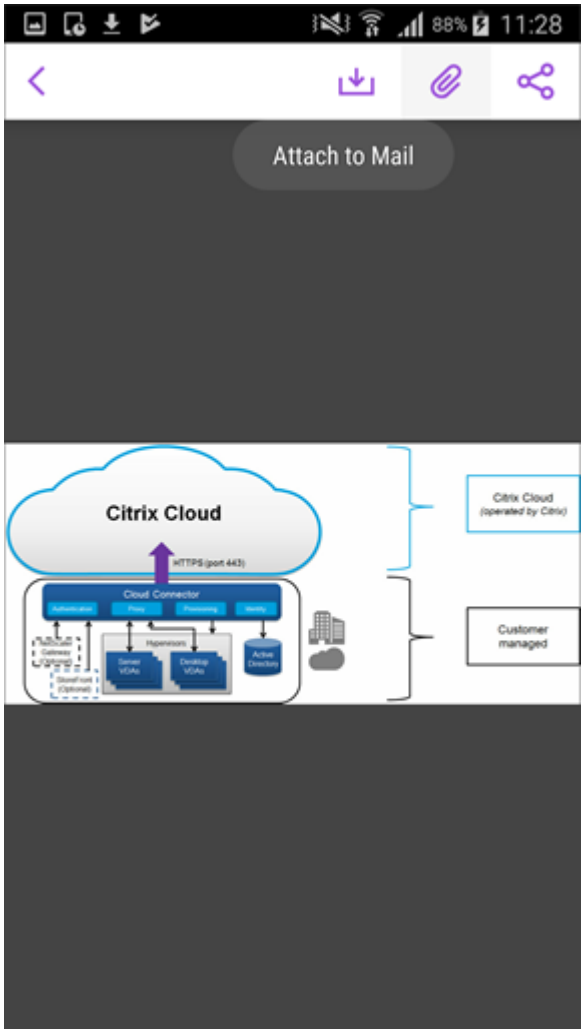
Wählen Sie eine neue Nachricht, an die Sie die Datei anfügen möchten

1. Öffnen Sie die E-Mail mit der Anlage.

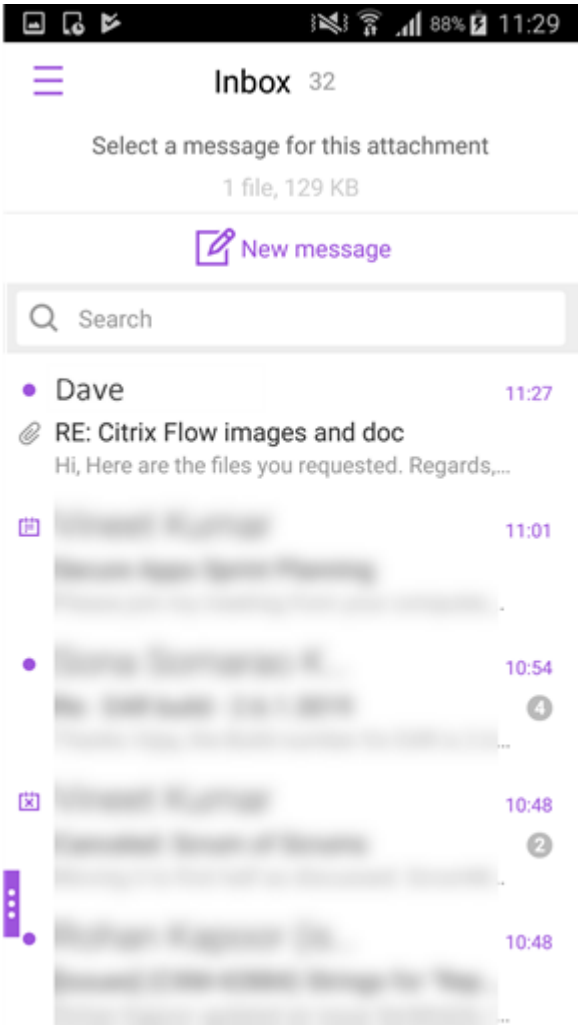


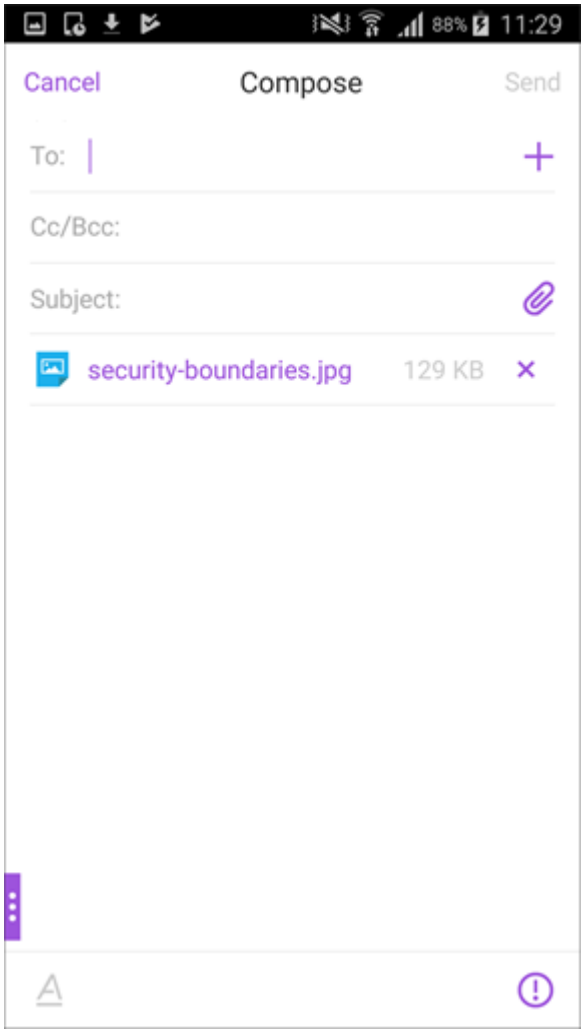
2. Tippen Sie auf die Anlage.
3. Tippen Sie auf das Symbol **Anfügen**.

   Der Posteingang wird angezeigt.



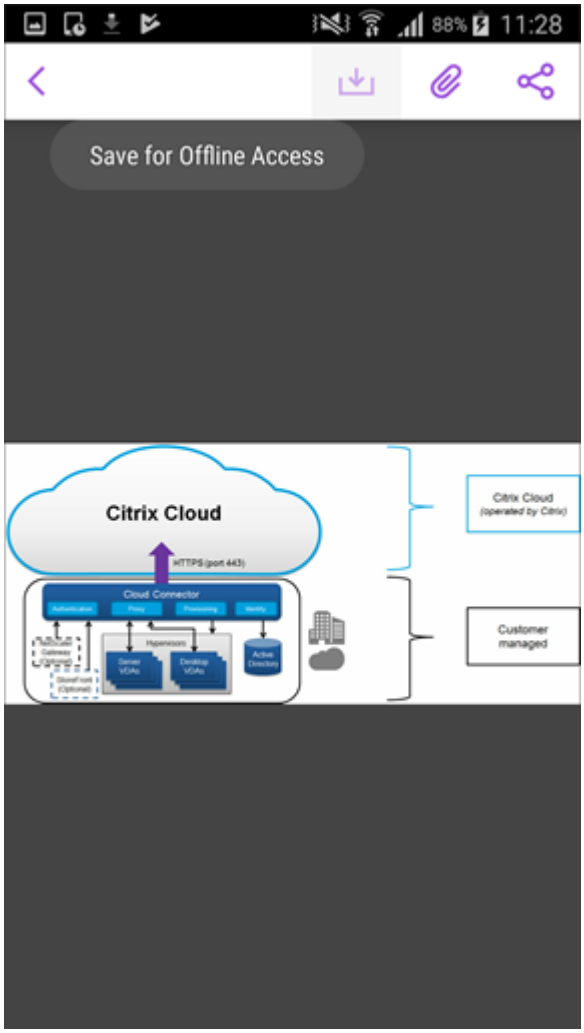
4. Wählen Sie eine vorhandene Nachricht, an die diese Datei angefügt werden soll, oder tippen Sie auf **Neue Nachricht**, um diese Datei an eine neue Nachricht anzufügen.





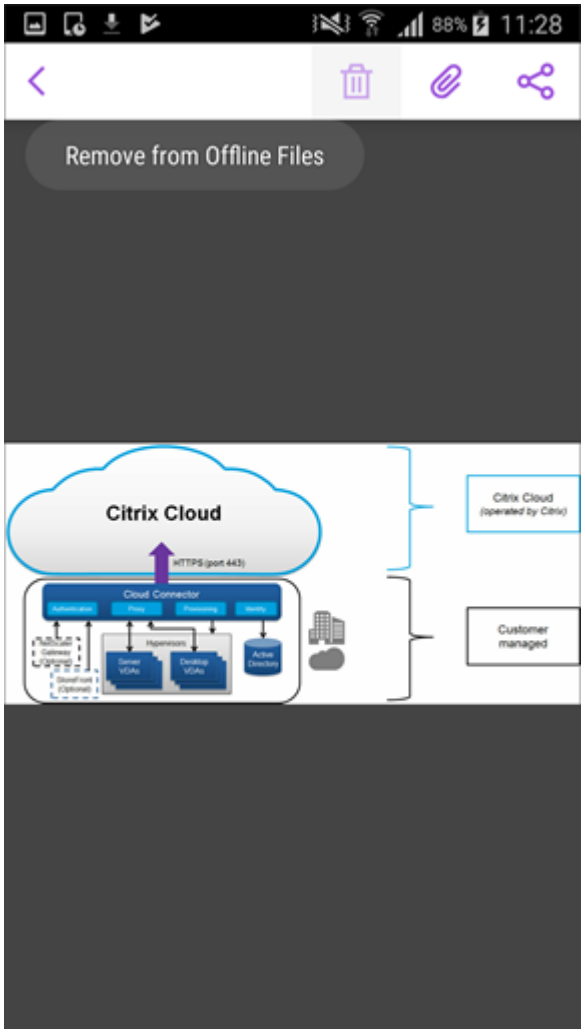
Speichern Sie die Datei für den Offlinezugriff

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



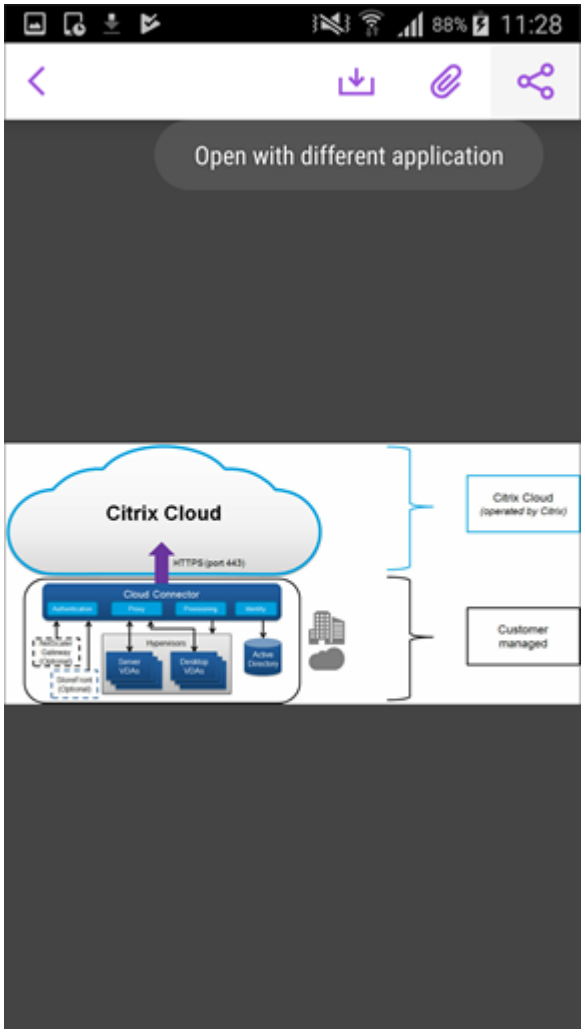
Löschen einer Anlage aus Offlinedateien

1. Öffnen Sie die Anlage.
2. Tippen Sie oben rechts auf der Seite auf das Symbol **Mehr** und dann auf **Aus Offlinedateien entfernen**, um die Anlage in den Offlinedateien zu löschen.

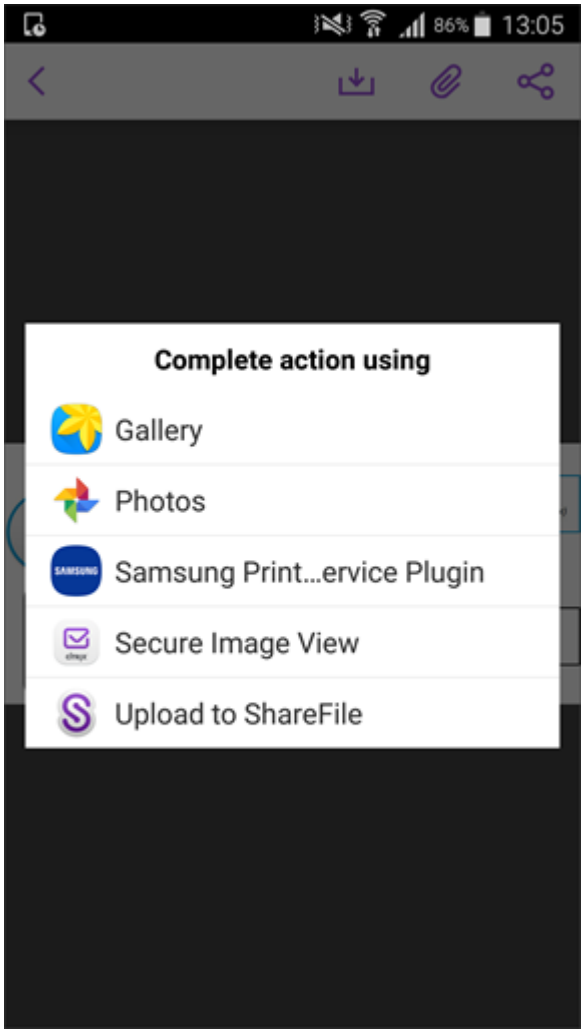


Öffnen Sie die Anlage mit einer anderen Anwendung

1. Öffnen Sie die Anlage.
2. Tippen Sie oben rechts auf der Seite auf das Symbol **Mehr** und dann auf **Öffnen mit**, um die Anlage mit einer anderen Anwendung zu öffnen.



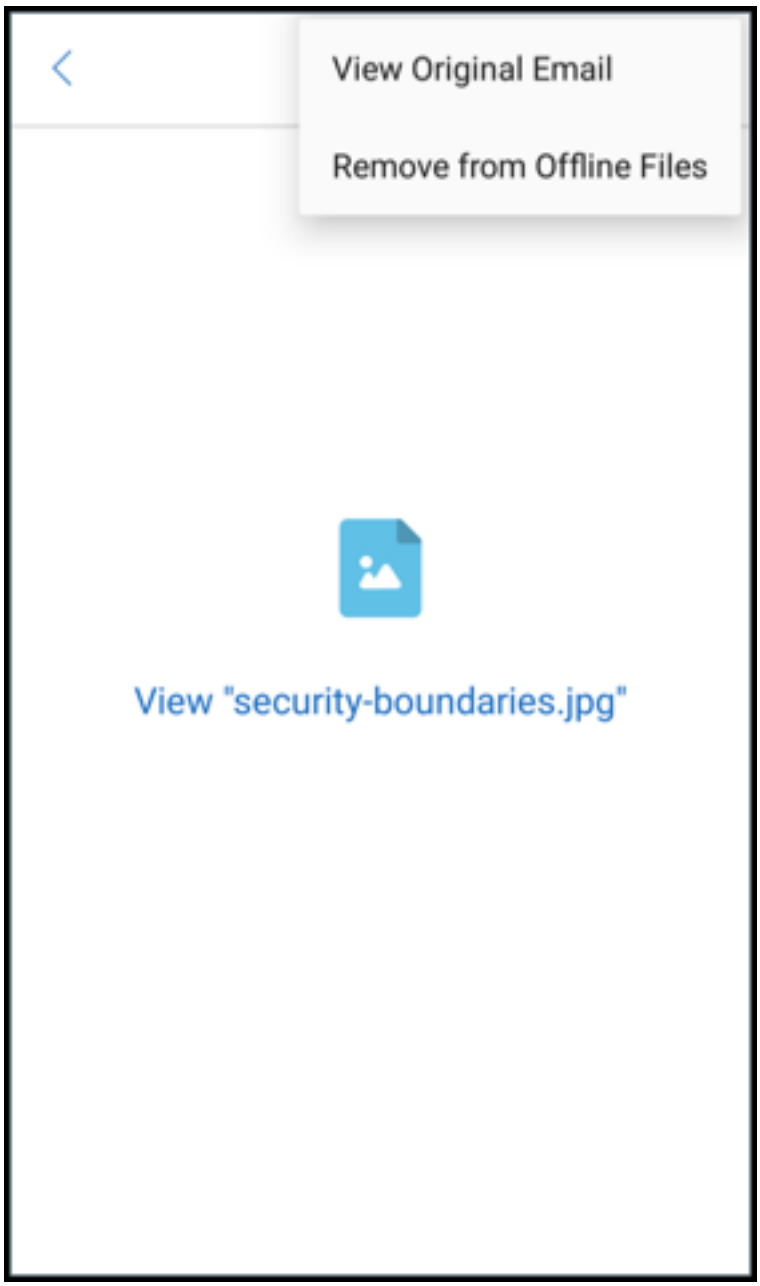
3. Tippen Sie unter den angezeigten Optionen auf die, mit der Sie die Anlage öffnen möchten.



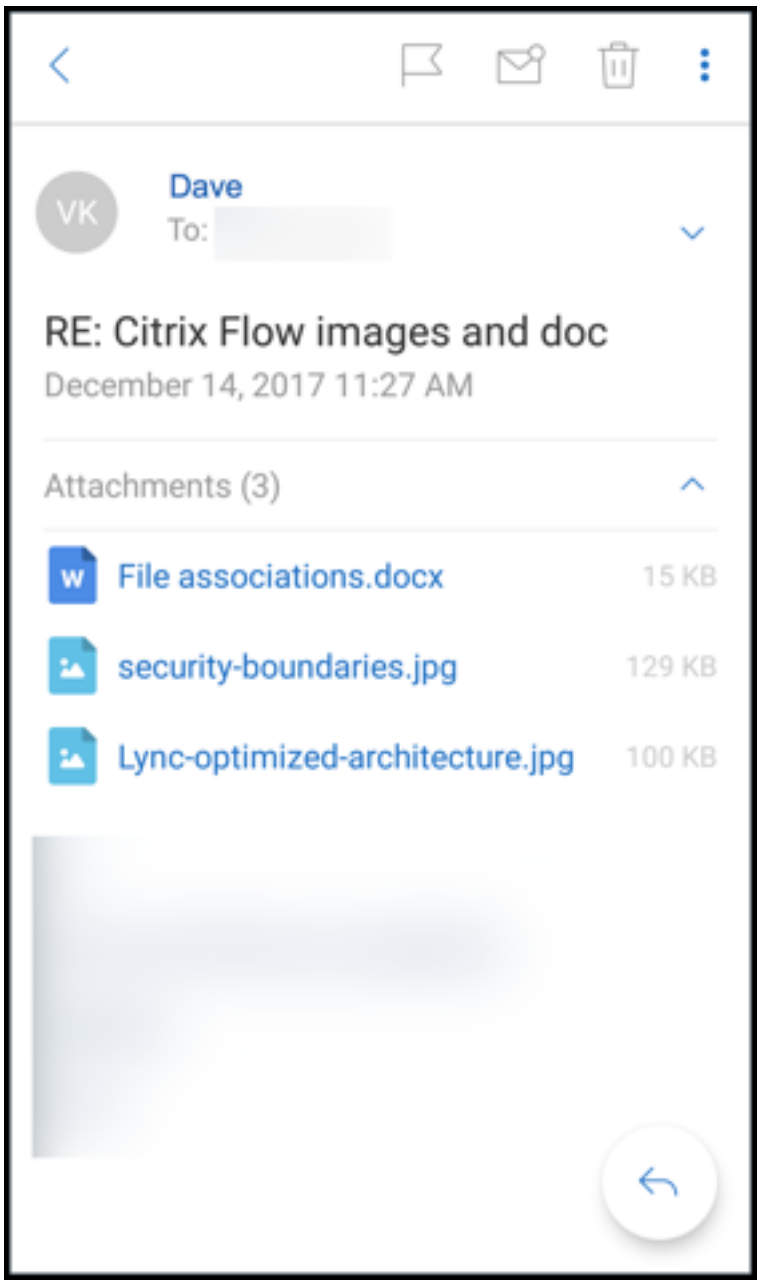
Zeigen Sie die Quell-E-Mail oder das Kalenderereignis der Anlage an

1. Tippen Sie unten rechts auf dem Bildschirm auf das Symbol **Anlagen**.
2. Tippen Sie auf **OFFLINE**.

3. Tippen Sie auf die Anlage und dann oben rechts auf dem Bildschirm auf das Symbol **Mehr**.



4. Die Quell-E-Mail wird angezeigt.



Migration von Benutzernamen auf E-Mail-Adressen (UPN)

In Secure Mail für iOS und Android können Sie von der Authentifizierung mit Exchange-Benutzernamen und -Kennwort auf eine Authentifizierung mit Benutzerprinzipalnamen (UPN) und Kennwort migrieren.

Bei aktiviertem Feature ist keiner der folgenden Schritte erforderlich:

- Neuinstallation von Secure Mail
- Löschen und Hinzufügen des Kontos in Secure Mail

- Ändern des Benutzernamens in Secure Mail

Voraussetzungen

Stellen Sie vor der Migration sicher, dass Benutzer Secure Mail Version 10.7.25 oder höher ausführen. Für dieses Feature müssen Sie die Richtlinie "Attempt Username Migration On Auth Failure" aktivieren.

Migration auf eine UPN-basierte Authentifizierung

1. Aktivieren Sie in Endpoint Management die Richtlinie "Bei Authentifizierungsfehler Migration von Benutzernamen versuchen".
2. Migrieren Sie Ihr Exchange-Benutzerkonto zu einem neuen UPN, der mit der primären SMTP-E-Mail-Adresse des Benutzers übereinstimmt.
   Dadurch wird ein Authentifizierungsfehler ausgelöst. Secure Mail versucht dann die Authentifizierung mit der primären SMTP-E-Mail-Adresse.

Bei erfolgreicher Authentifizierung wird das Benutzerkonto auf den aktualisierten UPN migriert.

Überprüfen der Migration

Auf iOS-Geräten: Gehen Sie zu **Einstellungen** und tippen Sie dann auf das Konto, um die Details anzuzeigen. Bei erfolgreicher Migration wird auf dem Bildschirm **Konto** die primäre SMTP-E-Mail-Adresse im Feld **Benutzername** angezeigt.

Auf Android-Geräten: Gehen Sie zu **Einstellungen** und tippen Sie dann auf das Konto, um die Details anzuzeigen. Bei erfolgreicher Migration wird auf dem Bildschirm **Kontodetails** die primäre SMTP-E-Mail-Adresse im Feld **Benutzername** angezeigt.

Persönliche Verteilerlisten

Voraussetzungen

- Exchange-Webdienste (EWS) sind auf Ihrem Exchange Server aktiviert.
- Microsoft Exchange Server Version 10 SP1 oder höher.

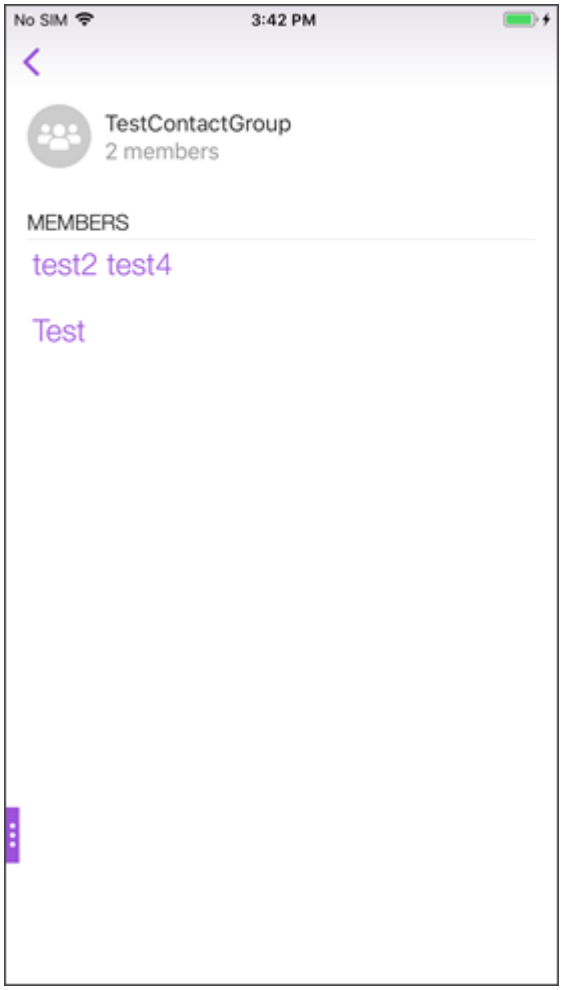
Secure Mail für iOS und Android unterstützt persönliche Kontaktgruppen. Sie können in Secure Mail Kontaktgruppen anzeigen, die Sie im Outlook-Desktopclient erstellt haben. Die Kontaktgruppen, die Sie erstellt haben, werden in Secure Mail in den Kontakten angezeigt.

> **Hinweis:**
>
> In Secure Mail können Sie nicht die Mitglieder einer verschachtelten Kontaktgruppe anzeigen.

Sie können die persönlichen Verteilerlisten beim Verfassen einer E-Mail oder Erstellen eines Kalenderereignisses verwenden. Wenn Sie eine Gruppe "Persönliche Kontakte"(Verteilerliste) mit Exchange erstellt haben, können Sie die Liste in Secure Mail anzeigen.

Anzeigen einer persönlichen Verteilerliste

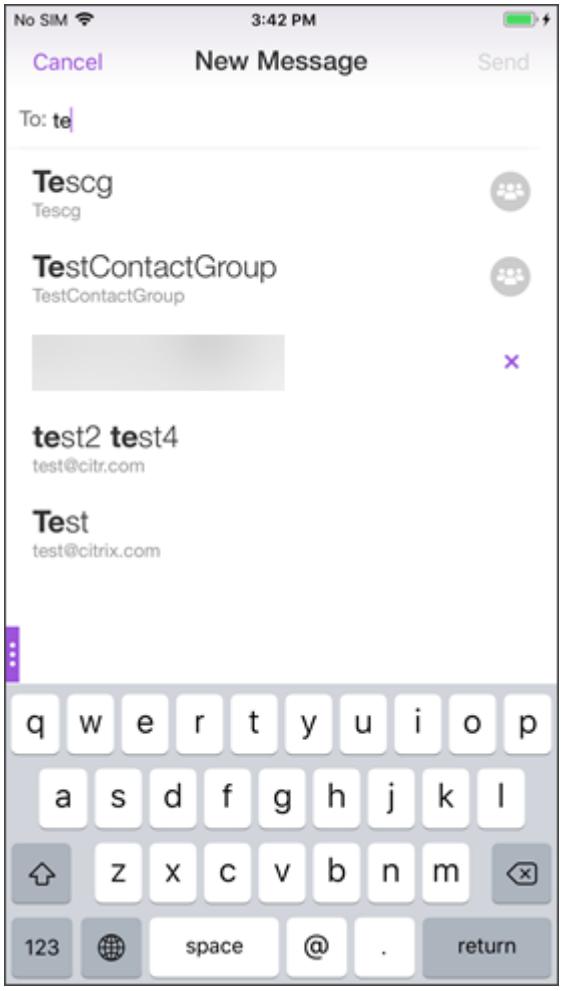
1. Öffnen Sie in Secure Mail **Kontakte**.
2. Geben Sie den Namen der Kontaktgruppe ein.
   Die Gruppe erscheint im Suchergebnis.
3. Tippen Sie auf die Kontaktgruppe, um die Mitglieder anzuzeigen.



> **Hinweis**:
>
> In Secure Mail können Sie nicht eine Kontaktgruppe bearbeiten.

Verfassen einer E-Mail an eine Kontaktgruppe

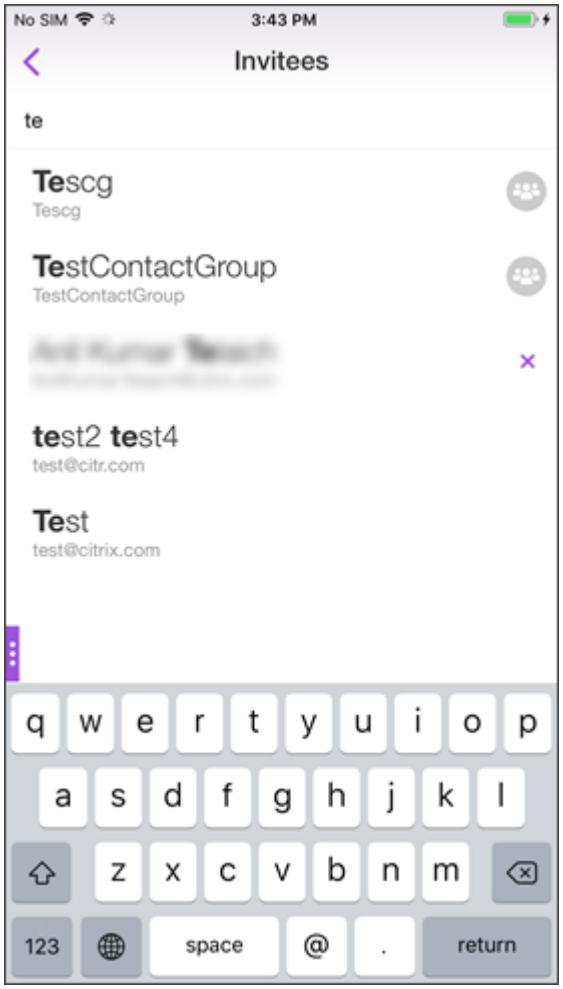
1. Öffnen Sie Secure Mail und tippen Sie auf die unverankerte Aktionsschaltfläche **Bearbeiten**, um eine E-Mail zu erstellen.
2. Geben Sie im Bildschirm **Neue Nachricht** den Namen der Kontaktgruppe in das Feld **An:** ein.
3. Wählen Sie in der Liste der angezeigten Kontakte die Kontaktgruppe aus.



Kontaktgruppen sind mit folgendem Symbol gekennzeichnet:

Senden einer Kalendereinladung an eine Kontaktgruppe

1. Öffnen Sie Secure Mail und navigieren Sie zu **Kalender**.
2. Tippen Sie auf das **+**-Symbol, um ein Kalenderereignis zu erstellen.
3. Tippen Sie auf dem Bildschirm **Neues Ereignis** auf **Eingeladene**, um Mitglieder hinzuzufügen.
4. Geben Sie den Namen der Kontaktgruppe ein, um die Einladung an die Gruppe zu senden.



5. Wählen Sie in der Liste der angezeigten Kontakte die Kontaktgruppe aus.

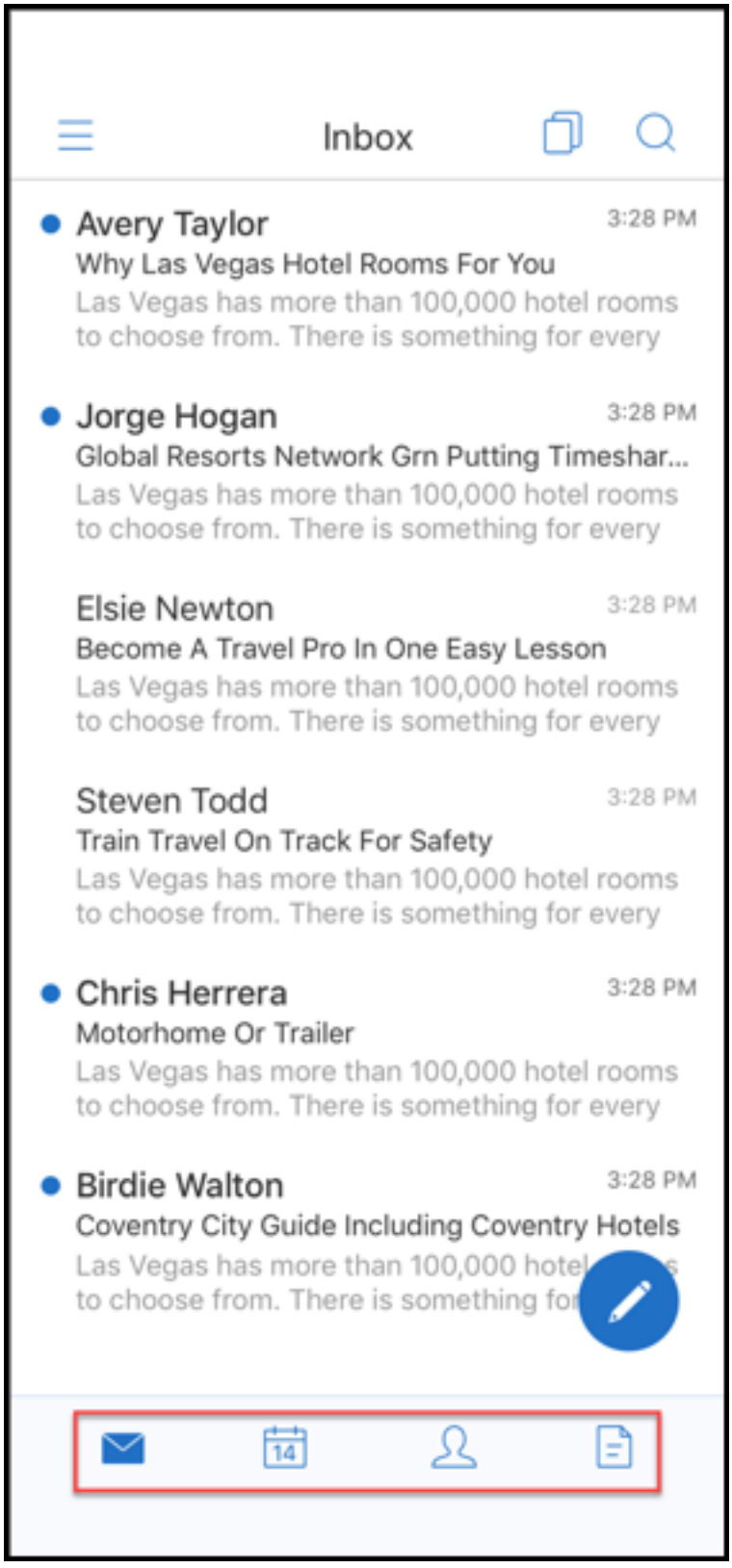
Ordnersynchronisierung

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

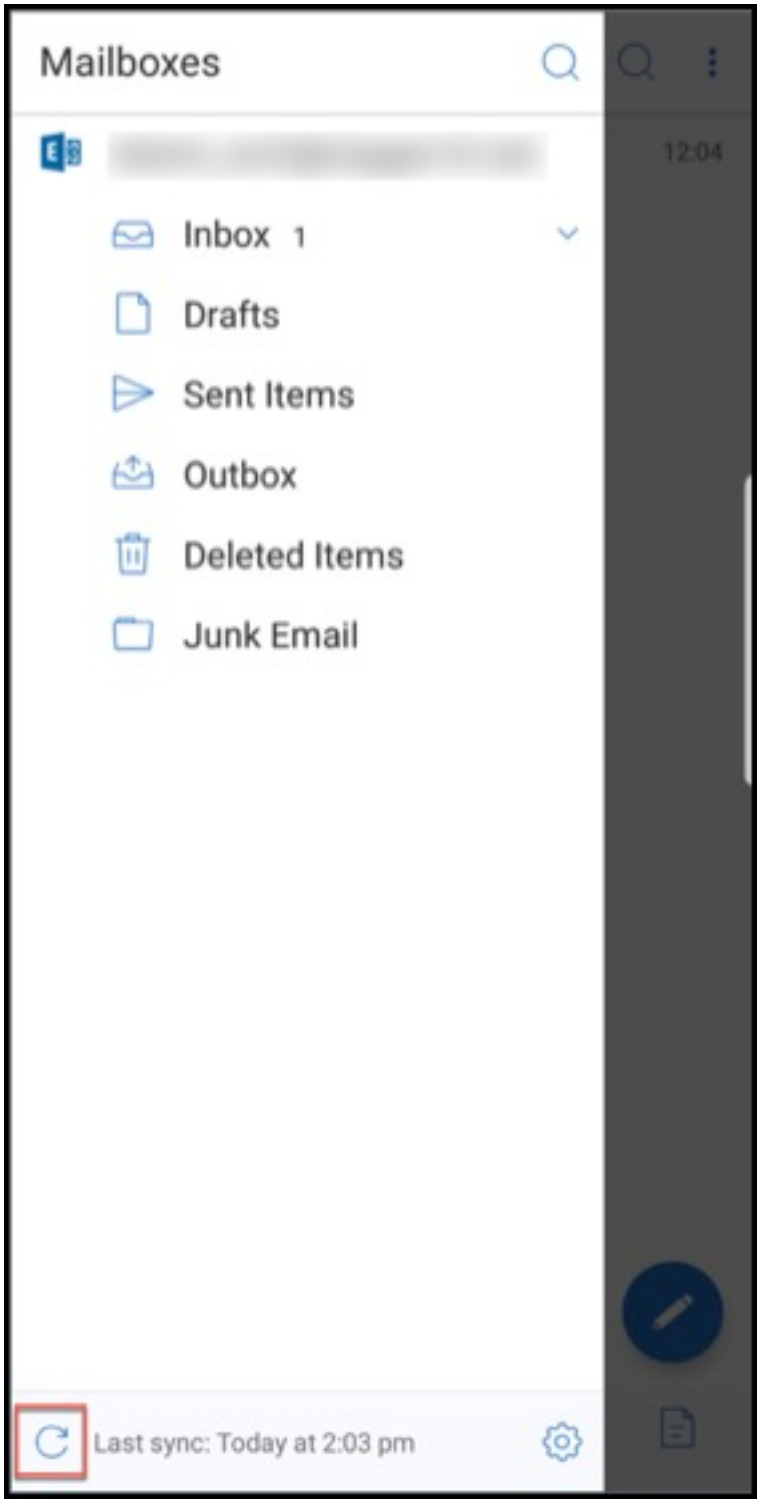
Synchronisieren von Ordnern

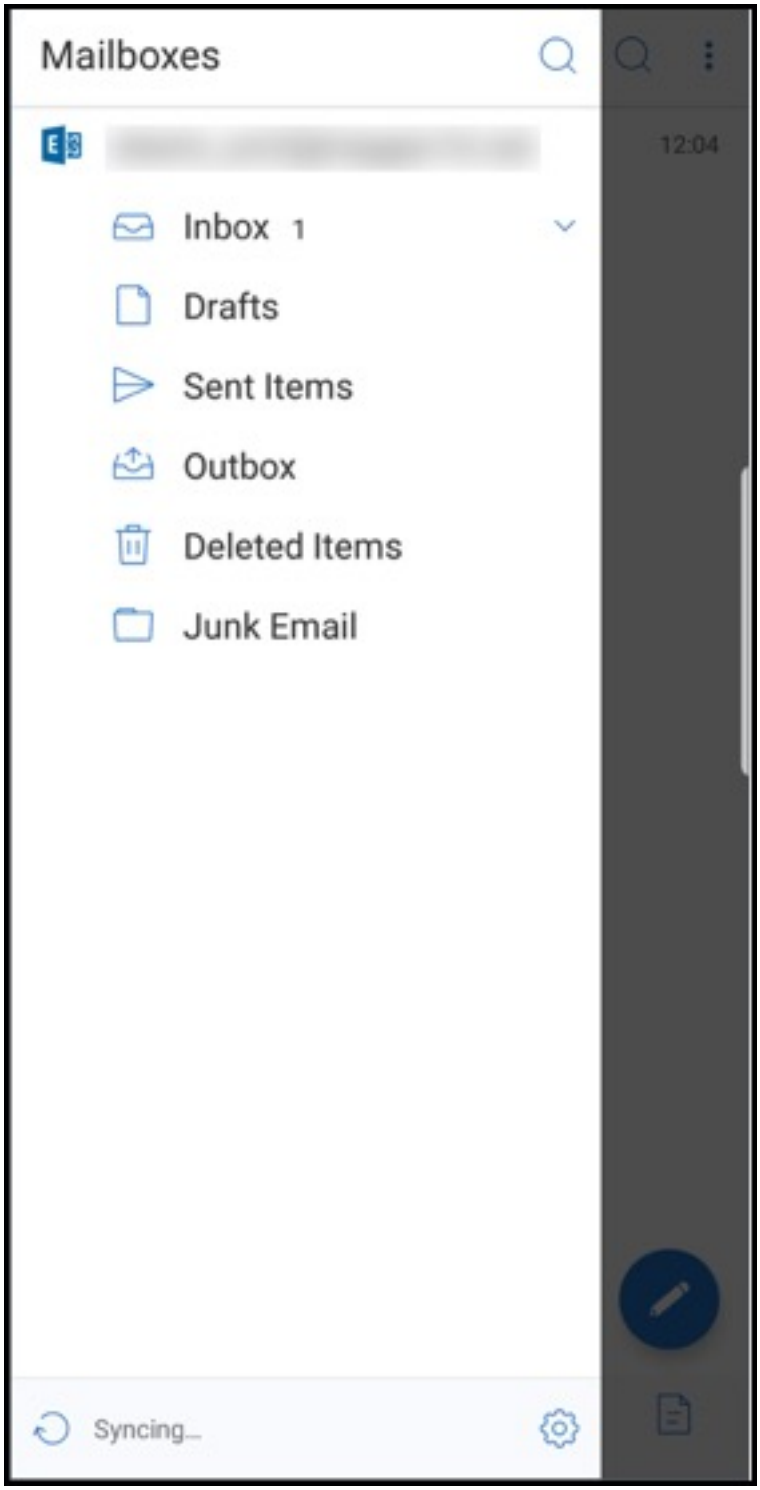
1. Öffnen Sie Secure Mail.
2. Tippen Sie in der Tastenleiste auf den Ordner, den Sie synchronisieren möchten.



3. Tippen Sie auf das Hamburgersymbol oben links.

4. Tippen Sie auf das **Synchronisierungssymbol** unten links.





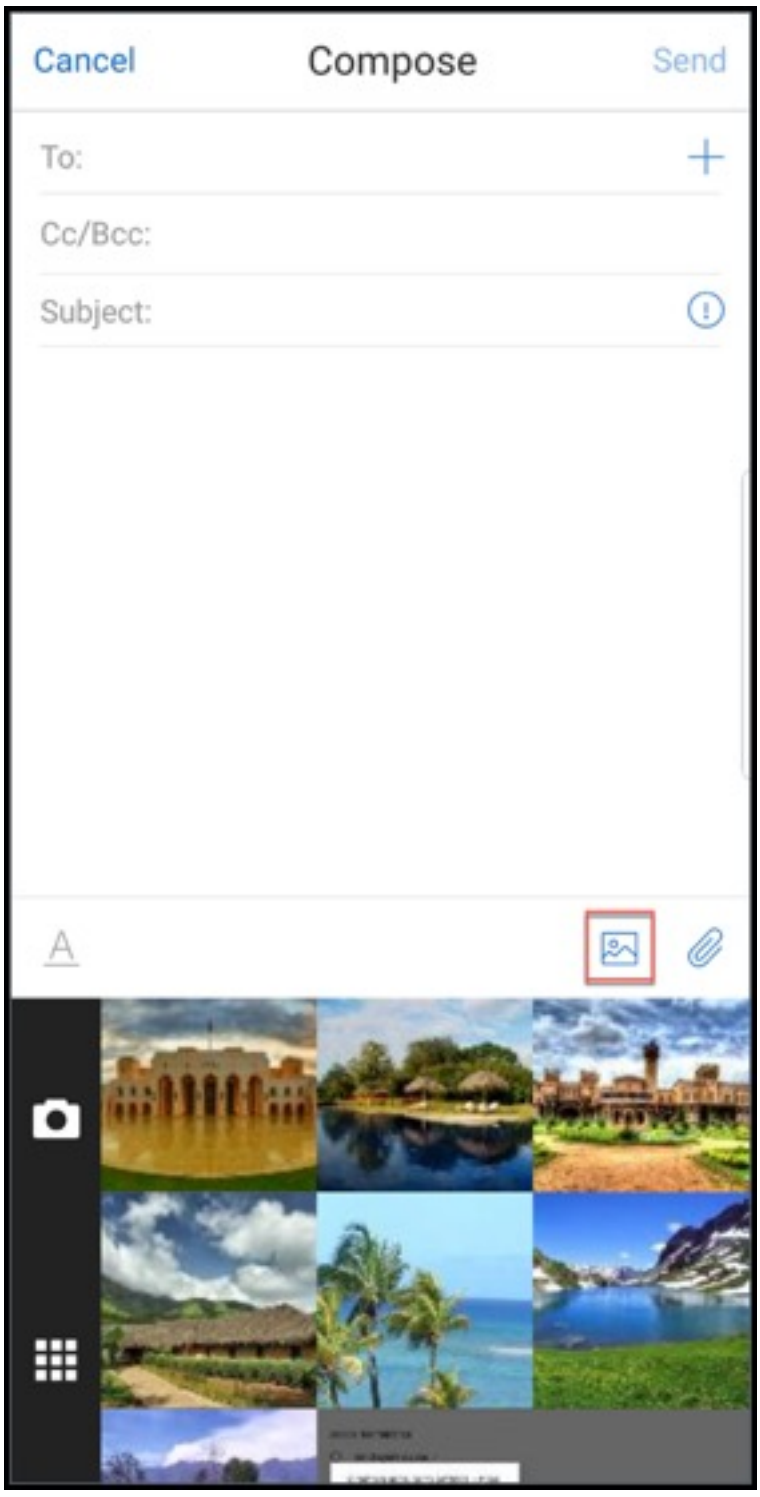
5. Der Ordner wird synchronisiert und der Inhalt aktualisiert. Der Zeitstempel wird neben dem **Synchronisierungssymbol** angezeigt.

Verbesserungen beim Anhängen von Fotos

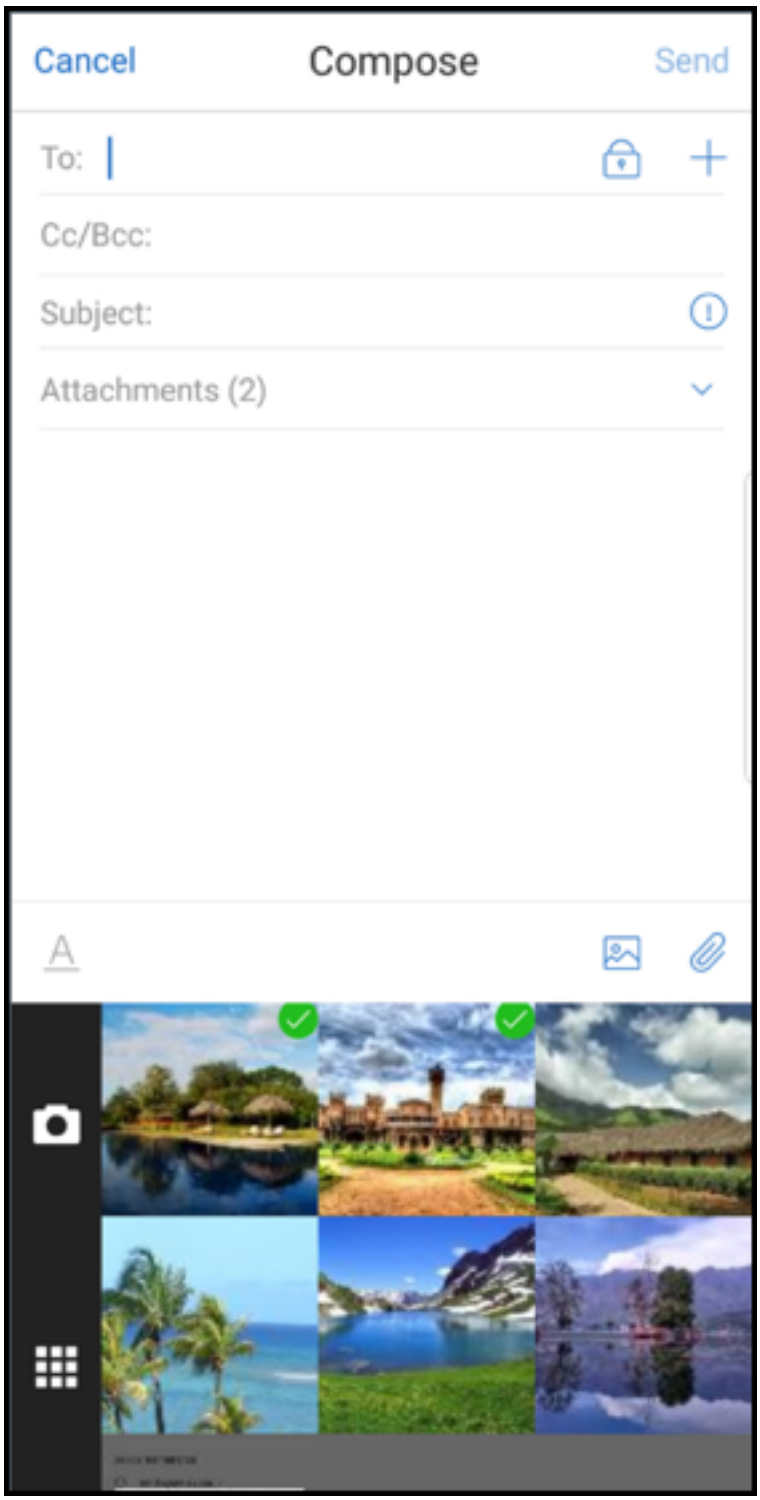
In Secure Mail für Android und iOS können Sie Fotos über das neue **Galerie**-Symbol mühelos anhängen.

Anhängen von Fotos an E-Mail

1. Öffnen Sie Secure Mail.
2. Tippen Sie auf **Erstellen**, um eine neue E-Mail zu erstellen, oder auf die unverankerte Schaltfläche **Antworten**, um auf eine E-Mail zu antworten.
3. Tippen Sie auf das **Galerie**-Symbol neben dem Symbol **Anlagen** unten rechts.



4. Ihre Galerie und die Symbole **Kamera** sowie **Aktuell** werden unten angezeigt.
5. Wählen Sie in der Galerie die gewünschten Bilder aus oder tippen Sie auf das **Kamera**-Symbol, um ein Bild aufzunehmen.

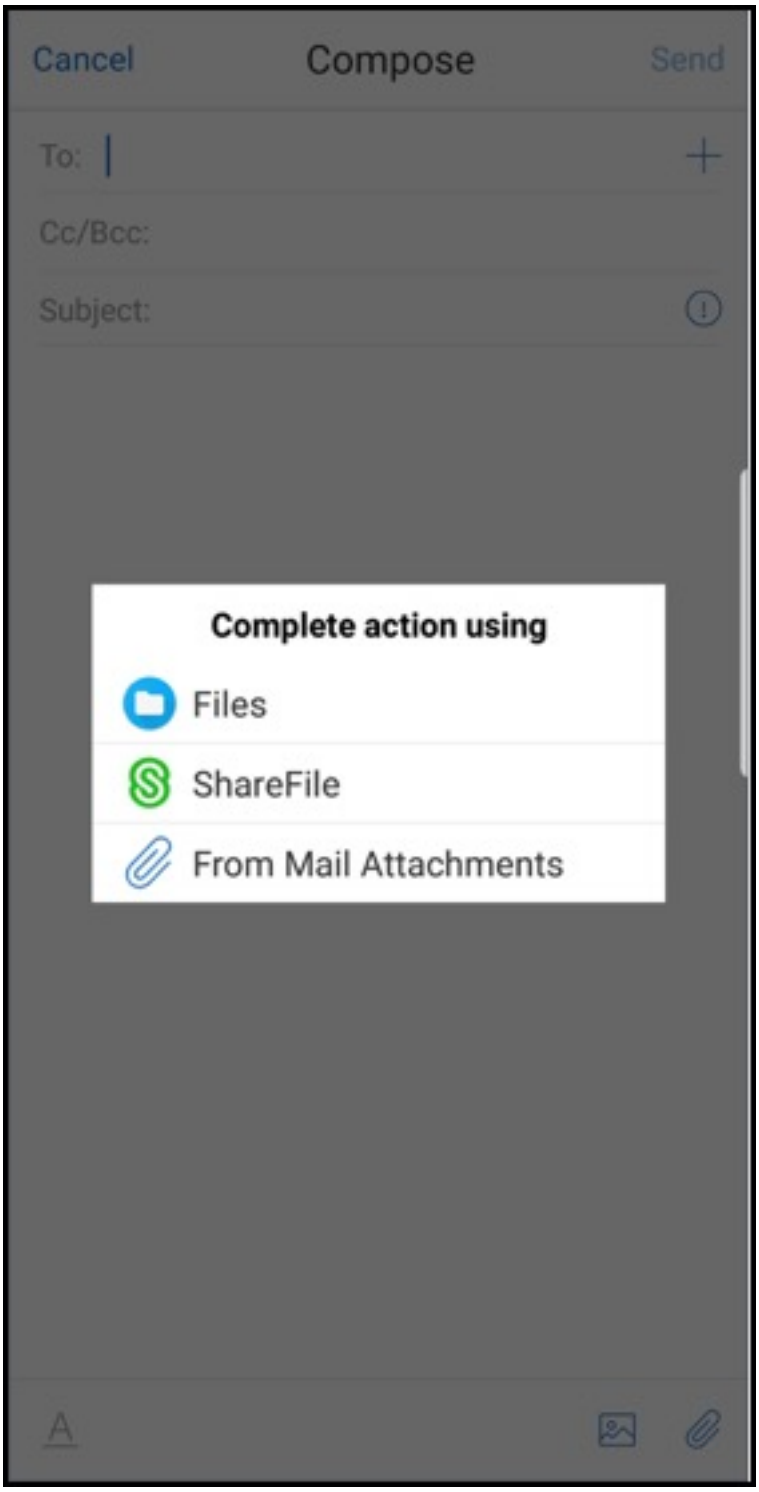


Hinweis:

Wenn Sie auf das Symbol **Anlagen** tippen, werden die folgenden Optionen angezeigt:

- Dateien

- ShareFile (jetzt Citrix Files)
- E-Mail-Anlagen



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.

Unterstützung für 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).

MDX-Richtlinie "Zulässige Secure Web-Domänen"für Secure Mail

In Secure Mail müssen einige externe URLs in einem nativen Browser anstelle von Secure Web geöffnet werden. Daher werden standardmäßig alle URLs in einem nativen Browser geöffnet. Sie können jedoch eine Liste der URLs erstellen, die in Secure Web geöffnet werden sollen. Konfigurieren Sie hierfür in der Citrix Endpoint Management-Konsole die MDX- Richtlinie "Zulässige Secure Web-Domänen".

Nach Bereitstellung der Richtlinie wird eine kommagetrennte Liste mit URL-Hostdomänen mit dem Hostnamenteil aller URLs abgeglichen, die die Anwendung normalerweise an einen externen Handler senden würde. In der Regel konfigurieren Sie diese Richtlinie als eine Liste von internen Domänen, die von Secure Web behandelt werden sollen.

Wenn Sie die Richtlinie leer lassen (Standardeinstellung), wird der gesamte Internetdatenverkehr an Secure Web geleitet, bis Sie die URLs aus der Filterung ausschließen oder umleiten. Zum Umleiten der URLs konfigurieren Sie die MDX-Richtlinie "Vom Filtern ausgeschlossene URL-Domänen". Diese Richtlinie gibt die URLs an, die im nativen Browser geöffnet werden müssen. Dieser Richtlinie hat Priorität vor der Secure Web-Domänenrichtlinie.

Sie können diese MDX-Richtlinien für Android und iOS konfigurieren.

Beispielkonfiguration der Secure Web-Domänenrichtlinie

Die folgenden Verfahren zeigen, wie Sie Benutzer mit Secure Mail für Android auffordern, URLs im nativen Chrome-Browser oder Secure Web zu öffnen. Für iOS zeigen die Schritte, dass normalerweise in Safari geöffnete URLs automatisch in Secure Web geöffnet werden.

Secure Mail für Android

1. Geben Sie in der App-Interaktionsrichtlinie für "Ausnahmeliste für eingeschränktes Öffnen" *{package=com.android.chrome}*ein.
2. Fügen Sie in der Richtlinie "App-Interaktion (ausgehende URL)"unter **Zulässige Secure Web-Domänen** das DNS-Suffix der internen Website hinzu.

Verwenden Sie für andere Browser von Drittanbietern das folgende Format:

```
{ package=<packageID of the browser> }
```

Secure Mail für iOS

1. Fügen Sie in der Richtlinie "App-Interaktion (ausgehende URL)"unter **Zulässige URLs** den Eintrag +^*safari* hinzu:
2. Fügen Sie unter **App-URL-Schemas** den Eintrag *safari:* hinzu.
3. Fügen Sie unter **Zulässige Secure Web-Domänen** das DNS-Suffix der internen Website hinzu.

Secure Mail-Integration in Slack

November 17, 2021

Citrix Secure Mail and its integration with Slack is not created by, affiliated with, or supported by Slack Technologies, Inc.

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

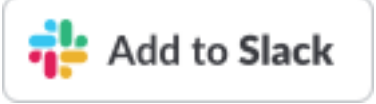
Wenn Sie das Feature aktivieren, haben Sie folgende Möglichkeiten:

- 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**.

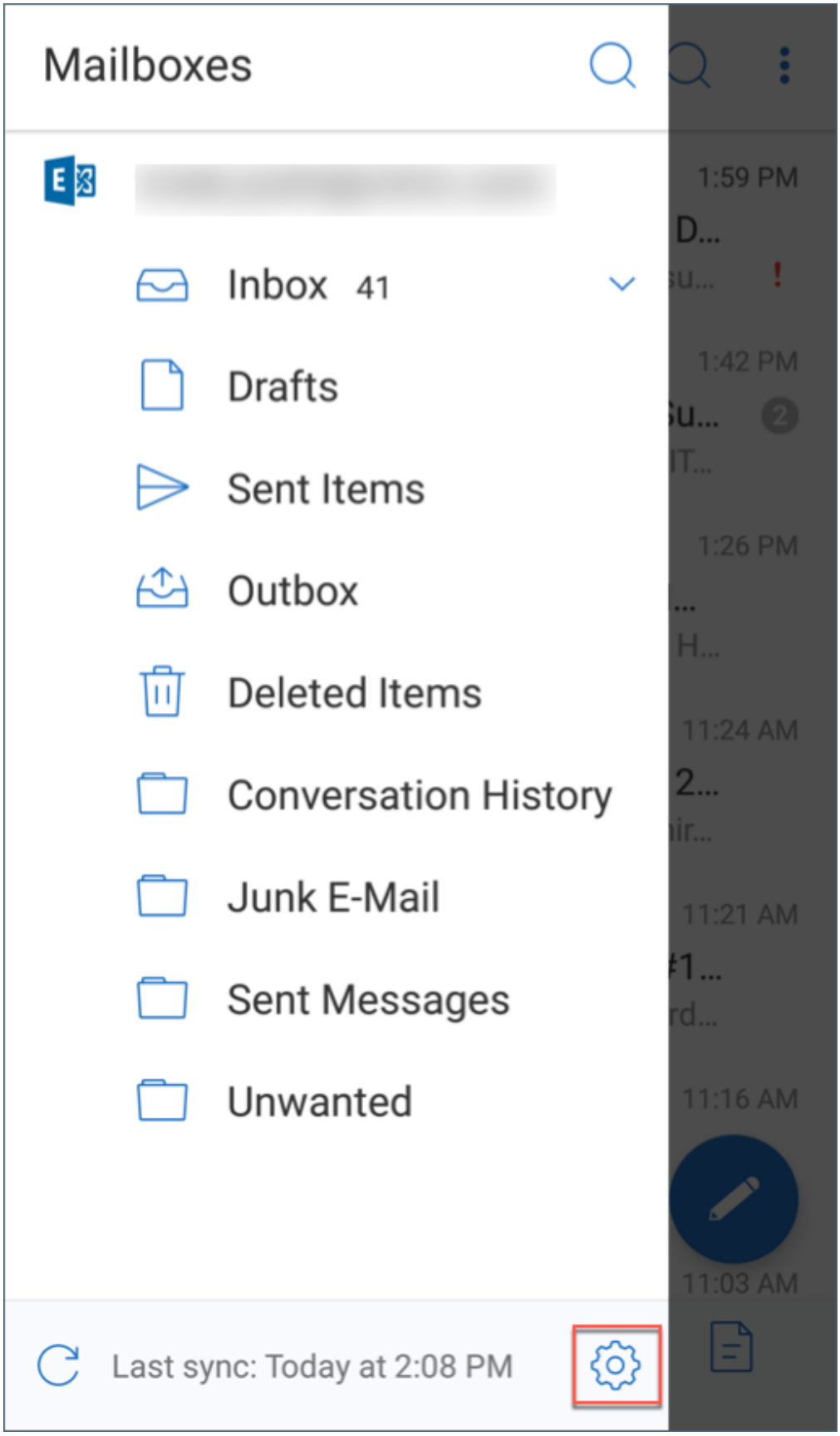
  - Vergewissern Sie sich, dass die Richtlinie **Slack aktivieren** auf **Ein** eingestellt ist. Richtliniendetails finden Sie unter:

    * Aktivieren der Slack-Richtlinie für iOS
    * Aktivieren der Slack-Richtlinie für Android

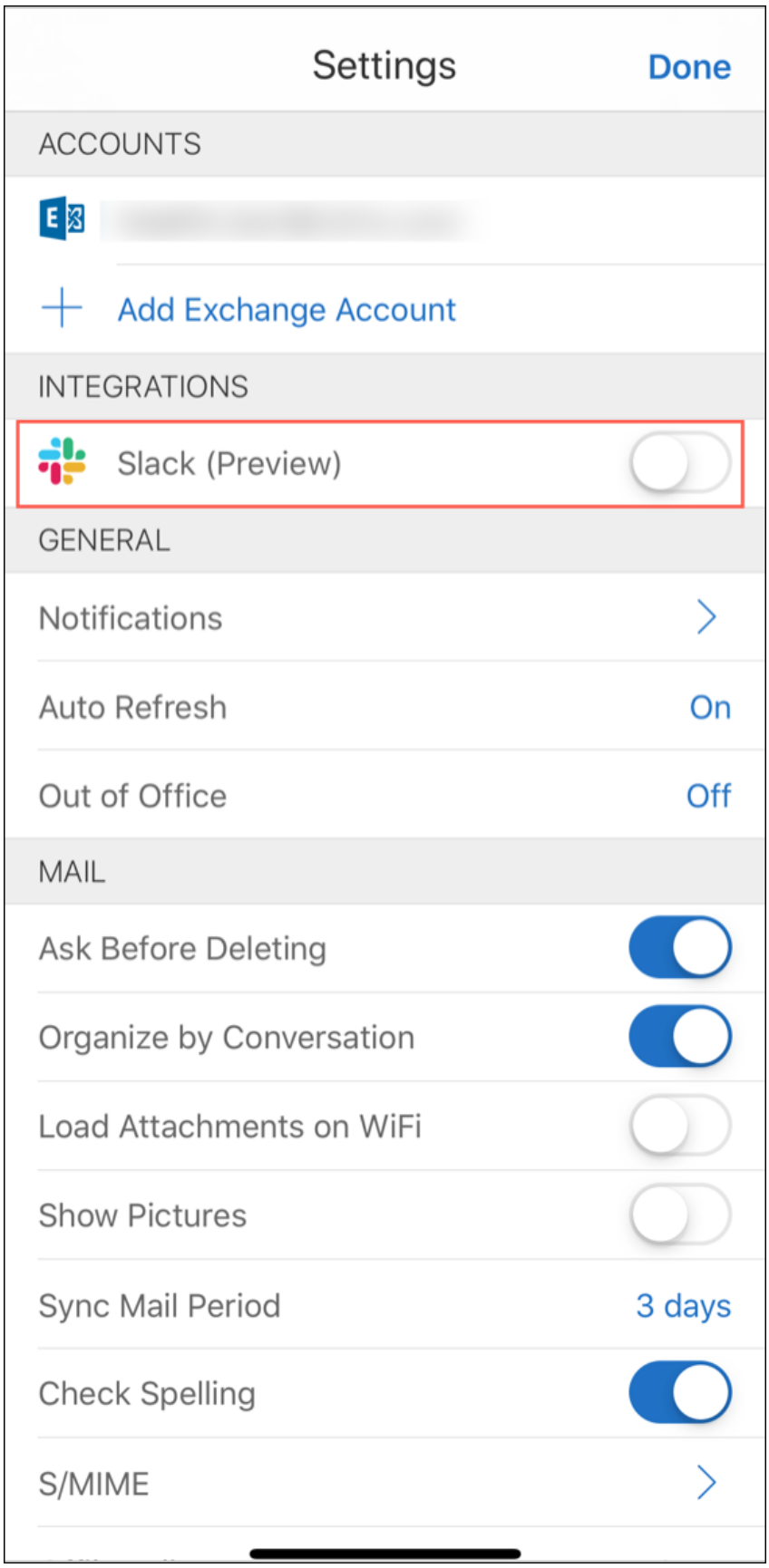
- Benutzer: Bevor Sie fortfahren, stellen Sie sicher, dass Sie ein Slack-Konto haben und die Slack-App auf Ihrem Gerät installiert ist.

Aktivieren dieses Features auf Ihrem Gerät

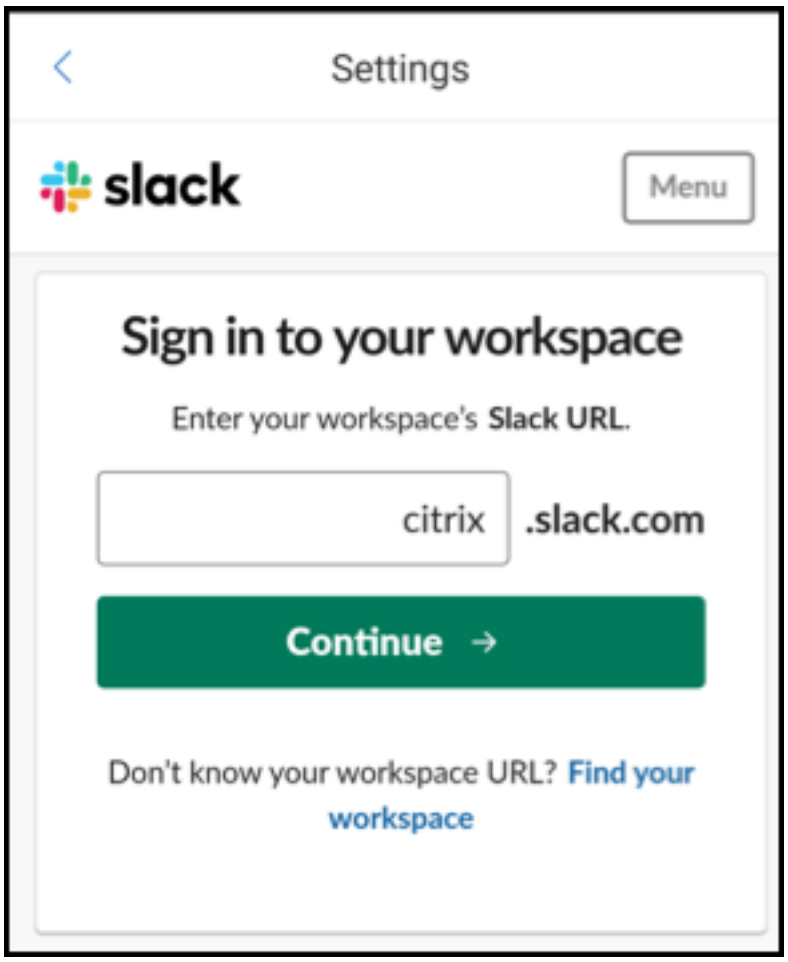
1. Öffnen Sie Secure Mail und tippen Sie auf das Hamburgersymbol.
2. Tippen Sie im Bildschirm **Postfächer** auf das Einstellungssymbol unten rechts.



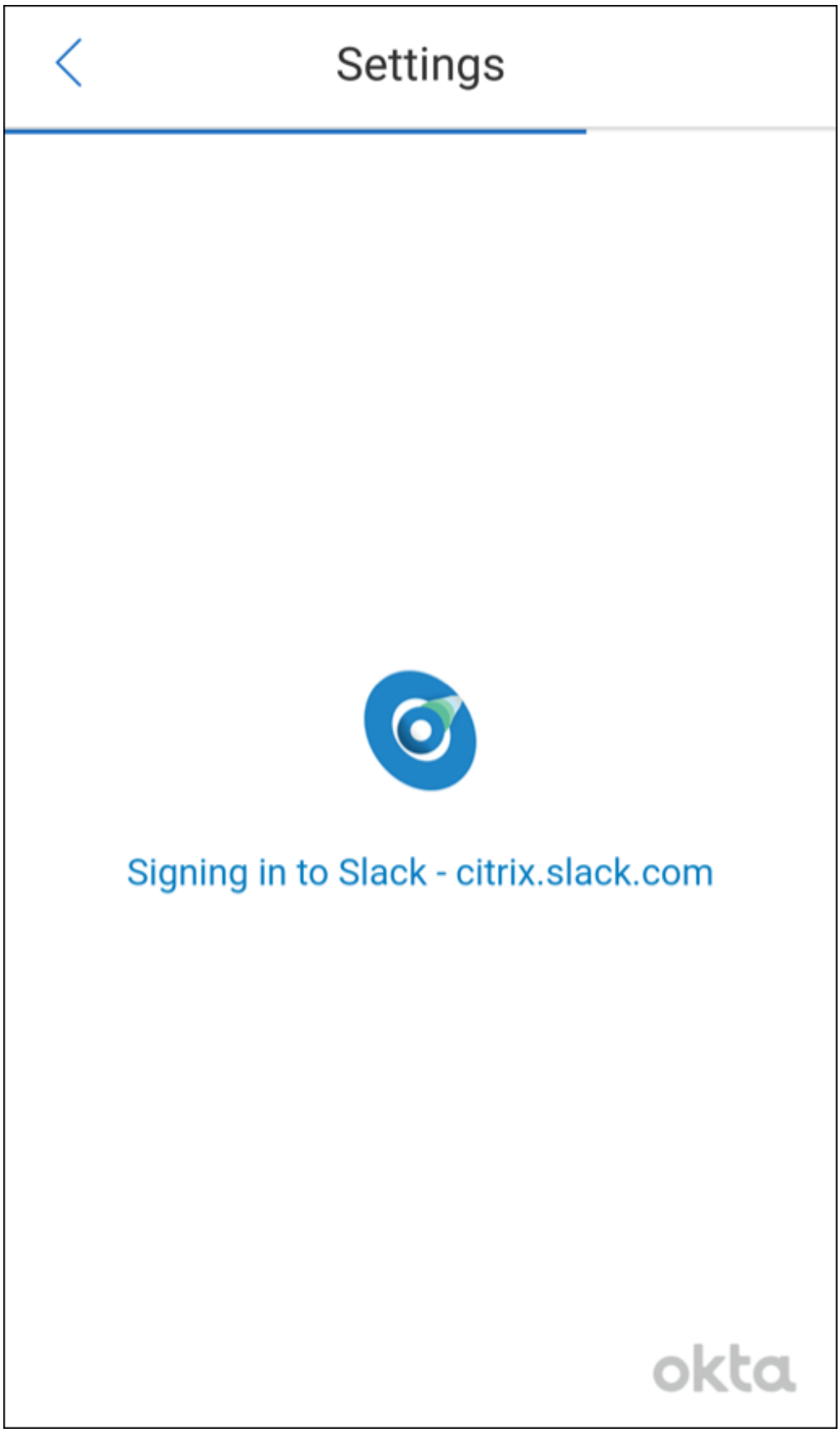
3. Tippen Sie auf dem Bildschirm **Einstellungen** auf **Slack**. Die Option wird unter **Integrationen** aufgeführt.



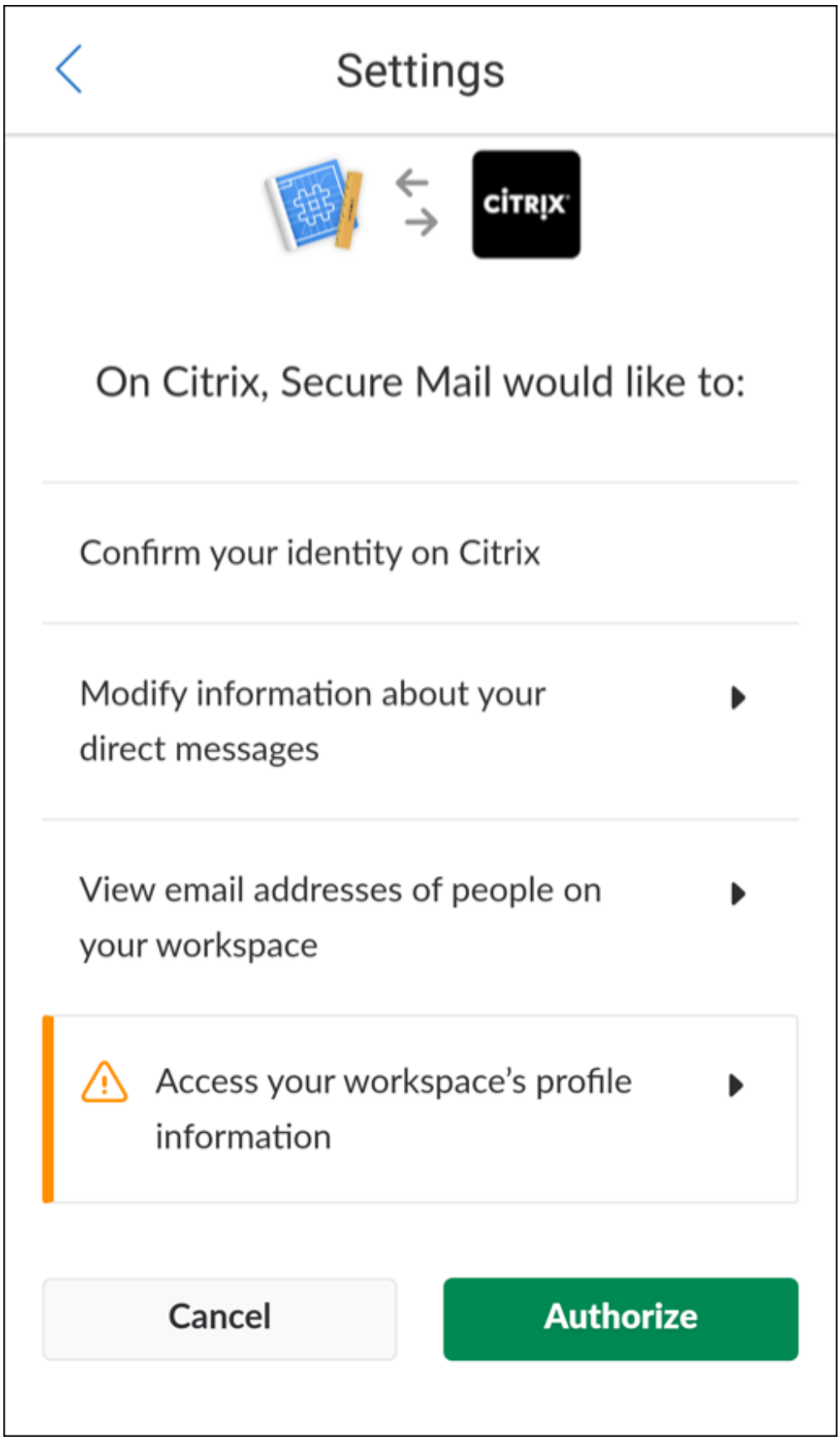
4. Geben Sie Ihre Workspace-Slack-URL an und tippen Sie auf **Weiter**.



5. Geben Sie Ihre Anmeldeinformationen ein und tippen Sie auf **Anmelden**.



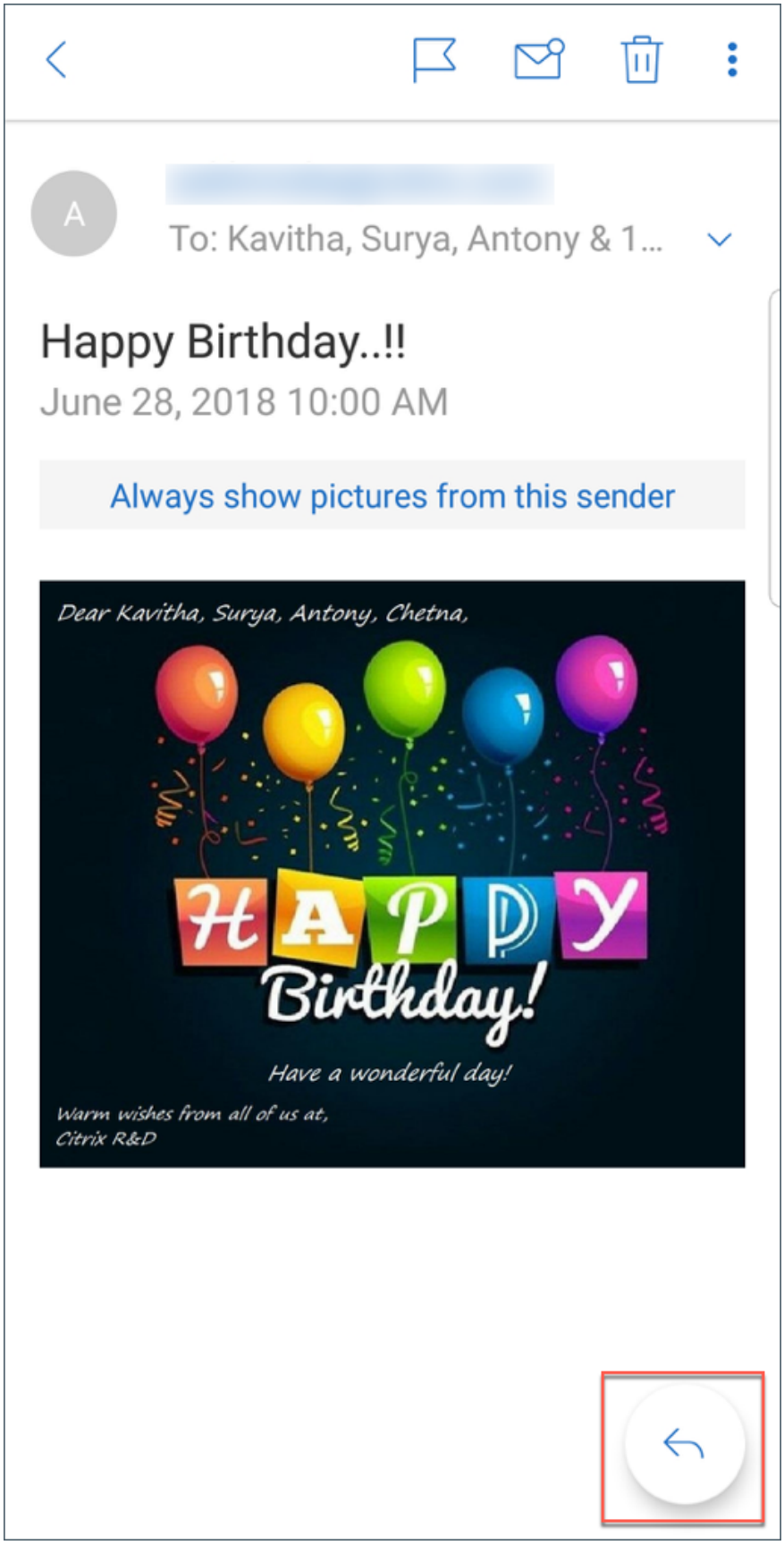
6. Wenn Sie aufgefordert werden, den Zugriff auf Informationen durch Secure Mail zuzulassen, tippen Sie auf **Autorisieren**.



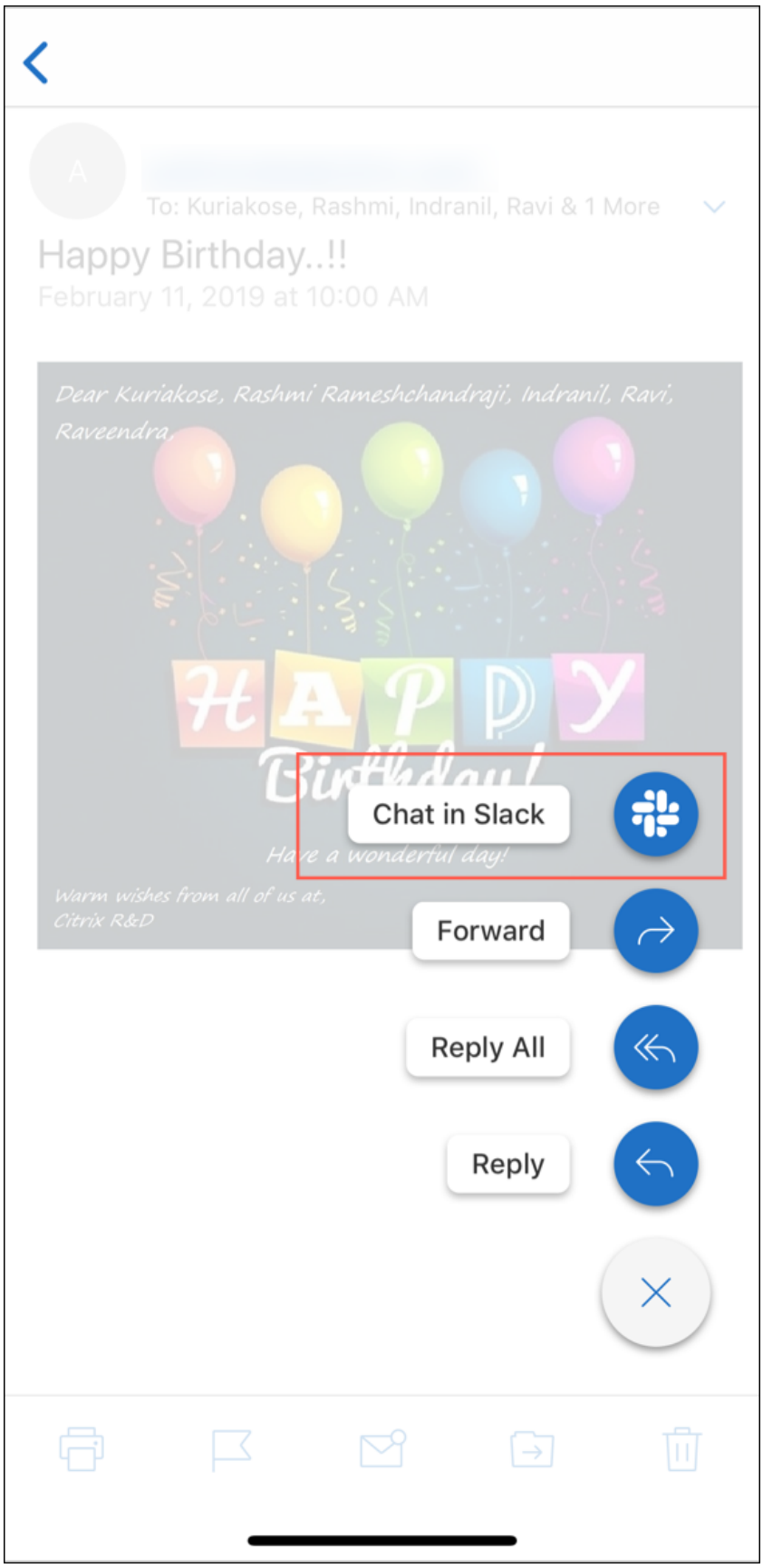
Sie sind jetzt mit Slack verbunden.

Verwenden des Features

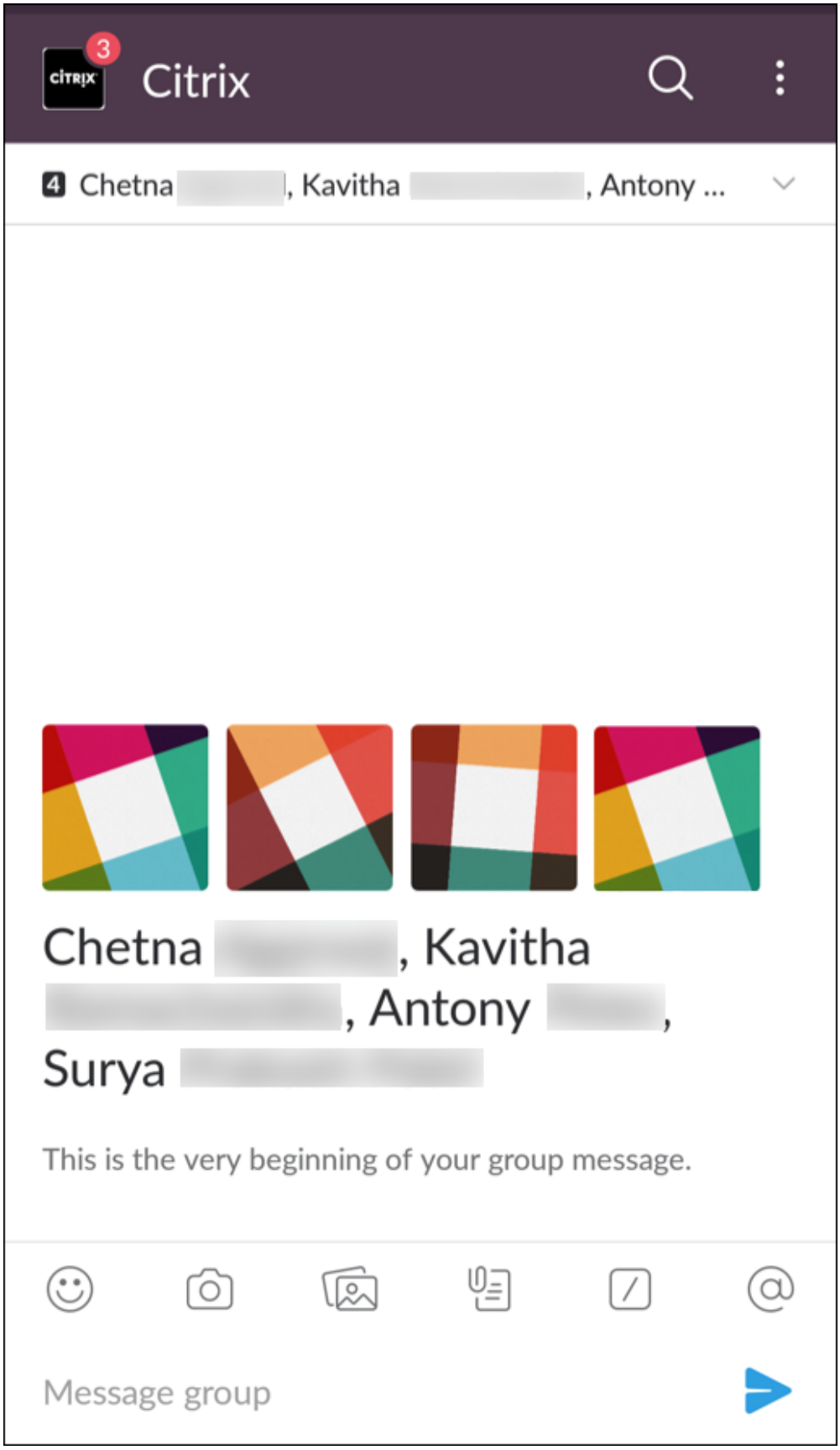
1. Öffnen Sie eine E-Mail-Unterhaltung in Secure Mail und tippen Sie auf die unverankerte Aktionsschaltfläche.



2. Tippen Sie **Chat in Slack**.



3. Die Unterhaltung wechselt mit den Empfängern der E-Mail zu Slack.



Beachten Sie 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 von Secure Mail die ersten acht Empfänger in der E-Mail-Unterhaltung ausgewählt.

Benachrichtigungen und Synchronisierung

December 7, 2021

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 Kalendereereignisse, 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 exportiert und mit den Telefonkontakten synchronisiert werden. Die Kontakte können selbst dann exportiert und synchronisiert werden, wenn Benutzer Hotmail oder Exchange 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**.

Einschränkung:

Wenn Sie **Mit lokalen Kontakten synchronisieren** aktivieren, wird nur der Standardordner für Kontakte synchronisiert. Eventuell vorhandene Unterordner sind nicht in den synchronisierten Kontakten enthalten.

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.
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 für Secure Mail

February 28, 2024

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 Remote-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

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

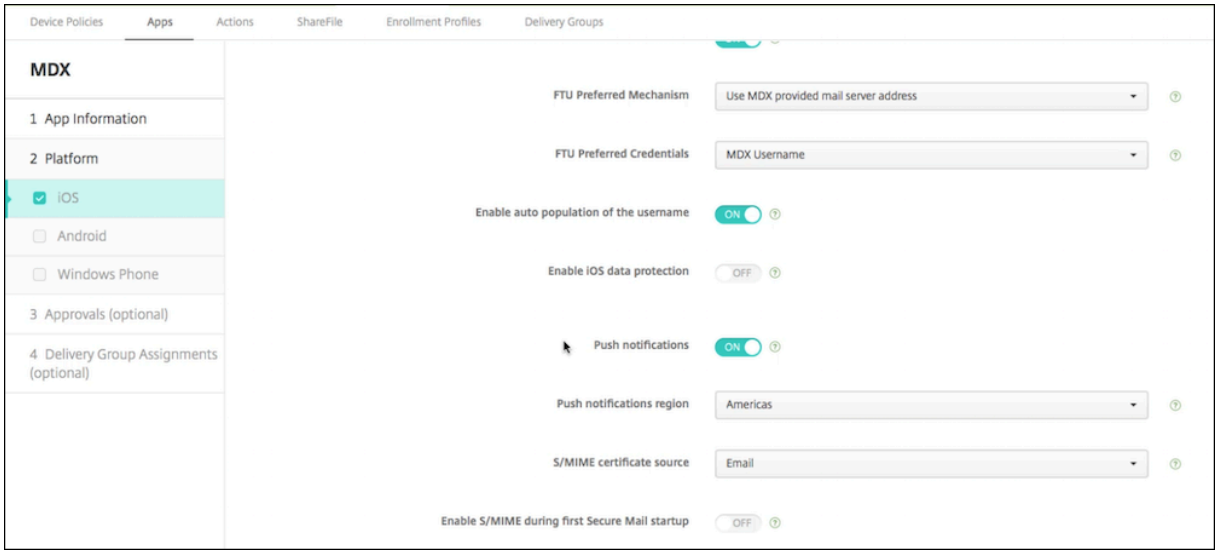
Wenn die Citrix Gateway-Konfiguration Secure Ticket Authority (STA) umfasst und Split-Tunneling deaktiviert ist, muss Citrix Gateway Datenverkehr (wenn von Secure Mail getunnelt) zu den folgenden

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. Beispiel:

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

```
1 <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

Obwohl 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. Weitere Informationen zur Integration von Citrix Endpoint Management mit Citrix Gateway finden Sie im Abschnitt Integration in Citrix ADC und Citrix Gateway.

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.

Häufig gestellte Fragen zu Secure Mail-Pushbenachrichtigungen

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 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.

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 im Hintergrund ist.

  > **Hinweis:**
  >
  > Diese Situation tritt nur auf, wenn Pushbenachrichtigungen mit Rich-Media-Inhalt deaktiviert sind. Weitere Informationen finden Sie unter Pushbenachrichtigungen mit Rich-Media-Inhalt für Secure Mail für iOS.

- 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.

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 in Secure Mail die Datensynchronisierung nicht durchgeführt werden. Das Ergebnis ist, dass Benachrichtigungen möglicherweise 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 folgenden Aktionen verstreichen:

- Eine E-Mail geht im Posteingang eines Benutzers unter Exchange ein.
- Secure Mail synchronisiert die E-Mail und generiert eine Sperrbildschirmbenachrichtigungen.

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 wichtiger Unterschied, der Verwirrung auslösen kann, besteht darin, dass Secure Mail neue E-Mails nicht immer in Echtzeit auf dem Sperrbildschirm anzeigt. Hierin unterscheidet es sich von Gmail, Microsoft Outlook und anderen Apps. Die primäre Ursache für diesen Unterschied ist der Aspekt der

Sicherheit. Zur Angleichung der Funktionsweise an die anderer Apps benötigt der Citrix Listener-Dienst die Anmeldeinformationen des Benutzers, um sich bei Exchange zu authentifizieren. Die Anmeldeinformationen sind erforderlich, um den E-Mail-Inhalt abzurufen. Die Anmeldeinformationen sind auch erforderlich, um E-Mail-Inhalt über den Citrix Listener-Dienst und an den Apple APNs-Dienst 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. Unabhängig von diesem Setup kann Outlook Sperrbildschirmbenachrichtigungen basierend auf Daten anzeigen, die Microsoft in den APNs-Benachrichtigungen übermittelt. Dies rührt daher, dass 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 bei Gmail. Bei Gmail generiert iOS einfach auf der Basis der Daten eine Sperrbildschirmbenachrichtigung. 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 der Benutzer anvertrauen. Diese Vertrauensstellung ermöglicht Microsoft den Zugriff auf Postfächer, was ein Sicherheitsrisiko darstellt.

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.

Pushbenachrichtigungen mit Rich-Media-Inhalt für Secure Mail für iOS

December 7, 2021

Secure Mail für iOS unterstützt Pushbenachrichtigungen mit Rich-Media-Inhalt. Benachrichtigungen mit Rich-Media-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-Media-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

- Über eine Integration von Endpoint Management in Microsoft InTune/EMS verwaltete Apps
- Mit abgeleiteten Anmeldeinformationen registrierte Geräte

Funktionsweise von Pushbenachrichtigungen in Secure Mail unter iOS

Secure Mail empfängt Pushbenachrichtigungen für die folgenden Posteingangsaktivitäten:

- **Neue E-Mails, Besprechungsanfragen, Besprechungsabsagen, Besprechungsupdates**: Wenn APNs Remotebenachrichtigungen an Secure Mail unter iOS sendet, aktualisiert Secure Mail alle Ordner, für die die automatische Aktualisierung aktiviert ist.

  > **Hinweis:**
  >
  > Standardmäßig ist die automatische Aktualisierung für die Ordner "Posteingang", "Kalender"und "Kontakte"aktiviert. Die Benutzer können unter **Secure Mail** > **Einstellungen** > **Automatische Aktualisierung** beliebige andere E-Mail-Ordner für die automatische Aktualisierung auswählen.

- Das Secure Mail-Symbol zeigt nur die Anzahl der ungelesenen und neuen Nachrichten im Exchange-Posteingangsordner an. Das Symbol wird von Secure Mail aktualisiert, wenn Benutzer E-Mails auf einem Desktop oder Laptop gelesen haben.
- 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.

Funktionsweise von Pushbenachrichtigungen ohne Unterstützung für Rich-Media-Inhalt

Bei Konfigurationen, die Pushbenachrichtigungen mit Rich-Media-Inhalt unter iOS nicht unterstützen, zeigt Secure Mail die Anzahl der ungelesenen E-Mails im Posteingang für den Synchronisierungszeitraum 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.

Häufig gestellte Fragen zu Secure Mail-iOS-Pushbenachrichtigungen

Wann übermittelt iOS Benachrichtigungen an Secure Mail

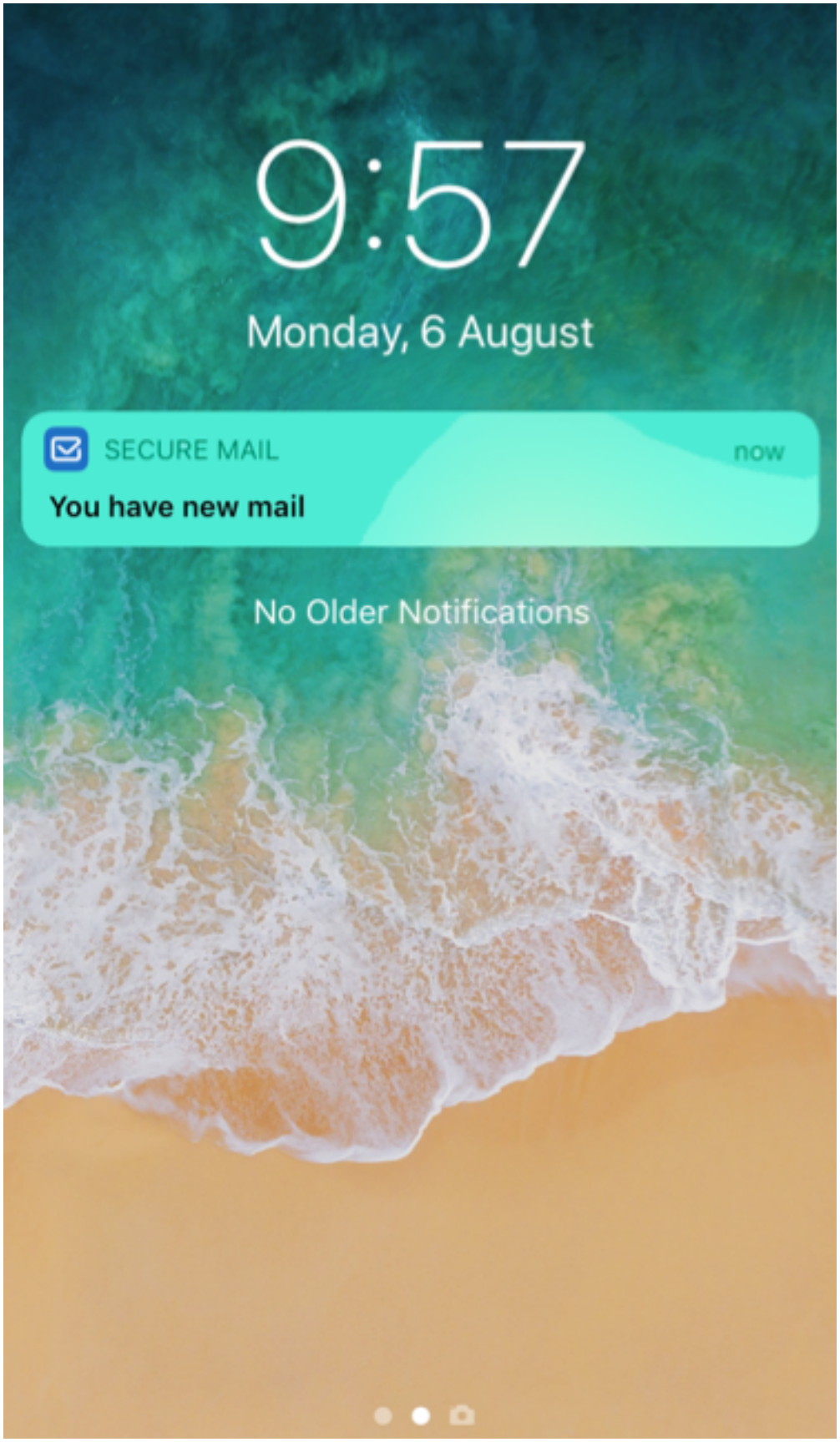
Ist das Feature Pushbenachrichtigungen mit Rich-Media-Inhalt aktiviert, sendet iOS Remotebenachrichtigungen an Secure Mail. Die Benachrichtigungen werden auch dann gesendet, wenn die App nicht im Hintergrund läuft oder im Energiesparmodus ist.

> **Hinweis:**
>
> Sind Pushbenachrichtigungen mit Rich-Media-Inhalt deaktiviert , werden Benachrichtigungen ggf. nicht an Secure Mail übermittelt, wenn dieses nicht aktiv ist. Dies kann beispielsweise aus folgenden Gründen vorkommen:

- Das Gerät ist im Energiesparmodus und Secure Mail im Hintergrund. Dies ist der häufigste Grund für eine Nichtzustellung von Benachrichtigungen.
- Die **Hintergrundaktualisierung** für Secure Mail ist **deaktiviert** und Secure Mail wird im Hintergrund ausgeführt: Diese Einstellung wird von den Benutzern gesteuert.
- Das Gerät hat eine schlechte Netzwerkverbindung: Dies hängt vom iOS-Gerät ab.

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

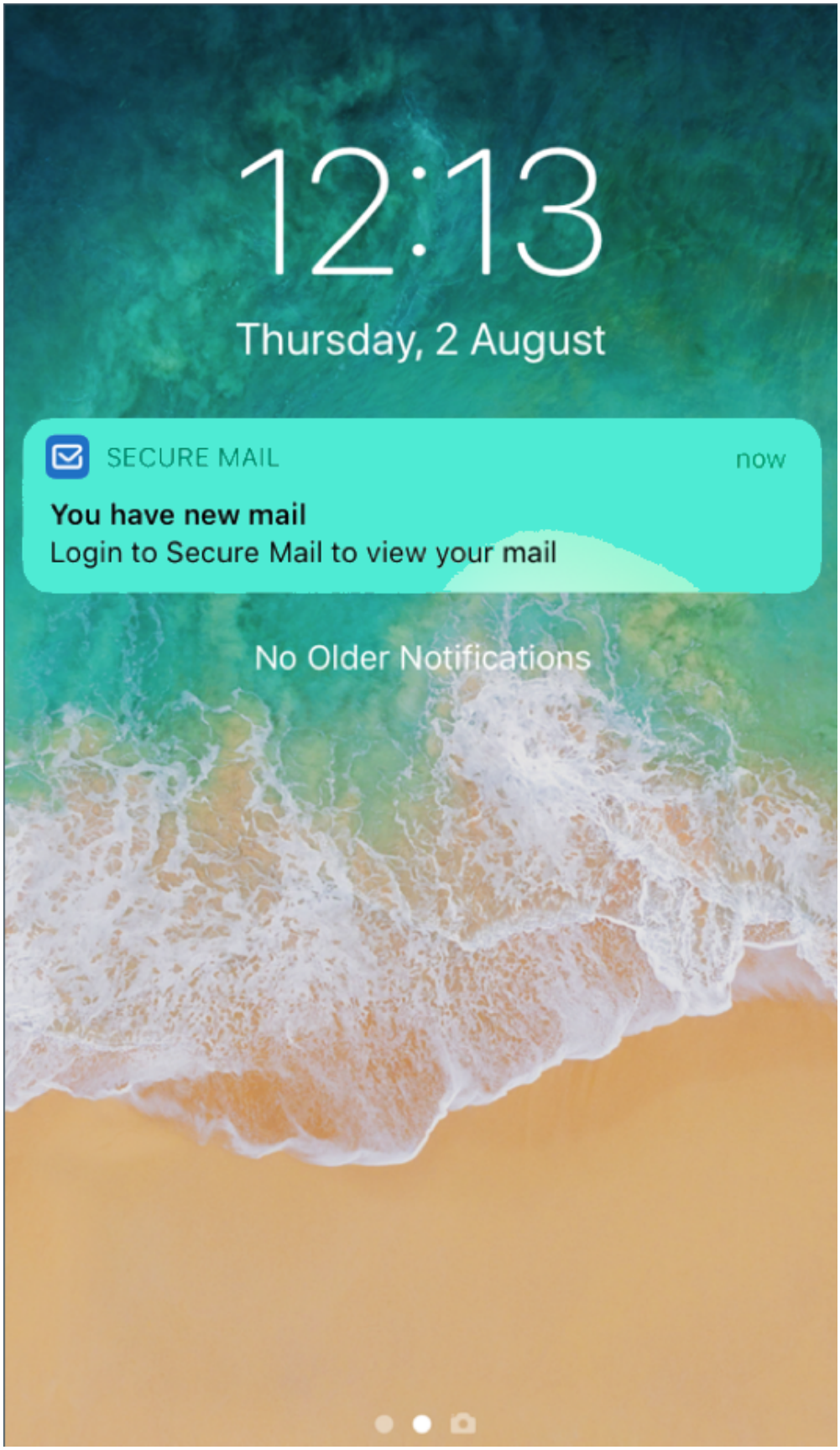
Die Benachrichtigung “Sie haben neue E-Mails”wird auf iOS-Geräten angezeigt, wenn Secure Mail von den Exchange-Webdiensten (EWS) innerhalb der festgelegten Zeit keine Antwort erhält. Das Abrufen der Nachrichtendetails dauert 30 Sekunden.



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

Abgesehen von der verzögerten EWS-Antwort zeigt Secure Mail 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 nicht in Secure Mail aktualisiert wurden. Die folgende Abbildung zeigt, wie die Benachrichtigung in diesem Szenario angezeigt wird.



- Wenn Secure Mail eine unerwartete Antwort von 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 erreichbar 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 Ihrer Organisation herstellen. Wenden Sie sich an den 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. Wenden Sie sich an den 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. Wenden Sie sich an den 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 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.

Interaktivität zwischen Secure Mail und anderen mobilen Produktivitätsapps und Citrix Files

July 17, 2023

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.

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

Testen und Problembehandlung von Secure Mail

May 5, 2023

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 folgt 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. 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 Kommunikation 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.

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.