



Secure Mail

Contents

Secure Mail 개요	2
Secure Mail 의 새로운 기능	3
알려진 문제와 수정된 문제	74
Secure Mail 배포	77
Secure Mail 구성	78
Microsoft Office 365 를 통한 최신 인증	79
iOS 및 Android 용 온-프레미스 Exchange 를 사용한 하이브리드 최신 인증	82
Secure Mail 에 대한 백그라운드 서비스	85
Exchange Server 또는 IBM Notes Traveler 서버 통합	89
Secure Mail 에 대한 S/MIME 구성	93
Secure Mail 에 대한 SSO	139
보안 고려 사항	141
iOS 기능	155
Android 기능	175
Secure Mail 의 iOS 및 Android 기능	211
Secure Mail 과 Slack 통합	267
알림 및 동기화	281
Secure Mail 을 위한 푸시 알림	283
iOS 용 Secure Mail 에 대한 다양한 방식의 푸시 알림	290
Secure Mail 과 다른 모바일 생산성 앱 및 Citrix Files 의 상호 작용	296
Secure Mail 테스트 및 문제 해결	297

Secure Mail 개요

November 1, 2023

Citrix Secure Mail 을 통해 사용자는 휴대폰 및 태블릿에서 전자 메일, 일정 및 연락처를 관리할 수 있습니다. Microsoft Outlook 또는 IBM Notes 계정으로부터 연속성이 유지되도록 Secure Mail 은 Microsoft Exchange Server 및 IBM Notes Traveler 서버와 동기화됩니다.

Citrix 앱 제품군의 하나인 Secure Mail 은 Citrix Secure Hub 와의 SSO(Single Sign-On) 호환성을 갖습니다. 사용자는 Secure Hub 에 로그인한 후 사용자 이름 및 암호를 다시 입력할 필요 없이 Secure Mail 로 매끄럽게 이동할 수 있습니다. 사용자의 장치가 Secure Hub 에 등록될 때 해당 장치로 Secure Mail 이 자동으로 푸시되도록 구성하거나 사용자가 Store 에서 이 앱을 추가할 수 있습니다.

참고:

Exchange Server 2010 에 대한 지원은 2020 년 10 월 13 일에 종료되었습니다.

Secure Mail 은 다음과 호환됩니다.

- Exchange Server 2019 누적 업데이트 13
- Exchange Server 2019 누적 업데이트 12
- Exchange Server 2019 누적 업데이트 11
- Exchange Server 2019 누적 업데이트 10
- Exchange Server 2019 누적 업데이트 9
- Exchange Server 2019 누적 업데이트 8
- Exchange Server 2019 누적 업데이트 7
- Exchange Server 2019 누적 업데이트 6
- Exchange Server 2016 누적 업데이트 23
- Exchange Server 2016 누적 업데이트 22
- Exchange Server 2016 누적 업데이트 21
- Exchange Server 2016 누적 업데이트 20
- Exchange Server 2016 누적 업데이트 19
- Exchange Server 2016 누적 업데이트 18
- Exchange Server 2016 누적 업데이트 17
- Exchange Server 2013 누적 업데이트 23
- Exchange Server 2013 누적 업데이트 22
- Exchange Server 2013 누적 업데이트 21
- HCL Domino 버전 12.0.2 FP2
- HCL Traveler 버전 12.0.2.1 빌드 202302010413_30
- HCL Domino 11(이전의 Lotus Notes)
- HCL Domino 10.0.1(이전의 Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197(이전의 Lotus Notes)

- HCL Domino 10.0.1.0 build 201811191126_20(이전의 Lotus Notes)
- HCL Domino 9.0.1.21(이전의 Lotus Notes)
- Microsoft Office 365(Exchange Online)

먼저 Secure Mail 및 기타 Endpoint Management 구성 요소를 [Citrix Endpoint Management 다운로드](#)에서 다운로드합니다.

Secure Mail 및 기타 모바일 앱 시스템 요구 사항은 [시스템 요구 사항](#)을 참조하십시오.

앱이 백그라운드에서 실행되고 있거나 닫힌 경우 iOS 및 Android 용 Secure Mail 의 알림에 대한 내용은 [Secure Mail 을 위한 푸시 알림](#)을 참조하십시오.

Secure Mail 에서 지원되는 iOS 기능은 [Secure Mail 의 iOS 기능](#)을 참조하십시오.

Secure Mail 에서 지원되는 Android 기능은 [Secure Mail 의 Android 기능](#)을 참조하십시오.

Secure Mail 에서 지원되는 iOS 및 Android 기능은 [Secure Mail 의 iOS 및 Android 기능](#)을 참조하십시오.

사용자 도움말 설명서는 Citrix User Help Center 의 [Citrix Secure Mail](#) 페이지를 참조하십시오.

Secure Mail 의 새로운 기능

February 27, 2024

다음 섹션에서는 현재 및 이전 Secure Mail 릴리스의 새로운 기능에 대해 설명합니다.

사용자 도움말 설명서는 Citrix User Help Center 의 [Citrix Secure Mail](#) 페이지를 참조하십시오.

참고:

Secure Mail 은 2023 년 9 월 기준으로 Android 7.x 및 iOS 12.x 를 지원하지 않습니다.

현재 버전의 새로운 기능

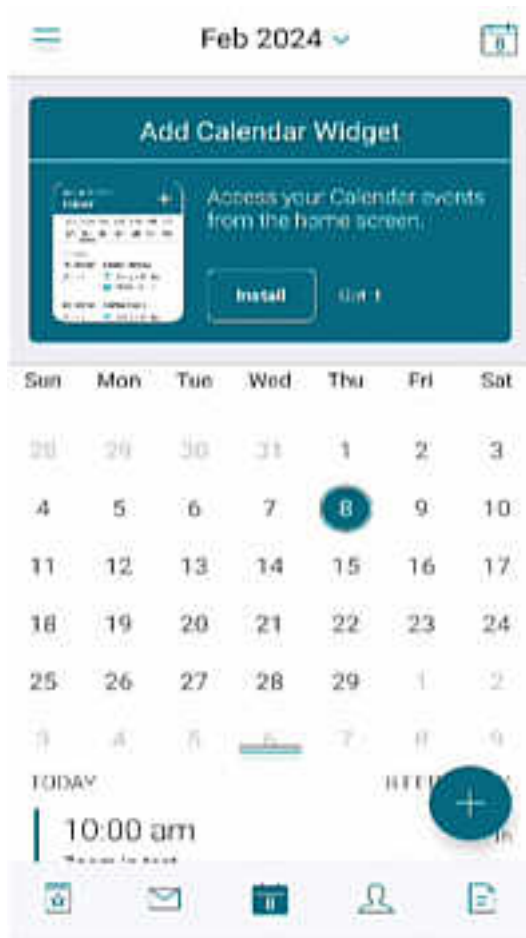
iOS 용 Secure Mail 24.2.0

이 릴리스에서는 전반적인 성능 및 안정성을 개선하는 영역을 다룹니다.

이전 버전의 새로운 기능

Android 용 Secure Mail 24.1.0

일정 이벤트 확대 기능 지원 릴리스 24.1.0 부터 Android 용 Secure Mail 은 일정 이벤트의 확대 기능을 지원합니다. 이 기능은 기본적으로 사용하도록 설정됩니다. 이제 확대 기능이 메시지와 일정 이벤트 모두에 적용됩니다. 개선된 확대 기능은 더 좋은 사용자 환경을 제공합니다.



iOS 용 Secure Mail 23.9.0

iOS 17 지원 이번 릴리스부터 Secure Mail 은 iOS 17 을 실행하는 장치에서 지원됩니다. Secure Mail 버전을 23.9.0 으로 업그레이드하면 iOS 17 로 업데이트된 장치를 지속적으로 지원할 수 있습니다.

HCL Domino 12 지원 이번 릴리스부터 Android 및 iOS 용 Secure Mail 에는 HCL Domino 버전 12.0.2 FP2 와 HCL Traveler 버전 12.0.2.1 빌드 202302010413_30 에 대한 지원이 포함됩니다.

참고:

HCL Domino 11 에서 HCL Domino 12 로 업그레이드하는 경우 Domino 서버의 **notes.ini** 파일에서 다음 사용자 에이전트를 업데이트해야 합니다. 이렇게 해야 임시 보관함 동기화 및 일정 첨부 파일과 같은 Secure Mail 의 모든 ActiveSync 16.1 기능이 계속해서 제대로 작동합니다. 자세한 내용은 [HCL Traveler Exchange ActiveSync 16.1](#) 지원을 위해 Citrix Secure Mail 클라이언트를 활성화하는 방법을 참조하십시오.

```
NTS_DEVICE_TYPE_USER_AGENT_APPLE=(^Apple-(iPhone|iPod|iPad|Touchdown))|(^Mozilla.(iPhone|iPod|iPad))|(^WorxMail.(iPhone|iPod|iPad))
```

Android 용 Secure Mail 23.8.2

워터마크 없이 첨부 파일 보기 Android 용 Secure Mail 버전 23.8.1 이하를 사용하는 경우 첨부 파일을 볼 때 워터마크가 표시됩니다. 워터마크 없이 첨부 파일을 보려면 Android 용 Secure Mail 버전 23.8.2 이상으로 업그레이드하십시오.

참고:

2023 년 10 월 31 일 이후에는 버전 23.8.1 로 업그레이드해도 첨부 파일의 워터마크 문제가 해결되지 않습니다. 따라서 버전 23.8.2 로 업데이트하는 것이 좋습니다.

Android 용 Secure Mail 23.8.1

워터마크 없이 첨부 파일 보기 Android 용 Secure Mail 버전 23.8.0 이하를 사용하는 경우 첨부 파일을 볼 때 워터마크가 표시될 수 있습니다. 워터마크 없이 첨부 파일을 보려면 Android 용 Secure Mail 버전 23.8.1 이상으로 업그레이드하십시오.

HCL Domino 12 지원 이번 릴리스부터 Android 및 iOS 용 Secure Mail 에는 HCL Domino 버전 12.0.2 FP2 와 HCL Traveler 버전 12.0.2.1 빌드 202302010413_30 에 대한 지원이 포함됩니다.

참고:

HCL Domino 11 에서 HCL Domino 12 로 업그레이드하는 경우 Domino 서버의 **notes.ini** 파일에서 다음 사용자 에이전트를 업데이트해야 합니다. 이렇게 해야 임시 보관함 동기화 및 일정 첨부 파일과 같은 Secure Mail 의 모든 ActiveSync 16.1 기능이 계속해서 제대로 작동합니다. 자세한 내용은 [HCL Traveler Exchange ActiveSync 16.1](#) 지원을 위해 Citrix Secure Mail 클라이언트를 활성화하는 방법을 참조하십시오.

```
NTS_DEVICE_TYPE_USER_AGENT_APPLE=(^Apple-(iPhone|iPod|iPad|Touchdown))|(^Mozilla.(iPhone|iPod|iPad))|(^WorxMail.(iPhone|iPod|iPad))
```

Android 용 Secure Mail 23.8.0

Android 14 에 대한 지원 이번 릴리스부터 Android 14 를 실행하는 장치에서 Secure Mail 이 지원됩니다. Secure Mail 버전을 23.8.0 으로 업그레이드하면 Android 14 로 업데이트된 장치를 계속 지원할 수 있습니다.

Android 용 Secure Mail 23.7.0

Microsoft Exchange 누적 업데이트 13 지원 23.7.0 릴리스부터 Secure Mail 은 Microsoft Exchange Server 2019 누적 업데이트 13 을 지원합니다.

온-프레미스 **Exchange** 를 사용한 하이브리드 최신 인증 지원 Secure Mail 은 이제 Exchange Server 2016 용 누적 업데이트 8 과 Exchange Server 2013 용 누적 업데이트 19 를 통해 하이브리드 최신 인증 (HMA) 을 지원합니다.

iOS 용 Secure Mail 23.7.0

온-프레미스 **Exchange** 를 사용한 하이브리드 최신 인증 지원 Secure Mail 은 이제 Exchange Server 2016 용 누적 업데이트 8 과 Exchange Server 2013 용 누적 업데이트 19 를 통해 하이브리드 최신 인증 (HMA) 을 지원합니다.

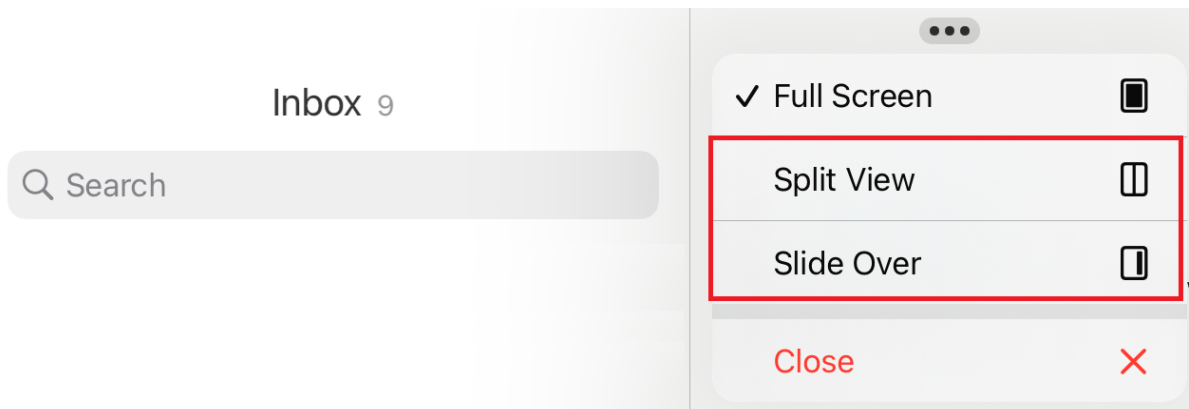
다크 모드 23.7.0 릴리스부터 Secure Mail 은 다크 모드를 지원합니다. 다크 모드에서 이메일을 보려면 앱 설정 > 앱 테마로 이동하여 다크 모드를 선택합니다.

Android 용 Secure Mail 23.6.0

다크 모드 23.6.0 릴리스부터 Secure Mail 은 다크 모드를 지원합니다. 다크 모드에서 이메일을 보려면 앱 설정 > 앱 테마로 이동하여 다크 모드를 선택합니다.

iOS 용 Secure Mail 23.5.0

분할 보기 및 슬라이드 오버 모드에서의 멀티태스킹 23.5.0 릴리스부터 Secure Mail 은 iPad 장치에서 멀티태스킹을 지원합니다. Secure Mail 을 열고 줄임표 (...) 를 눌러 분할 보기 또는 슬라이드 오버 옵션을 선택하여 멀티태스킹합니다. 이 기능은 사용자가 생산성을 유지하는 데 도움이 됩니다.



분할 보기에서는 두 번째 앱이 현재 앱 옆에 표시됩니다. 슬라이드 오버 레이아웃에서 두 번째 앱은 전체 화면 모드로 열리고 현재 앱은 화면 오른쪽이나 왼쪽으로 이동할 수 있는 더 작은 창으로 축소됩니다.

Secure Mail 23.3.5

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 23.2.0

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 22.11.0

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 22.9.0

iOS 용 Secure Mail 이제 Secure Mail 은 iOS 16 을 지원합니다.

Android 용 Secure Mail Secure Mail 가 이제 Android 13 을 지원합니다.

Secure Mail 22.6.2

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 22.6.0

이 릴리스부터 Secure Mail 은 Exchange Server 2016 누적 업데이트 23 에 대한 지원을 포함합니다.

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 22.3.0

iOS 용 Secure Mail HCL Domino 11 을 지원합니다. 이번 릴리스부터 iOS 용 Secure Mail 에는 HCL Domino 11(이전의 Lotus Notes) 에 대한 지원이 포함됩니다.

Google Analytics. Citrix Secure Mail 은 제품 품질을 개선하기 위해 Google Analytics 를 사용하여 앱 통계 및 사용 정보 분석 데이터를 수집합니다. Citrix 는 다른 개인 사용자 정보를 수집하거나 저장하지 않습니다. Secure Mail 에 대해 Google Analytics 를 비활성화하는 방법과 관련해서는 [Google Analytics 비활성화](#)를 참조하십시오.

Android 용 Secure Mail HCL Domino 11 을 지원합니다. 이번 릴리스부터 Android 용 Secure Mail 에는 HCL Domino 11(이전의 Lotus Notes) 에 대한 지원이 포함됩니다.

Google Analytics. Citrix Secure Mail 은 제품 품질을 개선하기 위해 Google Analytics 를 사용하여 앱 통계 및 사용 정보 분석 데이터를 수집합니다. Citrix 는 다른 개인 사용자 정보를 수집하거나 저장하지 않습니다. Secure Mail 에 대해 Google Analytics 를 비활성화하는 방법과 관련해서는 [Google Analytics 비활성화](#)를 참조하십시오.

Secure Mail 22.2.0

iOS 용 Secure Mail 피드 관리 옵션은 버전 21.5.0 에서 더 이상 사용되지 않습니다. 이 릴리스에서는 iOS 용 Secure Mail 에 다음과 같은 기본 피드 카드만 표시됩니다.

- 읽지 않음
- 모임 초대
- 예정된 모임
- 관리자가 보냄

현재 이 기능을 활성화하고 구성한 경우 기본 카드가 기본 카드로 재정의됩니다.

Android 용 Secure Mail 피드 관리 옵션은 버전 21.5.0 에서 더 이상 사용되지 않습니다. 이 릴리스에서는 iOS 용 Secure Mail 에 다음과 같은 기본 피드 카드만 표시됩니다.

- 읽지 않음
- 모임 초대
- 예정된 모임
- 관리자가 보냄

현재 이 기능을 활성화하고 구성한 경우 기본 카드가 기본 카드로 재정의됩니다.

Secure Mail 21.12.0


iOS 용 Secure Mail 사용자 지정 사용자 에이전트를 지원합니다. 이번 릴리스부터 Microsoft Office 365 for AD FS(Active Directory Federation Services) 또는 IDP(ID 공급자) 를 통한 인증에 사용자 지정 사용자 에이전트를 사용할 수 있습니다. 이 기능을 사용하려면 Citrix Endpoint Management 콘솔에서 최신 인증 정책을 위한 사용자 지정 사용자 에이전트를 사용하도록 설정하고 구성해야 합니다.


Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 21.11.0

Android 용 Secure Mail

자가 진단 도구 이제 Android 용 Secure Mail 에서 발생할 수 있는 모든 문제를 해결할 수 있습니다. 앱 설정의 지원 메뉴 옵션 아래에 있는 문제 해결 버튼을 사용합니다. 문제를 해결하려면 Secure Mail 을 열고 설정 > 문제 해결로 이동합니다.

 **Troubleshoot**

 Is Secure Mail not functioning as you would expect?
Try restoring default settings for features related to your issue, by using the suggestions.

Sync mail period
Click "Optimize now" to change sync mail period for offline usage.
Recommended setting: 3 days
[Optimize now](#)

Sync inbox frequency
Click "Optimize now" to change sync inbox frequency.
Recommended setting: ON
[Optimize now](#)

Sync email
Click "Optimize now" to sync email.
Recommended setting: ON
[Optimize now](#)

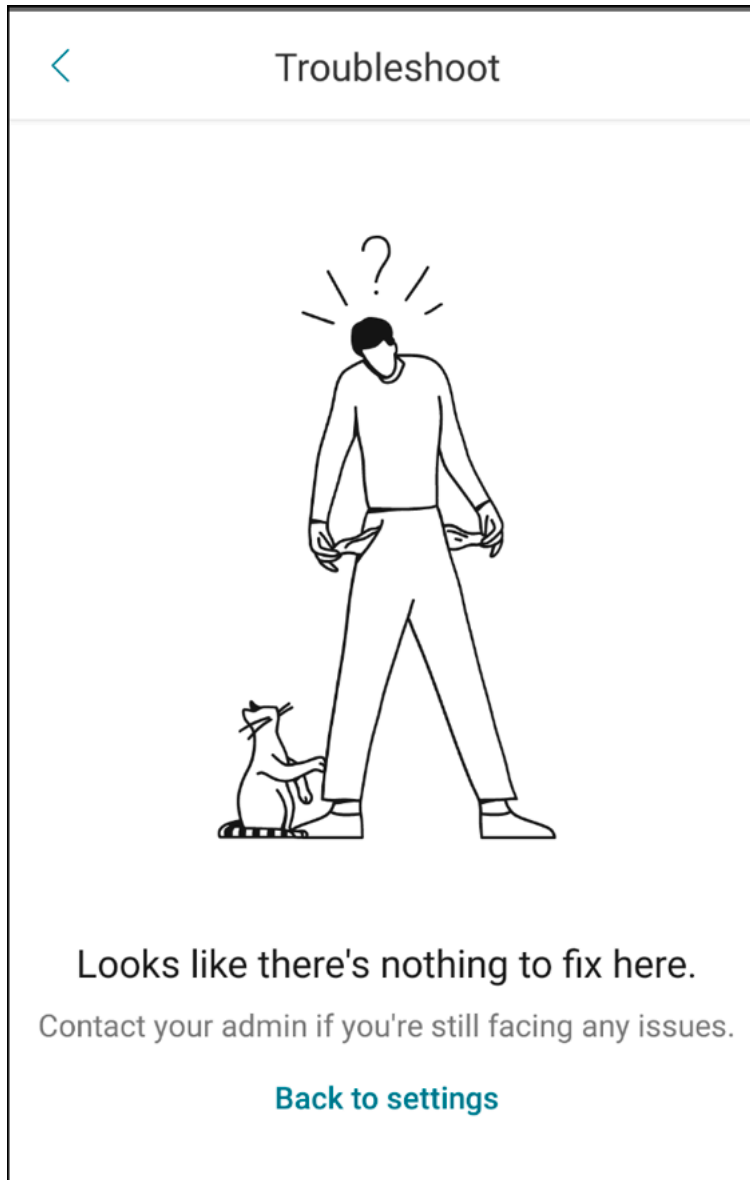
Show pictures
Click "Optimize now" to display pictures.
Recommended setting: OFF

문제 해결을 위해 다음 메뉴 항목이 나타납니다.

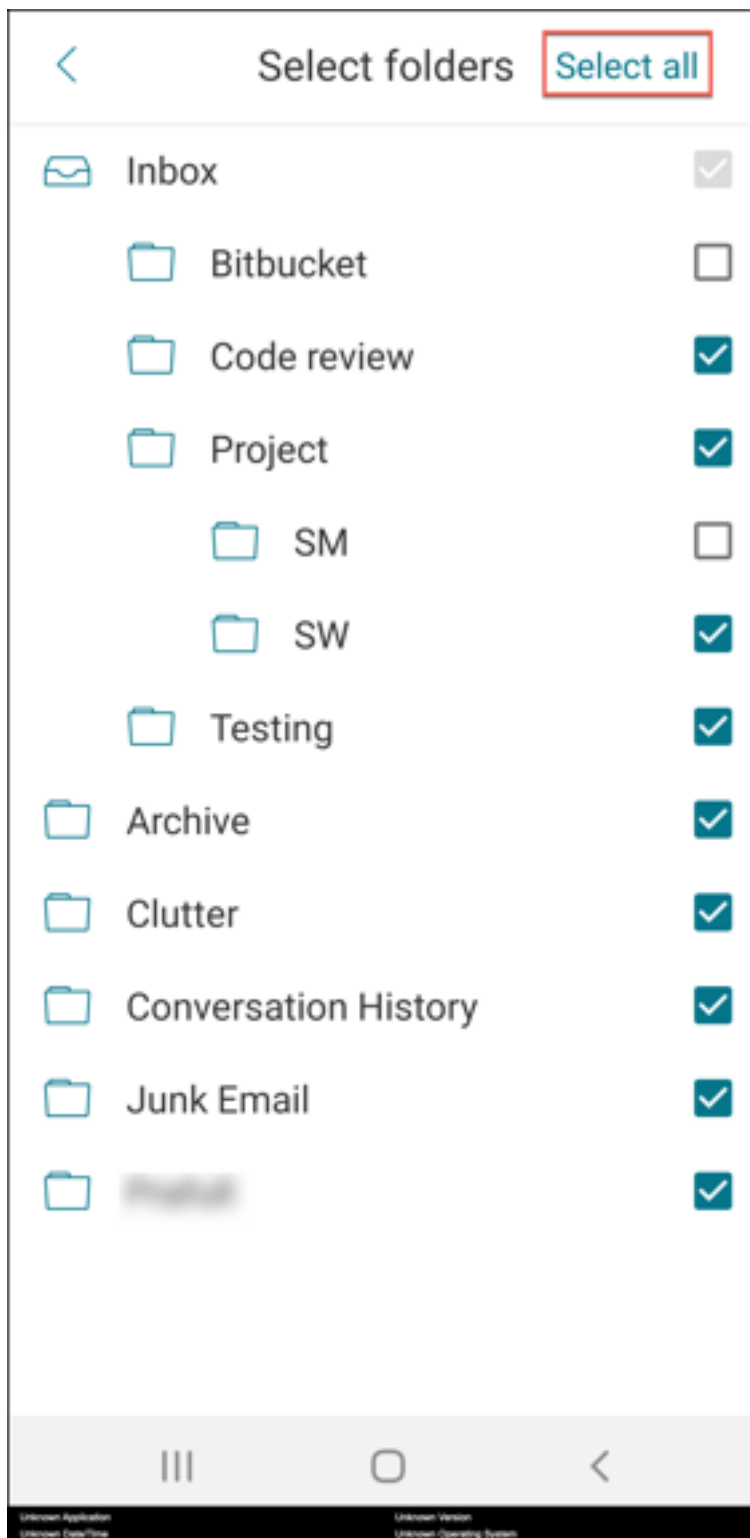
- 기본 앱 기본 설정 지우기
- 기본 알림 시간
- 배터리 최적화 무시
- 일정 알림 관리
- 메일 알림 관리
- 사진 표시

- 일정 동기화
- 연락처 동기화
- 전자 메일 동기화
- 받은 편지함 동기화 빈도
- 메일 동기화 기간

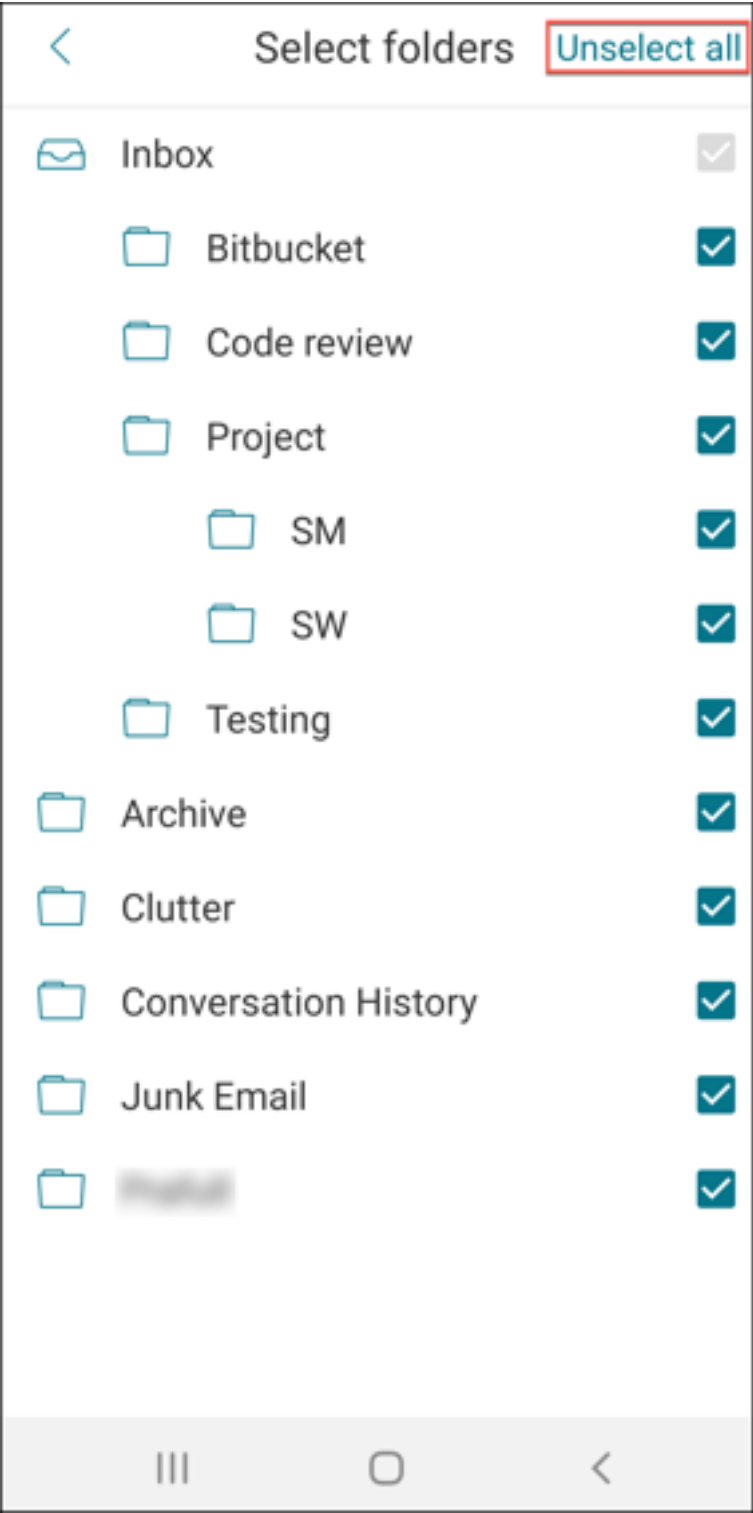
이러한 설정이 모두 기본값으로 복원되었는데도 Secure Mail 에 문제가 계속 발생하면 관리자에게 문의하십시오.



하위 폴더 알림 기능 항상 설정 > 알림 > 메일 폴더로 이동하여 폴더 선택 화면의 모두 선택 옵션을 클릭하면 모든 하위 폴더에 대한 알림을 받을 수 있습니다.



모두 선택 취소를 클릭하여 모든 하위 폴더에 대한 알림 수신을 중지할 수 있습니다.



Secure Mail 21.10.5

이 릴리스부터 Secure Mail 은 Exchange Server 2019 누적 업데이트 11 및 Exchange Server 2016 누적 업데이트 22 에 대한 지원을 포함합니다.

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

참고:

2021 년 10 월부터 Android 7 의 Secure Mail 에 대한 지원이 종료됩니다.

Secure Mail 21.10.0

Android 용 Secure Mail

- **Android 12** 를 지원합니다. 이번 릴리스부터 Android 12 를 실행하는 장치에서 Secure Mail 이 지원됩니다.
- Secure Mail 은 Android 11 에 대한 Google Play 의 현재 대상 API 요구 사항 (API 수준 30) 을 충족합니다.

Secure Mail 21.9.1

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 21.9.0

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 21.8.5

Android 용 Secure Mail 이미 등록된 장치에서 **Android 12 Beta 4** 를 지원합니다. Secure Mail 가 이제 Android 12 Beta 4 를 지원합니다. Android 12 Beta 4 로 업그레이드하려는 경우 먼저 Secure Hub 를 버전 21.7.1 로 업데이트해야 합니다. Secure Hub 21.7.1 은 Android 12 Beta 4 로 업그레이드하는 데 필요한 최소 버전입니다. 이 릴리스에서는 이미 등록된 사용자를 위해 Android 11 에서 Android 12 Beta 4 로 원활하게 업그레이드할 수 있습니다.

참고:

Citrix 는 Android 12 에 대한 1 일차 지원을 제공하기 위해 최선을 다하고 있습니다. 이후 버전의 Secure Mail 은 Android 12 를 완벽하게 지원하기 위해 추가 업데이트를 받습니다.

Secure Mail 21.8.0

iOS 용 Secure Mail

하이브리드 환경의 **Exchange Server** 전자 메일 기반 자동 검색 iOS 용 Secure Mail 에서는 전자 메일 주소를 사용하여 Microsoft 365 Exchange 계정을 구성할 수 있으므로 하이브리드 Exchange 서버의 원활한 로그인 환경이 보장됩니다. 이 기능은 온프레미스 Exchange Server 에서도 사용할 수 있습니다.

참고:

Exchange Server 에 대해 자동 검색 기능을 활성화해야 합니다.

Microsoft Office 365 를 사용하여 최신 인증을 실행하는 설정에 대한 풍부한 푸시 알림 이 릴리스에서 Secure Mail 은 네트워크 액세스 설정이 터널링됨 - 웹 **SSO** 로 설정되어 있고 Exchange Web Services (EWS) 호스트 이름이 제외 목록에 포함되어 있는 경우 푸시 알림을 지원합니다. EWS 와 ActiveSync 호스트가 동일한 경우 ActiveSync 호스트가 제외 목록 정책에 포함되어 있어야 합니다.

Secure Mail 의 듀얼 모드 MAM(모바일 애플리케이션 관리) SDK 를 사용하여 iOS 플랫폼에서 제공되지 않는 MDX 기능의 영역을 대체할 수 있습니다. MDX 래핑 기술은 2023 년 7 월에 EOL(수명 종료) 에 도달할 예정입니다.

Citrix Secure Mail 은 2023 년 7 월 예정인 MDX EOL 에 대비할 수 있도록 MDX 및 MAM SDK 프레임워크와 함께 릴리스됩니다. 엔터프라이즈 응용 프로그램을 계속 관리하려면 MAM SDK 를 포함해야 합니다. Citrix 는 **MAM SDK** 로의 전환을 권장합니다. 듀얼 모드 기능은 Secure Mail 앱을 새로운 MAM SDK 모델로 전환하는 방법을 제공하기 위해 만들어졌습니다.

듀얼 모드 기능을 사용하면 MDX(현재 레거시 **MDX**) 로 앱을 계속 관리하거나 새로운 **MAM SDK** 로 전환할 수 있습니다. **MDX** 또는 **MAM SDK** 정책 컨테이너에서 다음과 같은 정책 설정 옵션을 사용할 수 있습니다.

- **MAM SDK**
- 레거시 **MDX**

The screenshot shows the Citrix Cloud Endpoint Management interface. The left sidebar lists navigation options: Device Policies, Apps, Media, Actions, Content Collaboration, Enrollment Profiles, and Delivery Groups. The 'Apps' section is active, showing a list of applications under the 'MDX' category. The 'Secure Mail' application is selected, and its configuration page is displayed. The configuration includes fields for File name, App Description, App version, Minimum OS version, Maximum OS version, and Excluded devices. There are also toggle switches for 'Remove app if MDM profile is removed', 'Prevent app data backup', 'Force app to be managed', and 'App deployed via Volume purchase'. A red box highlights the 'MDX or MAM SDK policy container' section, which has two radio button options: 'MAM SDK' and 'Legacy MDX'. The 'Legacy MDX' option is currently selected. Below this, there is a section for 'MDX Policies' with a sub-section for 'Authentication'.

MDX 또는 **MAM SDK** 정책 컨테이너 정책에서는 레거시 **MDX** 에서 **MAM SDK** 로 옵션을 변경할 수만 있습니다.

전환하면 앱을 다시 설치해야 하므로 **MAM SDK** 에서 레거시 **MDX** 로 전환하지 않는 것이 좋습니다. 기본값은 레거시 **MDX** 입니다. 한 장치에서 실행되는 Secure Mail 과 Secure Web 모두에 대해 동일한 정책 모드를 설정해야 합니다. 동일한 장치에서 두 개의 서로 다른 모드를 실행할 수 없습니다.

MAM SDK 모드를 선택하면 앱이 자동으로 MAM SDK 프레임워크로 전환되며 관리자의 추가 작업 없이 장치 정책이 새로 고쳐 집니다.

참고:

레거시 **MDX** 에서 **MAM SDK** 프레임워크로 전환하면 네트워크 액세스 정책을 터널링됨—웹 **SSO** 또는 제한 없음 중 하나로 수정해야 합니다.

사전 요구 사항

듀얼 모드 기능을 성공적으로 배포하려면 다음 요구 사항이 충족되어야 합니다.

- Citrix Endpoint Management 를 버전 10.12 RP2 이상 또는 10.11 RP5 이상으로 업데이트합니다.
- 모바일 앱을 버전 21.8.0 이상으로 업데이트합니다.
- 조직에서 타사 앱을 사용하는 경우 MAM SDK 프레임워크로 전환하기 전에 타사 앱에 MAM SDK 를 통합해야 합니다. 관리되는 모든 앱을 한 번에 MAM SDK 로 이동해야 합니다.

제한 사항

- MAM SDK 는 MDX 암호화가 아닌 플랫폼 기반 암호화만 지원합니다.
- Citrix Endpoint Management 버전 10.12 RP2 이상 또는 10.11 RP5 이상으로 업데이트하지 않으면 중복된 정책 항목이 나타납니다. 정책 파일이 버전 21.8.0 이상에서 실행되는 경우 중복 항목이 생성됩니다.
- 앱 관리의 MAM SDK 모드로 전환하면 일부 기능이 지원되지 않거나 제공되지 않습니다. 또한 열기 및 복사/붙여넣기 같은 작업에는 모드가 서로 다른 앱 간의 상호 운용이 지원되지 않습니다. 예를 들어 레거시 **MDX** 모드에서 관리되는 앱의 콘텐츠를 **MAM SDK** 모드에서 관리되는 앱으로 복사하거나 그 반대로 복사할 수 없습니다. MAM SDK 모드에서 사용할 수 없는 기능은 다음 표를 참조하십시오.

기능	레거시 MDX	MAM SDK
공유 장치	예	아니요
Intune	예	아니요
SMIME 공유 인증서 저장소	예	아니요
파생된 자격 증명	예	아니요
UIWebView 터널링	예	아니요
전체 VPN	예	아니요

- 다음 정책은 더 이상 사용되지 않으며 MAM SDK 모드로 제공되지 않습니다.
 - 허용된 Secure Web 도메인
 - 허용된 Wi-Fi 네트워크
 - 대체 Citrix Gateway
 - 인증서 레이블
 - Citrix 보고
 - 명시적 로그오프 알림
 - Micro VPN 세션 필요
 - Micro VPN 세션에 필요한 유예 기간 (분)
 - 보고서 파일 캐시 최대값
 - Wi-Fi 필요
 - Wi-Fi 를 통해서만 보고서 보내기
 - 업로드 토큰

참고:

내부 서버에 대해 인증하기 위해 클라이언트 인증서를 사용하는 경우 클라이언트 인증은 Access Gateway 에 사용된 인증과 동일해야 합니다.

MAM SDK 에 대한 자세한 내용은 다음 문서를 참조하십시오.

- [MAM SDK Overview\(MAM SDK 개요\)](#)
- [모바일 애플리케이션 통합에 대한 Citrix Developer 문서](#)
- [Citrix 블로그 게시물](#)
- [Citrix 다운로드](#)에 로그인할 때 SDK 다운로드

Android 용 Secure Mail

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 21.7.0

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 21.6.0

iOS 용 Secure Mail 이 릴리스부터는 다음 네트워크 액세스 정책 옵션이 더 이상 지원되지 않습니다.

- 이전 설정 사용
- 터널링됨 - 전체 **VPN**
- 터널링됨 - 전체 **VPN** 및 웹 **SSO**

터널링됨 - 전체 **VPN** 또는 터널링됨 - 전체 **VPN** 및 웹 **SSO** 정책을 사용하는 경우 터널링됨 - 웹 **SSO** 정책으로 전환해야 합니다. 더 이상 사용되지 않는 정책을 계속 사용하는 경우 이메일이 동기화되지 않습니다.

참고:

STA(Secure Ticket Authority) 를 사용하려면 네트워크 액세스 정책을 터널링됨 - 웹 **SSO** 로 설정해야 합니다.

Android 용 Secure Mail 문제 해결 옵션을 사용하여 자가 진단을 지원합니다. 이 기능을 사용하면 앱의 올바른 작동에 중요한 기본 설정 및 설정이 기본값으로 설정되어 있는지 여부를 검토할 수 있습니다. 특정 Secure Mail 설정과 관련하여 오류가 발생하는 경우 이 기능을 사용하여 앱 문제를 해결하십시오.

이 기능에 액세스하려면 앱 설정을 열고 지원에서 문제 해결을 탭합니다. 검토하고 편집할 수 있도록 다음과 같은 메뉴 옵션이 표시됩니다.

- 메일 동기화 기간
- 받은 편지함 동기화 빈도
- 전자 메일 동기화

- 사진 표시
- 기본 알림 시간
- 일정 동기화
- 연락처 동기화

설정을 기본값으로 복원하려면 변경 사항 적용을 탭합니다. 모든 설정을 기본값으로 복원하려면 변경 사항 모두 적용을 탭합니다.

Secure Mail 21.5.0

이 릴리스부터 Secure Mail 은 Exchange Server 2019 누적 업데이트 9 및 Exchange Server 2016 누적 업데이트 20에 대한 지원을 포함합니다.

iOS 용 Secure Mail

- **Secure Mail** 일정 이벤트에서 **Microsoft Teams** 회의를 만들 수 있습니다. iOS 용 Secure Mail 에서 일정 이벤트를 만드는 중에 Microsoft Teams 회의 초대를 만들 수 있습니다. Microsoft Teams 회의를 만들려면 **Microsoft Teams** 회의를 전환합니다. 이벤트 세부 정보가 포함된 회의 초대 링크와 세부 정보가 자동으로 전송됩니다. 자세한 내용은 [Secure Mail 일정 이벤트에서 Microsoft Teams 회의 만들기](#)를 참조하십시오.
- 이 릴리스부터는 다음 네트워크 액세스 정책 옵션이 더 이상 사용되지 않으며 버전 21.6.0 부터 더 이상 지원되지 않습니다.
 - 이전 설정 사용
 - 터널링됨 - 전체 **VPN**
 - 터널링됨 - 전체 **VPN** 및 웹 **SSO**

터널링됨 - 전체 **VPN** 또는 터널링됨 - 전체 **VPN** 및 웹 **SSO** 정책을 사용하는 경우 터널링됨 - 웹 **SSO** 정책으로 전환해야 합니다. 더 이상 사용되지 않는 정책을 계속 사용하는 경우 이메일이 동기화되지 않습니다.

참고:

터널링됨 - 전체 **VPN** 을 사용하고 STA(Secure Ticket Authority) 가 구성되어 있는 경우 최신 인증 화면이 로드되지 않습니다.

Android 용 Secure Mail

- 이 릴리스의 경우 Citrix Endpoint Management 콘솔에서 필수 업그레이드 사용 안 함 기타 정책을 더 이상 사용할 수 없습니다. 앱이 Play Store 에서 제공되는 최신 버전으로 자동 업그레이드됩니다.
- 이 릴리스의 Android 용 Secure Mail 에서는 피드 관리 옵션이 더 이상 사용되지 않습니다. 현재 이 기능이 사용 설정 및 구성되어 있는 경우 피드 창의 기본 설정에 따라 피드가 계속 표시됩니다. 새 사용자이거나 이전에 모든 피드 카드를 제거한 경우 다음과 같은 기본 피드 카드를 사용할 수 있습니다.

- 읽지 않음
- 모임 초대
- 예정된 모임
- 관리자가 보냄

Secure Mail 21.4.5

Android 용 Secure Mail 전자 메일 기반 자동 검색 지원. Android 용 Secure Mail에서는 전자 메일 주소를 사용하여 Microsoft O365 Exchange 계정을 구성할 수 있으므로 원활한 로그인 환경이 보장됩니다. 하이브리드 환경에서 자동 검색을 사용하도록 설정한 경우 온-프레미스 사용자도 이 기능을 사용할 수 있습니다.

참고:

이 기능은 Exchange Server 2016 누적 업데이트 3 이상에서만 지원됩니다.

Secure Mail 21.4.0

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 21.3.5

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 21.3.0

iOS 용 Secure Mail Secure Mail iOS의 배포 대상이 **iOS 12.2**로 변경되었습니다. iOS용 Microsoft Intune App SDK 버전 14.1.3의 경우 타겟 앱의 최소 iOS 배포 버전이 iOS 12.2여야 합니다. 이 요구 사항을 준수하기 위해 Secure Mail의 배포 대상이 iOS 12.2로 업데이트되었습니다.

Android 용 Secure Mail Secure Mail 일정 이벤트에서 **Microsoft Teams** 회의를 만들 수 있습니다. Android용 Secure Mail에서 일정 이벤트를 만드는 중에 Microsoft Teams 회의 초대를 만들 수 있습니다.

Microsoft Teams 회의를 만들려면 **Microsoft Teams** 회의를 전환합니다. 이벤트 세부 정보가 포함된 회의 초대 링크와 세부 정보가 자동으로 전송됩니다. 자세한 내용은 [Secure Mail 일정 이벤트에서 Microsoft Teams 회의 만들기](#)를 참조하십시오.

Secure Mail 21.2.0

이 릴리스부터 Secure Mail은 Exchange Server 2019 누적 업데이트 8 및 Exchange Server 2016 누적 업데이트 19에 대한 지원을 포함합니다.

iOS 용 Secure Mail

- **Secure Mail** 의 색상 개선. Secure Mail 은 Citrix 브랜드 색상 업데이트를 준수합니다.

Android 용 Secure Mail

- **Secure Mail** 의 색상 개선. Secure Mail 은 Citrix 브랜드 색상 업데이트를 준수합니다.
- **Microsoft Intune** 에 대한 지원. Android 용 Secure Mail 은 Microsoft Intune 7.2.2 최신 버전을 지원합니다.
- 폴더블 장치의 안정적인 작동. Android 용 Secure Mail 에는 폴더블 장치에서 안정적으로 작동하기 위한 수정 사항이 포함되어 있습니다.

Secure Mail 21.1.5

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 21.1.0

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 20.12.0

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 20.11.0

참고:

Exchange Server 2010 에 대한 지원은 2020 년 10 월 13 일에 종료되었습니다.

Secure Mail 20.10.5

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Mail **AndroidX** 라이브러리가 지원됩니다. Google 의 권장 사항에 따라 Secure Mail 은 **android.support** 패키지 라이브러리를 대체하는 **AndroidX** 라이브러리를 지원합니다.

Secure Mail 20.10.0

이 릴리스부터 Secure Mail 에 Exchange Server 2019 누적 업데이트 7 및 Exchange Server 2016 누적 업데이트 18에 대한 지원이 포함됩니다.

iOS 용 Secure Mail Secure Mail 에서 **Microsoft Teams** 모임에 참가하기. iOS 용 Secure Mail 에서는 캘린더의 초대장에서 바로 Microsoft Teams 모임에 참가할 수 있습니다. Microsoft Teams 앱이 설치되어 있으면 앱이 열리고 회의에 참가합니다. 앱이 설치되지 않은 경우 App Store 로 이동하여 Microsoft Teams 를 설치하는 옵션이 표시됩니다. <https://teams.microsoft.com/l/meetup-join/meetinglink> 형식의 회의인 경우 앱이 열리고 회의에 바로 참가합니다.

참고:

관리자는 허용된 URL 정책에 `+^msteams:`를 포함해야 합니다. 자세한 내용은 [앱 상호 작용 \(아웃바운드 URL\)](#)을 참조하십시오.

Android 용 Secure Mail

- **Secure Mail** 에서 **Microsoft Teams** 모임에 참가하기. Android 용 Secure Mail 에서는 캘린더의 초대장에서 바로 Microsoft Teams 모임에 참가할 수 있습니다. Microsoft Teams 앱이 설치되어 있으면 앱이 열리고 회의에 참가합니다. 앱이 설치되지 않은 경우 Google Play 로 이동하여 Microsoft Teams 를 설치하는 옵션이 표시됩니다. <https://teams.microsoft.com/l/meetup-join/>meetinglink> 형식의 회의인 경우 앱이 열리고 회의에 바로 참가합니다.

참고:

관리자는 제한된 열기 제외 목록 정책에 { `action=android.intent.action.VIEW`
`scheme=msteams` `package=com.microsoft.teams` }가 포함되어 있는지 확인합니다.
자세한 내용은 [앱 상호 작용](#)을 참조하십시오.

- Secure Mail 는 Android 10 에 대한 Google Play 의 현재 대상 API 요구 사항을 지원합니다.

Secure Mail 20.9.5

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 20.9.0

Azure Government Cloud Computing 에 대한 지원. iOS 및 Android 용 Secure Mail 은 Azure Active Directory 테넌트에서 최신 인증 (OAuth) 을 위한 Government Cloud Computing(GCC) High 를 지원합니다. Secure Mail 은 모든 GCC High 서비스에 대한 Microsoft 의 필수 요구 사항을 충족하기 위해 GCC High 에 엔드포인트로 등록됩니다. 자세한 내용은 [Microsoft 365 Government 의 Azure Active Directory 에 대한 새로운 소식](#)을 참조하십시오.

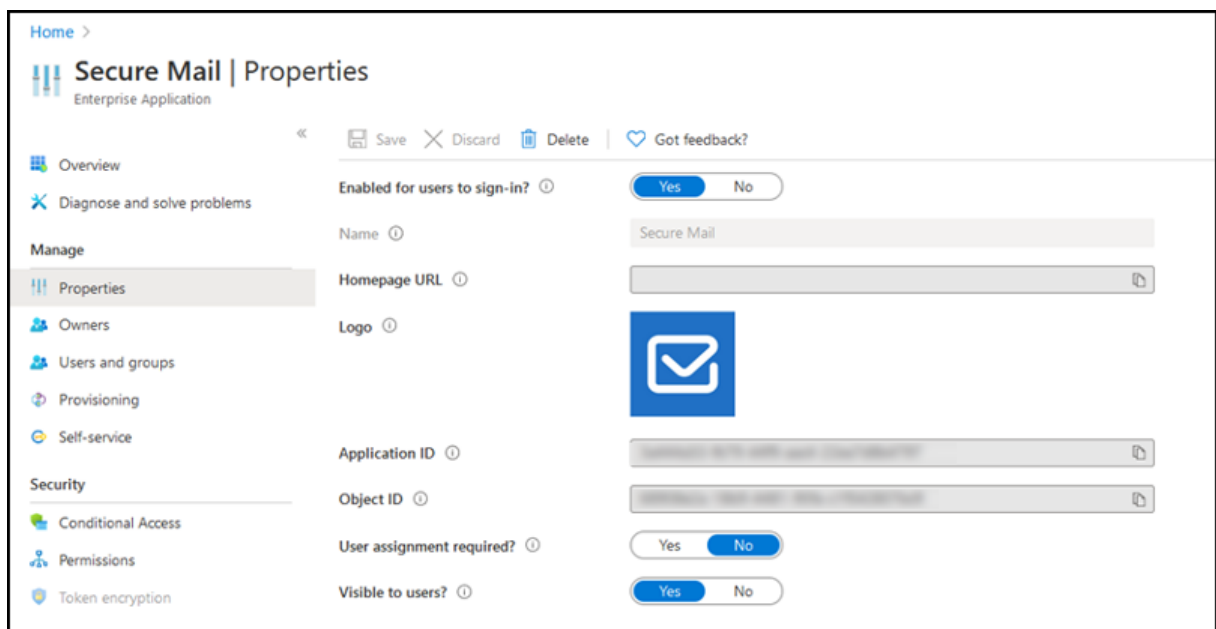
이번 변경을 통해 인증용 Azure Active Directory 테넌트에서 GCC High 로 라우팅됩니다. 또한 관리자는 Azure Active Directory 테넌트에서 Secure Mail 에 대한 권한을 허용해야 합니다.

사전 요구 사항 Azure Active Directory 의 전역 관리자가 다음을 수행하는지 확인합니다.

- 장치에 최신 버전의 Secure Mail 을 다운로드합니다.
- Secure Mail 앱에서 Exchange 계정을 구성하고 모든 사용자가 로그인할 수 있도록 Azure Active Directory 의 앱 권한을 허용합니다. 다음 화면을 참조하십시오.

참고:

이러한 단계는 일회성 요구 사항으로 전역 관리자에게만 해당됩니다. 앱에 액세스 권한이 부여되면 App Store 에서 간단하게 업그레이드할 수 있습니다.



업그레이드 후 업그레이드하고 나면 새로 고침 토큰이 만료된 후 다시 인증할 것인지를 묻는 메시지가 나타나며, Azure Active Directory 의 GCC High 로 리디렉션됩니다. 권한 부여 요청이 Azure Active Directory 의 GCC High 로 전송되도록 하려면 이전 워크플로의 유효성을 검사합니다.

다음 방법 중 하나를 사용하여 워크플로를 검증할 수 있습니다.

- 앱 이름 **Secure Mail-GCC High** 가 포함된 Secure Mail 이 Azure Active Directory 테넌트의 로그인 페이지에 나타납니다.
- Secure Mail 로그를 확인하여 재인증 후 <https://login.microsoftonline.us>를 통해 리디렉션이 수행되는지 확인합니다.

Secure Mail 20.8.5

Android 용 Secure Mail Android 용 Secure Mail 는 Android 11 을 지원합니다.

Secure Mail 20.8.0

이 릴리스부터 Secure Mail 은 Exchange Server 2019 누적 업데이트 6 및 Exchange Server 2016 누적 업데이트 17 에 대한 지원을 포함합니다.

Android 용 Secure Mail Secure Mail 에 대한 듀얼 모드 MAM(모바일 애플리케이션 관리) SDK 를 사용하여 iOS 및 Android 플랫폼에서 제공되지 않는 MDX 기능의 영역을 대체할 수 있습니다. MDX 래핑 기술은 2022 년 3 월에 EOL(수명 종료) 에 도달할 예정입니다. 엔터프라이즈 응용 프로그램을 계속 관리하려면 MAM SDK 를 포함해야 합니다.

버전 20.8.0 에서 Android 앱은 앞서 언급한 MDX EOL 전략에 대비하기 위해 MDX 및 MAM SDK 가 포함된 상태로 릴리스 됩니다. MDX 듀얼 모드는 레거시 MDX Toolkit 에서 새 MAM SDK 로의 전환 경로를 제공하기 위한 것입니다. 듀얼 모드를 사용하면 MDX Toolkit(현재의 레거시 MDX) 을 사용하여 계속해서 앱을 관리하거나 새로운 MAM SDK 로 전환하여 앱을 관리할 수 있습니다.

앱 관리를 위해 MAM SDK 로 전환하면 Citrix 가 추가 변경 사항을 구현하므로 관리자가 따로 조치를 취할 필요가 없습니다.

MAM SDK(미리 보기) 에 대한 자세한 내용은 다음 문서를 참조하십시오.

- [MAM SDK Overview\(MAM SDK 개요\)](#)
- [장치 관리](#)에 대한 Citrix Developer 섹션
- [Citrix 블로그 게시물](#)
- [Citrix 다운로드](#)에 로그인할 때 SDK 다운로드

사전 요구 사항 듀얼 모드 기능을 성공적으로 배포하려면 다음을 확인하십시오.

- Citrix Endpoint Management 를 버전 10.12 RP2 이상 또는 10.11 RP5 이상으로 업데이트합니다.
- 모바일 앱을 버전 20.8.0 이상으로 업데이트합니다.
- 정책 파일을 버전 20.8.0 이상으로 업데이트합니다.
- 조직에서 타사 앱을 사용하는 경우 Citrix 모바일 생산성 앱에 대한 MAM SDK 로 전환하기 전에 MAM SDK 를 타사 앱에 통합해야 합니다. 관리되는 모든 앱을 한 번에 MAM SDK 로 이동해야 합니다.

참고:

MAM SDK 는 모든 클라우드 기반 고객에 대해 지원됩니다.

제한 사항

- MAM SDK 는 Citrix Endpoint Management 배포의 Android Enterprise 플랫폼에 게시된 앱만 지원합니다. 새로 게시된 앱의 경우 플랫폼 기반 암호화가 기본 암호화입니다.

- MAM SDK 는 MDX 암호화가 아닌 플랫폼 기반 암호화만 지원합니다.
- Citrix Endpoint Management 를 업데이트하지 않고 버전 20.8.0 이상에서 모바일 앱에 대해 정책 파일을 실행하면 Secure Mail 에 대한 중복 네트워킹 정책 항목이 만들어집니다.

Citrix Endpoint Management 에서 Secure Mail 을 구성할 때 듀얼 모드 기능을 사용하면 MDX Toolkit(현재의 레거시 **MDX**) 을 사용하여 계속해서 앱을 관리하거나 새로운 **MAM SDK** 로 전환하여 앱을 관리할 수 있습니다. **MAM SDK** 는 모듈식이므로 조직에서 사용하는 MDX 기능의 하위 집합만 사용할 수 있습니다. 따라서 Citrix 에서서는 MAM SDK 로 전환하도록 권장합니다.

MDX 또는 **MAM SDK** 정책 컨테이너에서 다음과 같은 정책 설정 옵션을 사용할 수 있습니다.

- **MAM SDK**
- 레거시 **MDX**

The screenshot shows the Citrix Cloud Endpoint Management console. The left sidebar lists various sections under 'MDX', including '1 App Information', '2 Platform' (with 'iOS' selected), '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The main area displays the configuration for a 'Secure Mail' app. Key settings include 'App version' (20.4.5), 'Minimum OS version' (11.0), and 'Maximum OS version'. The 'MDX or MAM SDK policy container' section is highlighted with a red box, showing two radio button options: 'MAM SDK' and 'Legacy MDX'. Below this, the 'MDX Policies' section is visible, with 'Authentication' as a sub-section.

MDX 또는 **MAM SDK** 정책 컨테이너 정책에서는 레거시 **MDX** 에서 **MAM SDK** 로 옵션을 변경할 수만 있습니다. **MAM SDK** 에서 레거시 **MDX** 로 전환하는 옵션은 허용되지 않으며 앱을 다시 게시해야 합니다. 기본값은 레거시 **MDX** 입니다. 동일한 장치에서 실행되는 Secure Mail 과 Secure Web 모두에 대해 동일한 정책 모드를 설정해야 합니다. 동일한 장치에서 두 개의 서로 다른 모드를 실행할 수 없습니다.

iOS 용 Secure Mail 최적화된 사서함 동기화. iOS 용 Secure Mail 의 사서함 동기화가 더 나은 사용자 경험을 제공하도록 개선되었습니다. 일정과 연락처가 더 빠르게 동기화됩니다. 3 주가 지난 전자 메일은 동기화 시간을 줄이기 위해 잘립니다. 전자 메일을 열 때 전체를 볼 수 있습니다.

Secure Mail 20.7.5

참고:

Android 6.x 에 대한 지원은 2020 년 6 월 30 일에 종료되었습니다.

모바일 생산성 앱에 대한 최신 정보는 [최근 발표 내용](#) 문서를 참조하십시오.

Secure Mail 20.7.0

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 20.6.5

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 20.6.0

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 20.5.0

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 20.4.5

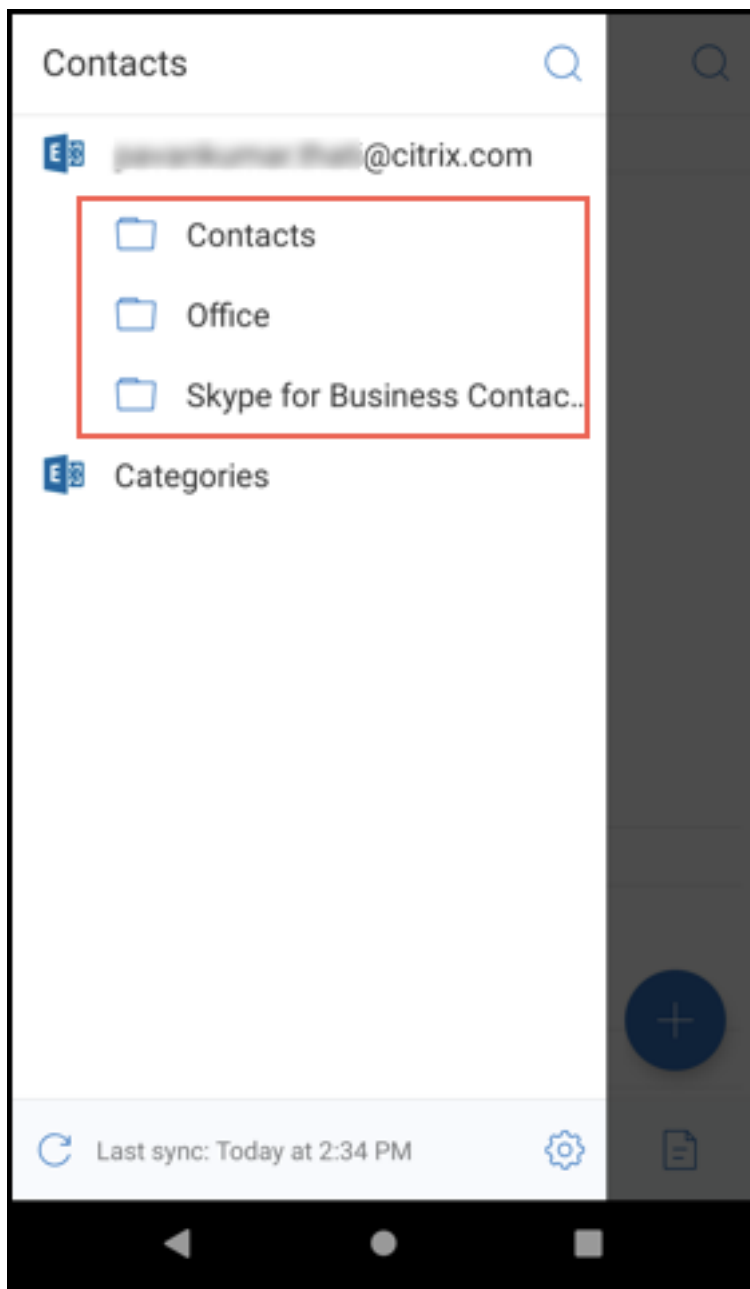
Android 용 Secure Mail 이 릴리스부터 Secure Mail 은 Exchange Server 2019 누적 업데이트 5 및 Exchange Server 2016 누적 업데이트 16 에 대한 지원을 포함합니다.

Secure Mail 20.4.0

이 릴리스부터 Secure Mail 은 Exchange Server 2016 누적 업데이트 15 및 Exchange Server 2013 누적 업데이트 23 에 대한 지원을 포함합니다.

Secure Mail 20.3.0

Android 용 Secure Mail 연락처에 폴더 만들기. Android 용 Secure Mail 의 전자 메일 계정 연락처 섹션에서 폴더를 추가, 편집 및 삭제할 수 있습니다.



iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 20.2.0

Android 용 Secure Mail

임시 보관함 최소화

Android 용 Secure Mail 에서 전자 메일을 작성하고 앱 내에서 탐색하는 동안 임시 보관함을 최소화할 수 있습니다. 이 기능에 대한 사용자 도움말 문서는 Citrix User Help Center 문서 [임시 보관함 전자 메일 최소화](#)를 참조하십시오.

Secure Mail 20.1.5

iOS 용 Secure Mail 이 릴리스부터 Secure Mail 은 Exchange Server 2019 누적 업데이트 4 에 대한 지원을 포함합니다.

Android 용 Secure Mail

- 양방향 연락처 동기화. Android 용 Secure Mail 에서 로컬 연락처 목록을 사용하여 Secure Mail 연락처를 생성, 편집 및 삭제할 수 있습니다.
- **ICS** 파일 지원. Android 용 Secure Mail 에서 첨부 파일로 받은 ICS 파일을 미리 보고 이벤트로 일정에 가져올 수 있습니다.
- 이 릴리스부터 Secure Mail 은 Exchange Server 2019 누적 업데이트 4 에 대한 지원을 포함합니다.

Secure Mail 20.1.0

이 릴리스부터 Secure Mail 은 Exchange Server 2016 누적 업데이트 14 에 대한 지원을 포함합니다.

Secure Mail 19.12.5

iOS 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Android 용 Secure Mail 보낸 메일 실행 취소. Android 용 Secure Mail 에서 보낸 메일을 실행 취소할 수 있습니다. 보내기 단추를 누르면 보낸 작업을 실행 취소할 수 있는 알림 메시지가 표시됩니다. 실행 취소를 눌러 보낸 작업을 되돌리고 메일 및 메일 수신자를 편집하거나 첨부 파일을 첨부 또는 제거하거나 메일을 삭제합니다.

임시 보관함 폴더에서 첨부 파일 동기화. Android 용 Secure Mail 에서 임시 보관함 폴더가 동기화되면 첨부 파일도 동기화되고 모든 장치에서 사용할 수 있게 됩니다. 이 기능은 Exchange ActiveSync 버전 16 이상을 실행하는 장치에서 사용할 수 있습니다.

Secure Mail 19.11.5

iOS 용 Secure Mail **Secure Mail** 의 연락처 사진. iOS 용 Secure Mail 에서 전자 메일 또는 모임 초대에 받는 사람을 추가할 때 연락처 사진을 볼 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [연락처의 사진 표시](#)를 참조하십시오.

Android 용 Secure Mail 앱에서 바로 **PDF** 파일 보기. Android 용 Secure Mail 의 경우 PDF 파일을 책갈피 및 주석과 함께 앱 내에서 볼 수 있습니다. 다른 Microsoft Office 첨부 파일의 향상된 보기도 가능합니다.

iOS 용 Secure Mail 19.10.6

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 19.10.5

iOS 용 Secure Mail 임시 보관함 최소화. iOS 용 Secure Mail에서는 전자 메일을 작성하는 동안 임시 보관함을 최소화하고 앱 내에서 탐색할 수 있습니다. 이 기능은 iOS 13 이상을 실행하는 장치에서 사용할 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [임시 보관함 전자 메일 최소화](#)를 참조하십시오.

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 19.10.0

Office 365 Exchange Server 정책을 사용하여 **Office 365** 서버 주소 정의. Secure Mail iOS 및 Android에서 **OAuth**의 **Office 365** 지원 섹션 아래에 **Office 365 Exchange Server**라는 이름의 새 정책이 추가되었습니다. 이 정책을 사용하면 클라우드에 있는 Office 365 사서함의 호스트 이름을 정의할 수 있습니다. 이 정책을 사용하면 정부 기관에 대한 Office 365도 지원할 수 있습니다. 호스트 이름은 *outlook.office365.com*과 같은 단일 값입니다. 기본값은 *outlook.office365.com*입니다.

Secure Mail iOS 및 Android의 암호화 관리 지원. 암호화 관리를 사용하면 최신 장치 플랫폼 보안을 사용하는 동시에 플랫폼 보안을 효과적으로 사용하기에 충분한 상태를 유지할 수 있습니다. 암호화 관리를 사용하면 iOS 또는 Android 플랫폼에서 파일 시스템 암호화가 제공되므로 로컬 데이터 암호화 중복을 제거할 수 있습니다. 이 기능을 사용하려면 관리자가 Citrix Endpoint Management 콘솔에서 암호화 유형 MDX 정책을 규정 준수를 적용하여 플랫폼 암호화로 구성해야 합니다.

암호화 관리 기능을 사용하려면 Citrix Endpoint Management 콘솔에서 암호화 유형 정책을 규정 준수를 적용하여 플랫폼 암호화로 설정합니다. 이렇게 하면 암호화 관리와 사용자 장치에 있는 기존의 모든 암호화된 앱 데이터가 MDX가 아닌 장치로 암호화된 상태로 원활하게 전환됩니다. 이 전환 중에 일회성 데이터 마이그레이션을 위해 앱이 일시 중지됩니다. 마이그레이션이 성공하면 로컬로 저장된 데이터의 암호화에 대한 책임이 MDX에서 장치 플랫폼으로 이전됩니다. MDX는 앱을 시작할 때마다 장치의 규정 준수를 계속 확인합니다. 이 기능은 MDM + MAM 및 MAM 전용 환경 모두에서 작동합니다.

암호화 유형 정책을 규정 준수를 적용하여 플랫폼 암호화로 설정하면 새 정책이 기존 MDX 암호화를 대체합니다.

Secure Mail에 대한 암호화 관리 MDX 정책에 대한 자세한 내용은 다음 위치에서 암호화 섹션을 참조하십시오.

- [Android 용 모바일 생산성 앱의 MDX 정책](#)
- [iOS 용 모바일 생산성 앱의 MDX 정책](#)

장치가 최소 규정 준수 요구 사항을 충족하지 못하는 경우 규정을 준수하지 않는 장치 동작 정책을 사용하여 수행할 작업을 선택할 수 있습니다.

- 앱 허용 - 앱의 정상적인 실행을 허용합니다.
- 경고 후 앱 허용 - 앱이 최소 규정 준수 요구 사항을 충족하지 않는다는 내용의 경고를 사용자에게 표시하고 앱의 실행을 허용합니다. 기본값입니다.
- 앱 차단 - 앱 실행을 차단합니다.

iOS 를 실행하는 장치 장치가 iOS 를 실행하는 장치에 대한 최소 규정 준수 요구 사항을 충족하는지 여부는 다음 기준에 따라 결정됩니다.

- iOS 10 - 앱이 지정된 버전 이상의 운영 체제 버전을 실행하고 있습니다.
- 디버거 액세스 - 앱에 디버깅이 활성화되어 있지 않습니다.
- 탈옥된 장치 - 앱이 탈옥 장치에서 실행되고 있지 않습니다.
- 장치 암호 - 장치 암호가 켜져 있습니다.
- 데이터 공유 - 앱에 대해 데이터 공유가 활성화되지 않았습니다.

Android 를 실행하는 장치 장치가 Android 를 실행하는 장치에 대한 최소 규정 준수 요구 사항을 충족하는지 여부는 다음 기준에 따라 결정됩니다.

- Android SDK 24(Android 7 Nougat) - 앱이 지정된 버전 이상의 운영 체제 버전을 실행하고 있습니다.
- 디버거 액세스 - 앱에 디버깅이 활성화되어 있지 않습니다.
- 루팅 장치 - 앱이 루팅된 장치에서 실행되고 있지 않습니다.
- 장치 잠금 - 장치 암호가 켜져 있습니다.
- 장치 암호화 - 앱이 암호화된 장치에서 실행 중입니다.

Secure Mail 19.9.5

iOS 용 Secure Mail **ICS** 파일 지원. iOS 용 Secure Mail 에서 첨부 파일로 받은 ICS 파일을 이벤트로 일정에 가져올 수 있습니다.

Android 용 Secure Mail 이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 19.9.0

이 릴리스부터 Secure Mail 이 다음과 같은 서버에 대한 지원을 포함합니다.

- Exchange Server 2016 누적 업데이트 13
- IBM Lotus Notes Traveler 버전 10.0.1.0 빌드 201811191126_20
- IBM Domino Mail Server 버전 10.0.1

iOS 용 Secure Mail

- iOS 용 Secure Mail 은 iOS 13 을 지원합니다.
- **MIME** 헤더를 사용하여 피싱 전자 메일 보고. iOS 용 Secure Mail 에서 사용자가 피싱 메일을 보고하면 EML 파일이 해당 메일의 첨부 파일로 생성됩니다. 관리자는 이 메일을 수신하고 보고된 메일에 연결된 MIME 헤더를 볼 수 있습니다. 이 기능을 사용하려면 관리자가 Citrix Endpoint Management 콘솔에서 피싱 보고 전자 메일 주소 정책을 구성하고 피싱 보고 메커니즘을 첨부 파일을 통해 보고로 설정해야 합니다. 자세한 내용은 [첨부 파일로 피싱 전자 메일 보고](#)를 참조하십시오.
- 반응형 전자 메일 지원. iOS 용 Secure Mail 이 반응형 전자 메일을 제공하도록 최적화되었습니다. 이전에는 큰 테이블이나 이미지가 포함된 전자 메일 내용이 잘못 렌더링되었습니다. 이 기능은 전자 메일의 형식과 크기에 관계없이 지원되는 모든 장치에서 전자 메일 내용을 더 쉽게 읽을 수 있도록 합니다.
- 일정 이벤트 끌어서 놓기. iOS 용 Secure Mail 에서 이벤트를 끌어서 놓는 방법으로 기존 일정 이벤트의 시간을 변경할 수 있습니다. 이벤트를 드래그하여 같은 날의 원하는 시간 슬롯 또는 업데이트하려는 날짜에 놓습니다.
- 자동으로 넘어가기. iOS 용 Secure Mail 에서 **Conversations(대화)**의 메시지를 삭제할 때 돌아갈 메시지를 선택할 수 있습니다. 이 기능을 사용하려면 **Settings(설정) > Auto Advance(자동 진행)**로 이동합니다. 그런 다음 사용 가능한 선택 항목에서 기본 설정을 선택합니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [대화에서 전자 메일 삭제 및 자동 진행](#)을 참조하십시오.
- **WkWebView** 지원. iOS 용 Secure Mail 은 WkWebView 를 지원합니다. 이 기능은 Secure Mail 의 전자 메일 및 일정 이벤트가 장치에서 렌더링되는 방식을 개선합니다.

Android 용 Secure Mail 이 릴리스부터 Android 용 Secure Mail 은 Android 6 이상을 실행하는 장치에서만 지원됩니다.

Android 용 Secure Mail 19.8.5

이 릴리스에는 버그 수정이 포함되어 있습니다.

Secure Mail 19.8.0

iOS 용 Secure Mail 이 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

Android 용 Secure Mail

- Android Q 지원.
- **Google Play** 의 **64** 비트 앱 지원. Android 용 Secure Mail 은 64 비트 아키텍처를 지원합니다.
- **Android 용 Secure Mail** 에서 당겨서 새로 고침 **UI** 개선. Material Design 지침에 따라 당겨서 새로 고침 기능을 다소 개선했습니다. 햄버거 아이콘을 누르면 화면 하단에서 동기화 타임스탬프를 사용할 수 있습니다.

Secure Mail 19.7.5

iOS 용 Secure Mail

- **임시 보관함 폴더 자동 동기화.** iOS 용 Secure Mail 에서 임시 보관함 폴더가 자동으로 동기화되고 모든 장치에서 임시 보관함을 사용할 수 있습니다. 이 기능은 Exchange ActiveSync v16 이상을 실행하는 설정에서 사용할 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [임시 보관함 폴더 자동 동기화](#)를 참조하십시오.
- **iOS 용 Secure Mail** 은 **MDM + MAM** 모드에서 **Microsoft Intune** 을 사용할 때 **Single Sign-on** 을 지원합니다. 이 기능을 사용하려면 장치에 Microsoft Authenticator 앱이 설치되어 있어야 합니다. Microsoft Authenticator 앱 설치에 대한 자세한 내용은 [Docs.microsoft.com](https://docs.microsoft.com) 에서 **Microsoft Authenticator** 앱 다운로드 및 설치를 참조하십시오.

Android 용 Secure Mail

참고:

OS 를 Android Q 로 업그레이드하기 전에 Citrix 에서는 Secure Mail 버전 19.7.5 로 업그레이드할 것을 권장합니다.

- **Microsoft Office 365** 로 최신 인증을 실행하는 설정의 터널링 정책에 웹 **SSO** 를 사용할 수 있습니다. Android 용 Secure Mail 에 **Use Web SSO for tunneling**(터널링에 웹 **SSO** 사용)이라는 이름의 새 정책이 추가되었습니다. 이 정책을 사용하면 OAuth 트래픽을 터널링하여 터널링됨—웹 SSO 를 통과할 수 있습니다. 이 작업을 수행하려면:
 - **Use Web SSO for tunneling**(터널링에 웹 **SSO** 사용) 정책을 **On**(켜기) 으로 설정합니다.
 - 네트워크 액세스 정책에서 **Tunneled - Web SSO**(터널링됨 - 웹 **SSO**) 옵션을 선택합니다.
 - **Background services**(백그라운드 서비스) 정책에서 OAuth 와 관련된 모든 호스트 이름을 제외합니다.
- **Android 용 Secure Mail** 은 **MDM + MAM** 모드에서 **Microsoft Intune** 을 사용할 때 **Single Sign-on** 을 지원합니다. 이 기능을 사용하려면 장치에 Intune Company Portal 앱이 설치되어 있어야 합니다. Intune Company Portal 앱에 로그인한 후에는 Secure Mail 에서 자격 증명을 사용하여 재인증하지 않고도 MDM + MAM 모드에서 SSO 를 사용할 수 있습니다.

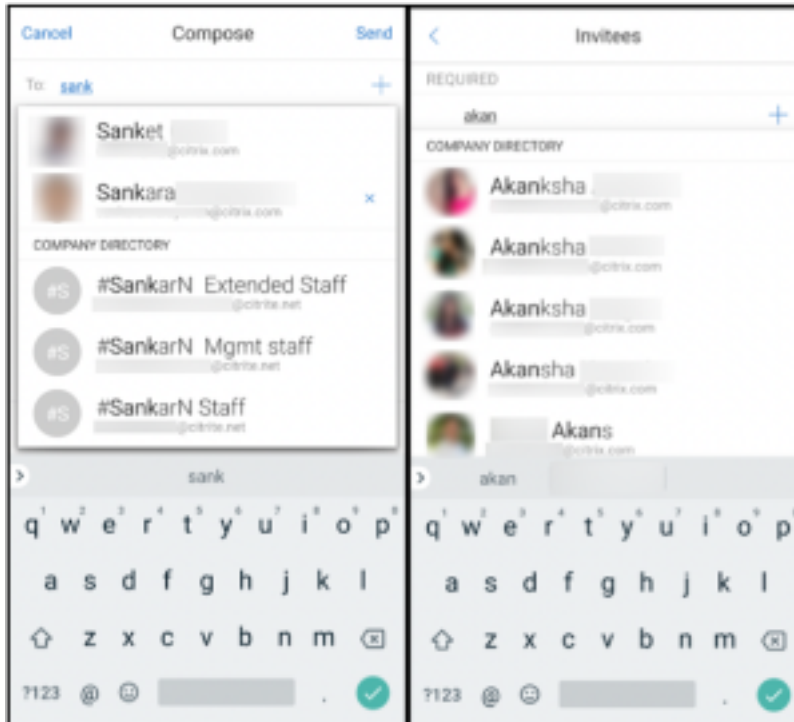
Secure Mail 19.6.5

iOS 용 Secure Mail iOS 용 Secure Mail 버전 19.6.5 에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다. 해결된 문제 및 알려진 문제 목록은 [알려진 문제와 수정된 문제](#)를 참조하십시오.

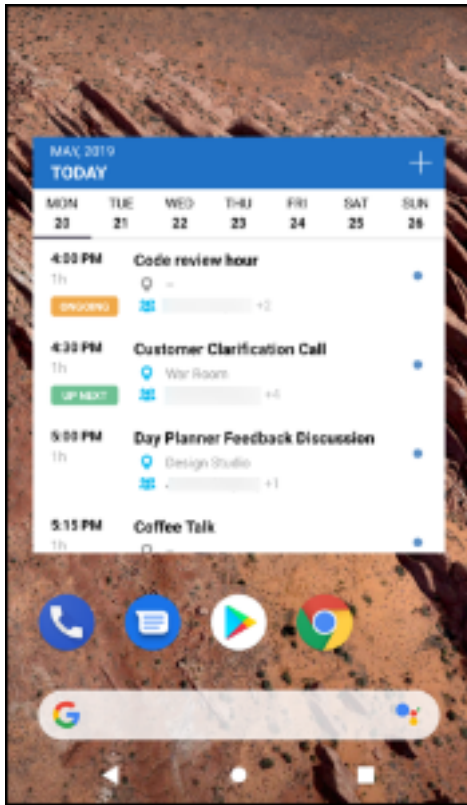
Android 용 Secure Mail

- **일정 이벤트 끌어서 놓기.** Android 용 Secure Mail 에서 이벤트를 끌어서 놓는 방법으로 기존 일정 이벤트의 시간을 변경할 수 있습니다. 이 일정 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [일정 이벤트 시간 변경](#)을 참조하십시오.
- **반응형 전자 메일 지원.** Android 용 Secure Mail 이 반응형 전자 메일을 제공하도록 최적화되었습니다. 이전에는 큰 테이블이나 이미지가 포함된 전자 메일 내용이 잘못 렌더링되었습니다. 이 기능은 전자 메일의 형식과 크기에 관계없이 지원되는 모든 장치에서 전자 메일 내용을 더 쉽게 읽을 수 있도록 합니다.

- **Secure Mail**의 연락처 사진. Android 용 Secure Mail 에서 전자 메일 또는 모임 초대에 받는 사람을 추가할 때 연락처 이미지를 볼 수 있습니다. 연락처의 이미지가 이름 옆에 표시됩니다. 이름이 같은 사람이 여러 명인 경우 전자 메일 또는 모임 초대에 받는 사람을 추가할 때 이미지가 있으면 받는 사람을 올바르게 식별하는 데 도움이 됩니다. 로컬로 저장되지 않은 연락처를 검색하려는 경우 받는 사람의 이름을 4 자 이상 입력하면 이미지가 표시됩니다.



- 일정 목록에 대한 위젯. Android 용 Secure Mail 에서 일정 목록을 위젯으로 사용할 수 있습니다. 이 위젯에서 일정한 주 동안 예정된 이벤트를 볼 수 있습니다. 이 기능을 사용하면 일정 이벤트를 만들고 기존 이벤트를 보고 세부 정보를 편집할 수 있습니다. 홈 화면에 배치된 위젯에는 화면 캡처 차단 정책이 적용되지 않습니다. 그러나 일정 목록 위젯 허용 정책을 사용하여 위젯을 사용하지 않도록 설정할 수 있습니다.



Secure Mail 19.5.5

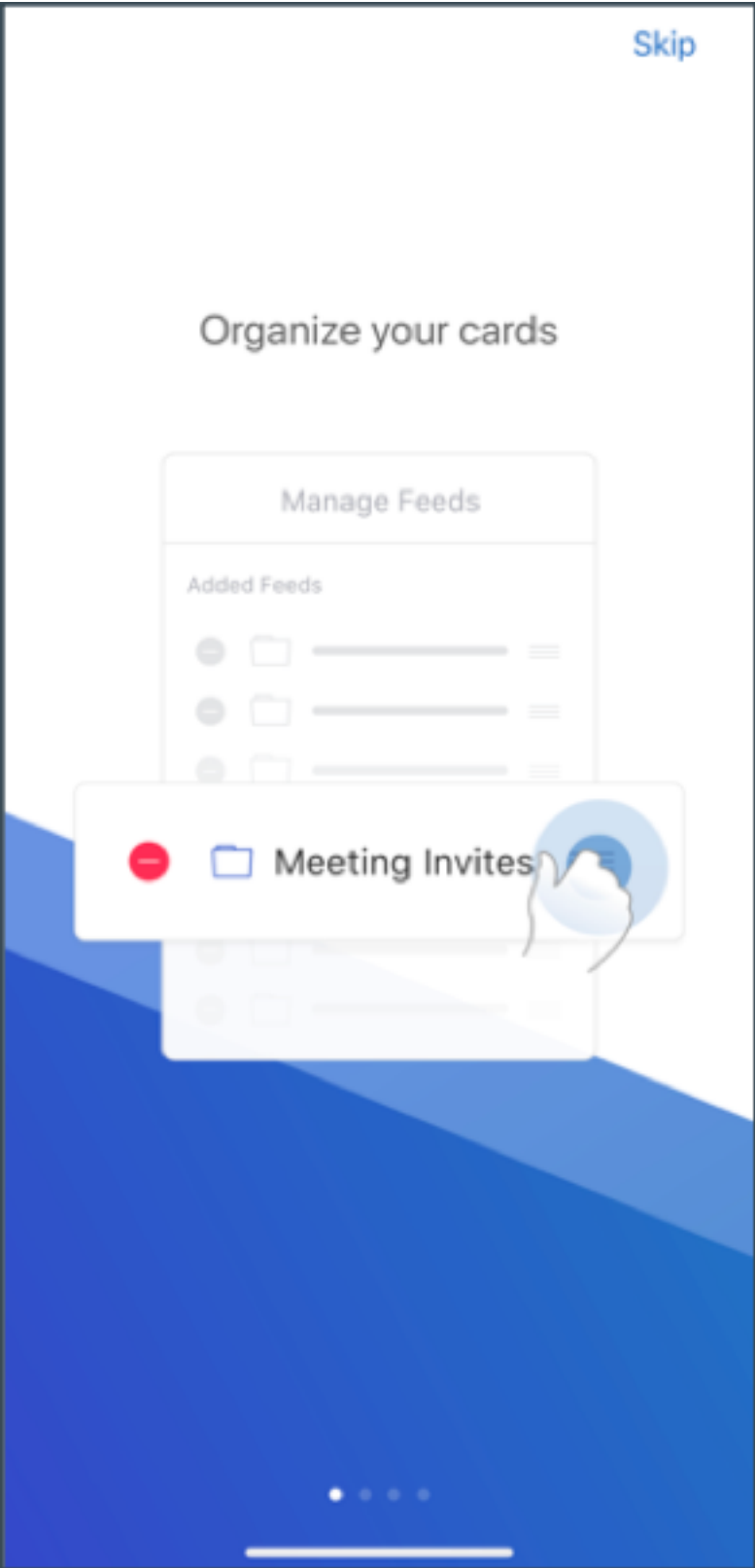
Android 용 Secure Mail Android 용 Secure Mail 버전 19.5.5에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다. 해결된 문제 및 알려진 문제 목록은 [알려진 문제](#)와 [수정된 문제](#)를 참조하십시오.

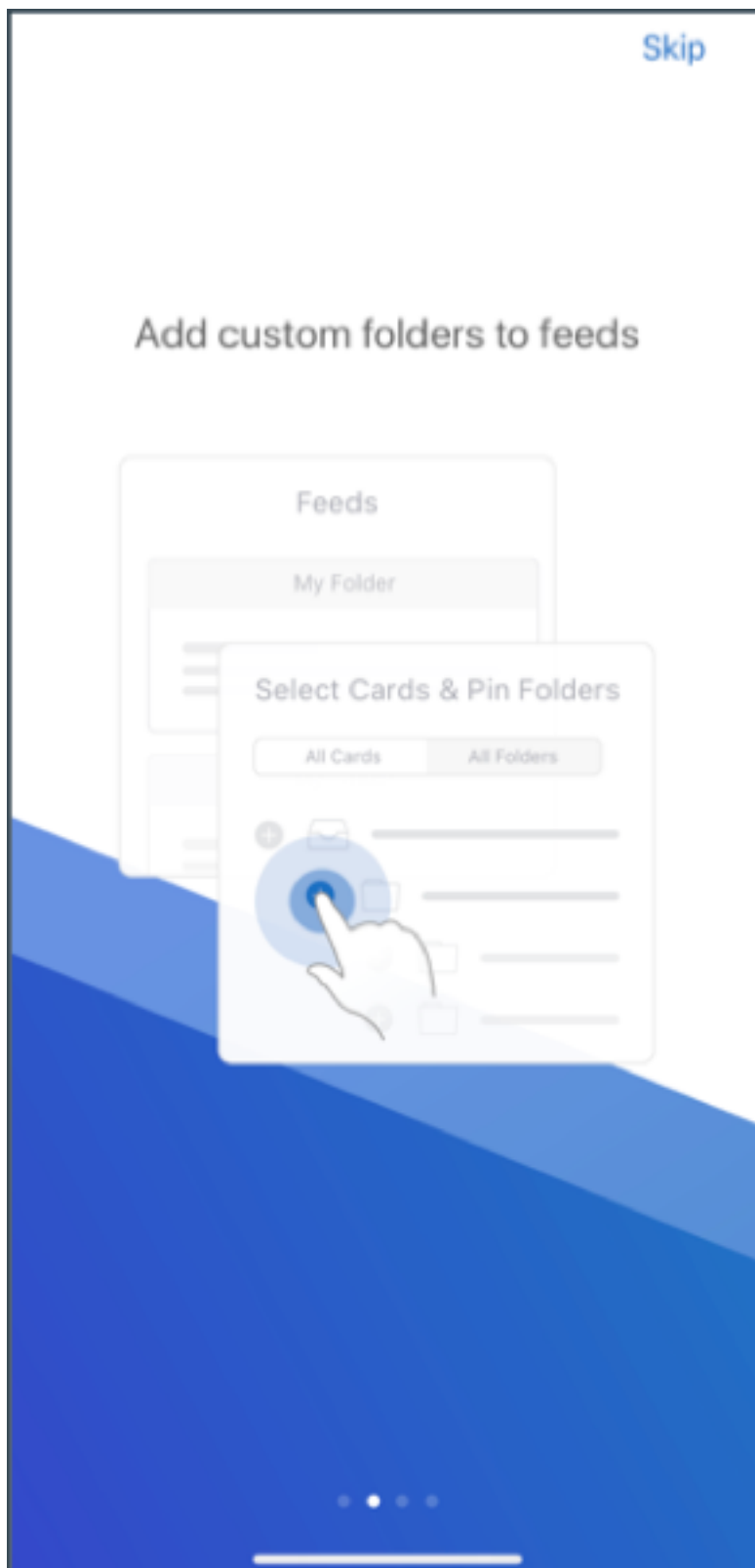
iOS 용 Secure Mail

- iOS 용 Secure Mail은 MDM + MAM 모드에서 Microsoft Intune을 사용할 때 Single Sign-on을 지원합니다. 이 기능을 사용하려면 장치에 Microsoft Authenticator 앱이 설치되어 있어야 합니다. Microsoft Authenticator 앱은 앱 스토어에서 얻을 수 있습니다.
- **Slack EMM** 지원: Slack EMM은 EMM(엔터프라이즈 모바일리티 관리)을 사용하는 Slack 고객을 위해 제공됩니다. iOS 용 Secure Mail은 응용 프로그램 **Slack EMM**을 지원하며, 이를 통해 관리자가 Secure Mail을 **Slack** 앱과 통합할지 아니면 **Slack EMM** 앱과 통합할지 선택할 수 있습니다.

Secure Mail 19.5.0

Android 용 Secure Mail 피드 관리. Android 용 Secure Mail에서 필요에 따라 피드 카드를 구성할 수 있습니다.





피드 관리에 대한 자세한 내용은 [피드 관리](#)를 참조하십시오.

임시 보관함 폴더 자동 동기화. Android 용 Secure Mail 에서 임시 보관함 폴더가 자동으로 동기화되고 모든 장치에서 임시 보관함을 사용할 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [임시 보관함 폴더 자동 동기화](#)를 참조하십시오.

Android 용 Secure Mail 19.4.6, 19.4.5 및 19.3.5

이러한 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

해결된 문제 및 알려진 문제 목록은 [알려진 문제와 수정된 문제](#)를 참조하십시오.

Secure Mail 19.3.0

이 릴리스부터 Secure Mail 이 다음과 같은 서버에 대한 지원을 포함합니다.

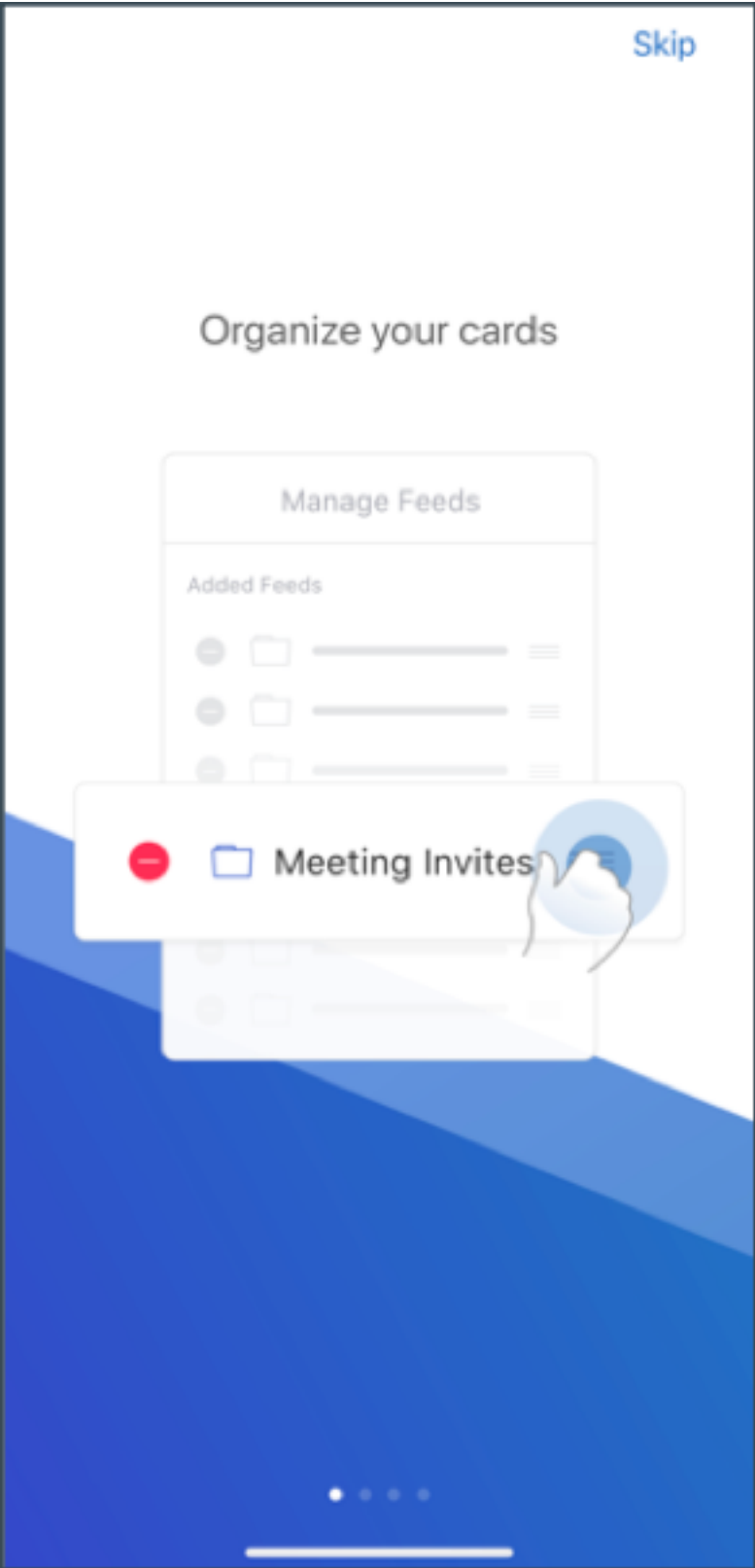
- Exchange Server 2019 누적 업데이트 1
- Exchange Server 2016 누적 업데이트 12
- Exchange Server 2013 누적 업데이트 22
- Exchange Server 2010 SP3 업데이트 롤업 26

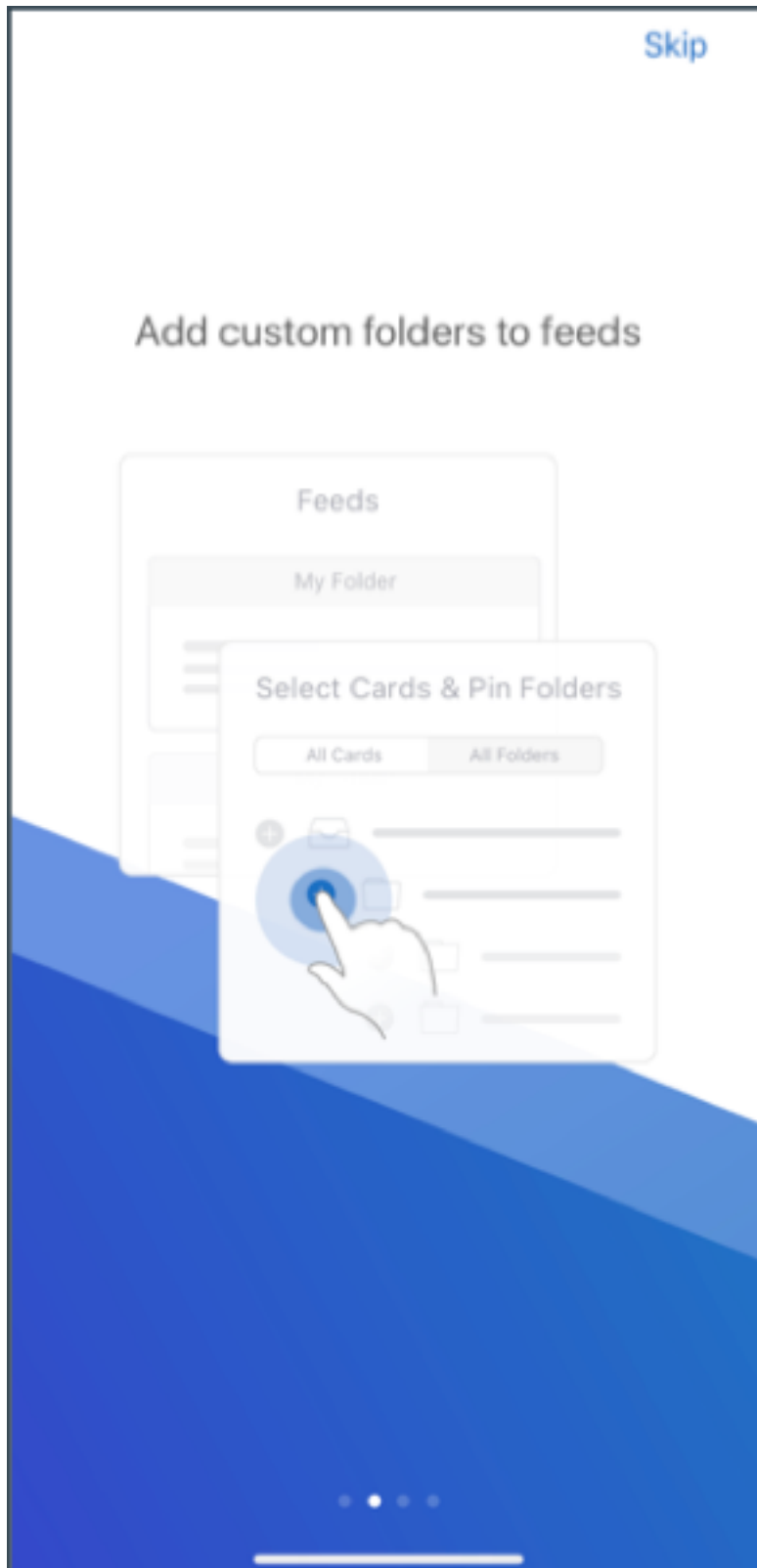
Secure Mail 서버 호환성 전체 목록에 대한 자세한 내용은 [Secure Mail 개요](#)를 참조하십시오.

iOS 용 Secure Mail 피드 관리. 이제 iOS 용 Secure Mail 에서 필요에 따라 피드 카드를 구성할 수 있습니다.

참고:

이 기능은 iPad 에서 사용할 수 없습니다.





피드 관리에 대한 자세한 내용은 [피드 관리](#)를 참조하십시오.

iOS 및 Android 용 Secure Mail 내부 도메인. 외부 조직에 속한 전자 메일 받는 사람을 식별하고 편집할 수 있습니다. 이 기능을 사용하려면 Citrix Endpoint Management 에서 내부 도메인 정책을 사용하도록 설정했는지 확인합니다.

전자 메일을 작성하거나, 회신하거나, 전달할 때 외부 받는 사람이 메일 그룹에서 강조 표시됩니다. 연락처 아이콘이 화면 왼쪽 아래에 경고로 나타납니다. 연락처 아이콘을 눌러 메일 그룹을 수정합니다.

Cancel

New Message

Send

To: john@citrix.com, john@outlook.com

Cc: john@yahoo.com |

+

Bcc: abc@citrix.com abc@gmail.com

Subject:

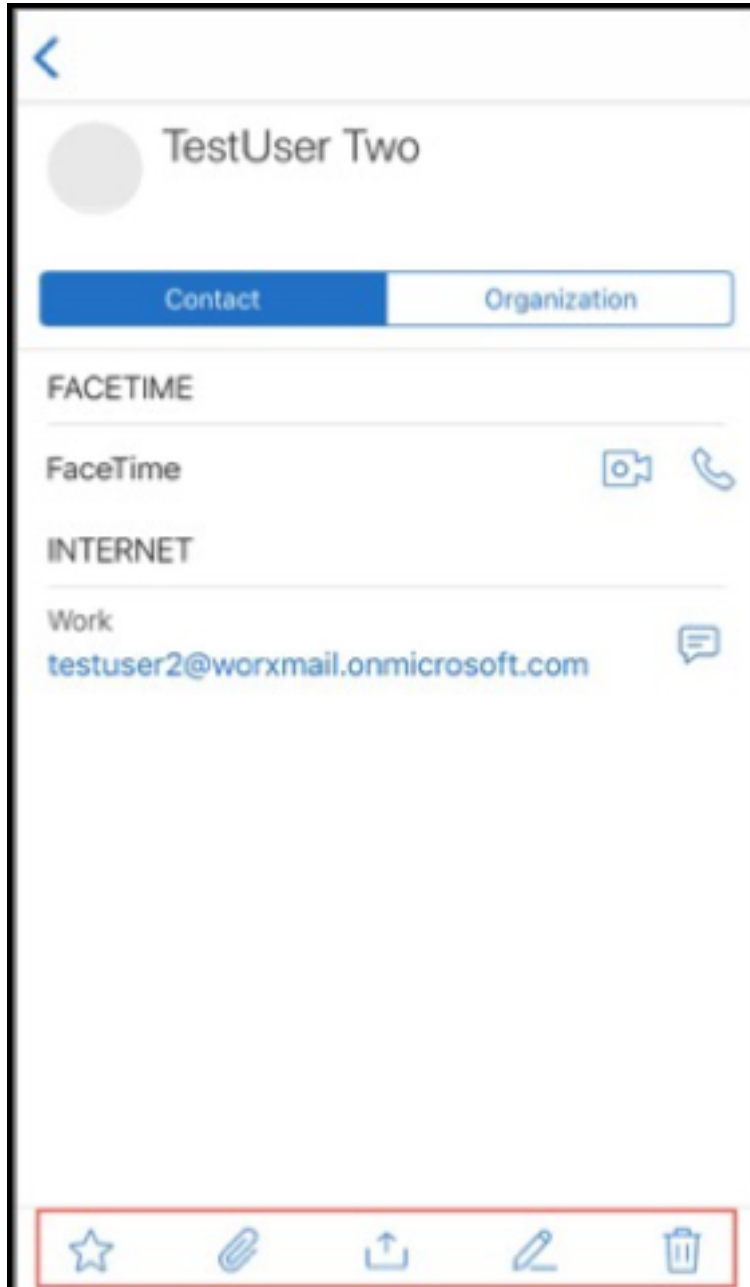
!

내부 도메인에 대한 자세한 내용은 [내부 도메인](#)을 참조하십시오.

인체공학적 개선 사항. 작업 단추가 화면 상단에서 하단으로 이동되어 쉽게 액세스할 수 있게 되었습니다. 이러한 변경 사항은 받은 편지함, 일정 및 연락처 화면에 적용됩니다.

참고:

Android 를 실행하는 장치에서 받은 편지함 및 일정 화면이 변경됩니다.



인체공학적 개선 사항 대한 자세한 내용은 [인체공학적 개선 사항](#)을 참조하십시오.

Secure Mail 19.2.0

iOS 용 Secure Mail 이 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

해결된 문제 및 알려진 문제 목록은 [알려진 문제와 수정된 문제](#)를 참조하십시오.

Android 용 Secure Mail

- **연락처 기능 개선.** Android 용 Secure Mail 에서 연락처를 누르고 연락처를 선택하면 해당 연락처의 세부 정보가 연락처 탭에 나타납니다. 조직 탭을 누르면 관리자, 직속 부하 및 동료 같은 조직 계층 세부 정보가 나타납니다. 화면 오른쪽의 자세히 아이콘을 누르면 다음 옵션이 나타납니다.

- 메일에 첨부
- 공유
- 삭제

조직 탭에서 관리자, 직속 부하 또는 동료 오른쪽의 자세히 아이콘을 누릅니다. 그런 다음 전자 메일 또는 일정 초대장을 만듭니다. 전자 메일 또는 일정 이벤트의 받는 사람: 필드에는 관리자, 직속 부하 또는 동료의 세부 정보가 자동으로 입력됩니다.

필수 구성 요소:

Exchange Server 에서 EWS(Exchange 웹 서비스) 가 사용되도록 설정되었는지 확인합니다.

연락처 세부 정보는 Active Directory 에서 가져온 조직 세부 정보를 기반으로 나타납니다. 연락처에 대한 정확한 세부 정보를 표시하려면 관리자가 Active Directory 에서 조직 계층을 구성했는지 확인합니다.

참고:

이 기능은 IBM Lotus Notes 서버에서 지원되지 않습니다.

- **네트워크 액세스 정책.** Android 용 Secure Mail 에서 터널링됨 - 웹 **SSO** 라는 새 옵션이 네트워크 액세스 MDX 정책에 추가되었습니다. 이 정책을 구성하면 터널링됨-웹 SSO 및 STA(Secure Ticket Authority) 를 통해 내부 트래픽을 동시에 유연하게 터널링할 수 있습니다. 또한 NTLM, Okta, Kerberos 등과 같은 인증 서비스에 대해 터널링됨-웹 SSO 연결을 허용할 수 있습니다. STA 를 처음 구성할 때 서비스 주소의 개별 FQDN 및 포트를 백그라운드 네트워크 서비스 정책에 추가해야 합니다. 하지만 터널링됨 - 웹 **SSO** 옵션을 구성하는 경우 이러한 구성이 필요하지 않습니다.

Citrix Endpoint Management 콘솔에서 Android 용 Secure Mail 에 대해 이 정책을 사용하도록 설정하려면:

1. Android 용.mdx 파일을 다운로드하여 사용합니다. 자세한 내용은 [MDX 앱 추가](#)의 단계를 참조하십시오.
2. 네트워크 액세스 정책에서 터널링됨-웹 **SSO** 옵션을 클릭합니다. 자세한 내용은 [앱 네트워크 액세스](#)를 참조하십시오.

iOS 용 Secure Mail 19.1.6

이 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

Secure Mail 19.1.5

이 릴리스부터 Secure Mail 이 다음과 같은 서버에 대한 지원을 포함합니다.

- Exchange Server 2016 누적 업데이트 11
- Exchange Server 2010 SP3 업데이트 롤업 24

Secure Mail-서버 호환성의 전체 목록에 대한 자세한 내용은 [Secure Mail 개요](#)를 참조하십시오.

Secure Mail 19.1.0

iOS 용 Secure Mail

- 연락처 기능 개선. iOS 용 Secure Mail 에서 연락처를 누르고 연락처를 선택하면 해당 연락처의 세부 정보가 연락처 탭에 나타납니다. 조직 탭을 누르면 관리자, 직속 부하 및 동료 같은 조직 계층 세부 정보가 나타납니다. 화면 오른쪽의 자세히 아이콘을 누르면 다음 옵션이 나타납니다.

- 편집
- VIP 에 추가
- 취소

조직 탭에서 관리자, 직속 부하 또는 동료 오른쪽의 자세히 아이콘을 누를 수 있습니다. 이 작업을 수행하여 전자 메일 또는 일정 이벤트를 만들 수 있습니다. 전자 메일 또는 일정 이벤트의 받는 사람: 필드에는 관리자, 직속 부하 또는 동료의 세부 정보가 자동으로 입력됩니다. 전자 메일을 작성하고 보낼 수 있습니다.

필수 구성 요소:

Exchange Server 에서 EWS(Exchange 웹 서비스) 가 사용되도록 설정되었는지 확인합니다.

연락처 세부 정보는 Active Directory 에서 가져온 조직 세부 정보 (Outlook 연락처) 를 기반으로 나타납니다. 연락처에 대한 정확한 세부 정보를 표시하려면 관리자가 Active Directory 에서 조직 계층을 구성했는지 확인합니다.

참고:

이 기능은 IBM Lotus Notes 서버에서 지원되지 않습니다.

- 모임 시간 및 위치를 기본 일정으로 내보내기. iOS 용 Secure Mail 에서 모임 시간, 위치이라는 새로운 값이 일정 내보내기 MDX 정책에 추가되었습니다. 이 개선을 통해 Secure Mail 일정 이벤트의 모임 시간 및 위치를 기본 일정으로 내보낼 수 있습니다.
- iOS 용 Secure Mail 은 Microsoft EMS(Enterprise Mobility + Security)/Intune 및 최신 인증 (O365) 을 실행하는 설정에서 서식 있는 푸시 알림을 지원합니다.

서식 있는 푸시 알림 기능을 사용하려면 다음 사전 요구 사항을 충족해야 합니다.

- Endpoint Management 콘솔에서 푸시 알림을 켜짐으로 설정합니다.

- 네트워크 액세스 정책이 제한 없음으로 설정되어 있습니다.
- 잠긴 화면 알림 제어 정책이 허용 또는 전자 메일 보낸 사람 또는 이벤트 제목으로 설정되어 있습니다.
- **Secure Mail** > 설정 > 알림으로 이동하여 메일 알림을 사용하도록 설정합니다.
- Secure Mail 사용자는 Zoom 앱을 사용하여 모임에 참가할 수 있습니다. Zoom 앱을 사용하는 데 필요한 정책을 구성하는 방법에 대한 자세한 내용은 [일정에서 모임 참가](#)를 참조하십시오.
- 이 릴리스에는 iPad Pro 11 인치 및 iPad Pro 12.9 인치에 대한 지원이 포함됩니다.

Android 용 Secure Mail

- 첨부 파일 기능 개선. Android 용 Secure Mail에서는 첨부 파일을 간편하게 볼 수 있습니다. 사용자 경험을 개선하기 위해 불필요한 단계를 제거했지만 이전 릴리스의 첨부 파일 옵션은 유지했습니다.

Secure Mail 앱 내에서 첨부 파일을 볼 수 있습니다. Secure Mail 을 사용하여 볼 수 있는 첨부 파일은 직접 열립니다. Secure Mail 을 사용하여 첨부 파일을 볼 수 없는 경우 앱 목록이 나타납니다. 필요한 앱을 선택하여 첨부 파일을 볼 수 있습니다. 자세한 내용은 [첨부 파일 보기](#)를 참조하십시오.
- Secure Mail 사용자는 Zoom 앱을 사용하여 모임에 참가할 수 있습니다. Zoom 앱을 사용하는 데 필요한 정책을 구성하는 방법에 대한 자세한 내용은 [일정에서 모임 참가](#)를 참조하십시오.
- 모임 시간 및 위치를 기본 일정으로 내보내기. Android 용 Secure Mail 에서 모임 시간, 위치라는 값이 일정 내보내기 MDX 정책에 추가되었습니다. 이 값을 사용하면 Secure Mail 일정 이벤트의 모임 시간 및 위치를 기본 일정으로 내보낼 수 있습니다.

참고:

Android 5.x 에 대한 지원은 2018 년 12 월 31 일에 종료되었습니다.

Secure Mail 18.12.0

이 릴리스에는 성능 개선 사항 및 버그 수정이 포함되어 있습니다.

해결된 문제 및 알려진 문제 목록은 [알려진 문제와 수정된 문제](#)를 참조하십시오.

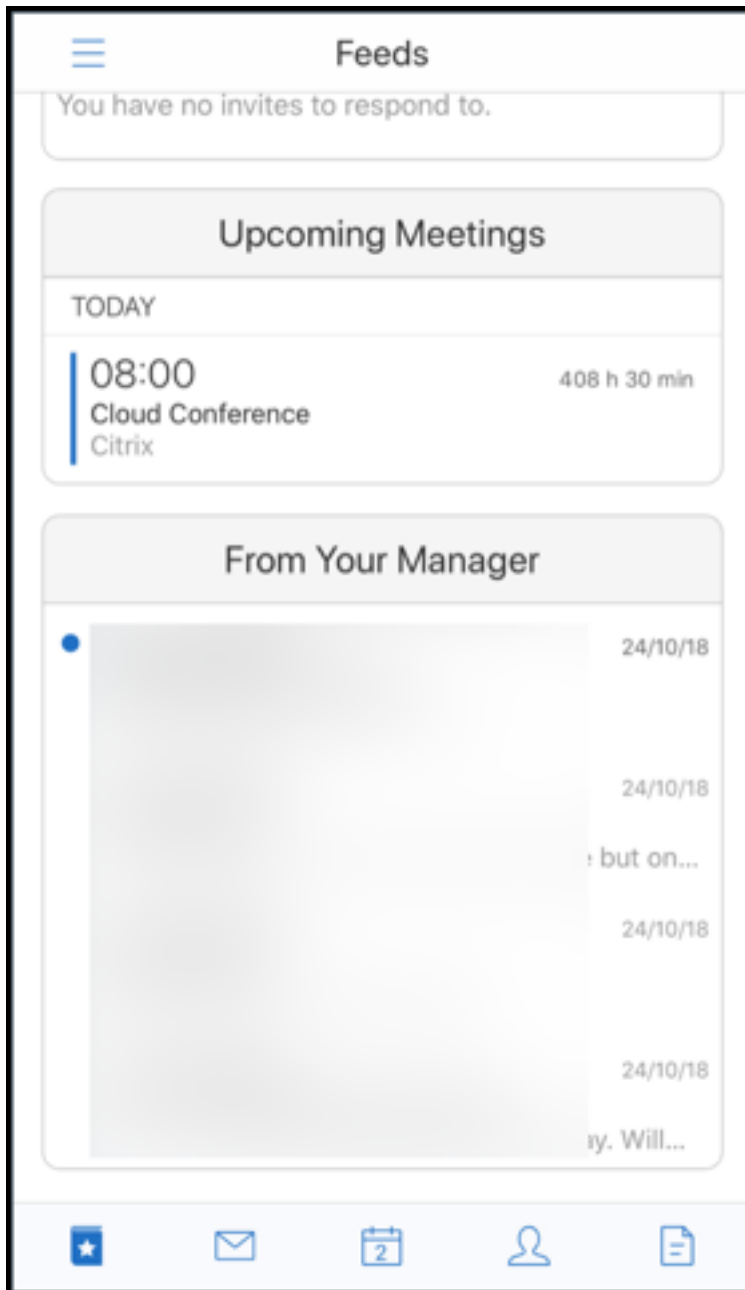
Secure Mail 18.11.5

Android 용 Secure Mail

- **ActiveSync** 헤더를 사용하여 피싱 전자 메일 보고. Android 용 Secure Mail 에서 사용자가 피싱 메일을 보고하면 EML 파일이 해당 메일의 첨부 파일로 생성됩니다. 관리자는 이 메일을 수신하고 보고된 메일에 연결된 ActiveSync 헤더를 볼 수 있습니다.

이 기능을 사용하려면 관리자가 피싱 보고 전자 메일 주소 정책을 구성하고 피싱 보고 메커니즘을 첨부 파일을 통해 보고로 설정해야 합니다. 관리자는 Citrix Endpoint Management 콘솔에서 이러한 설정을 구성합니다. Secure Mail 의 MDX 정책 구성에 대한 자세한 내용은 [모바일 생산성 앱에 대한 MDX 정책](#)을 참조하십시오.

- 전자 메일 및 일정 이벤트 인쇄. Android 용 Secure Mail 에서 Android 장치의 전자 메일 및 일정 이벤트를 인쇄할 수 있습니다. 이 인쇄 기능은 Android 인쇄 프레임워크를 사용합니다. 자세한 내용은 [전자 메일 및 일정 이벤트 인쇄](#)를 참조하십시오.
- 관리자의 피드. Android 용 Secure Mail 의 피드 화면에서 관리자의 전자 메일을 볼 수 있습니다. 관리자가 보낸 메일 피드에는 메일 동기화 기간 설정에 따라 최대 5 개의 전자 메일이 나타납니다. 더 많은 관리자 전자 메일을 보려면 모두 보기를 누릅니다.



필수 구성 요소:

Exchange Server 에서 EWS(Exchange 웹 서비스) 가 사용되도록 설정되었는지 확인합니다.

관리자 카드는 Active Directory 에서 가져온 조직 세부 정보 (Outlook 연락처) 를 기반으로 나타냅니다. 관리자 피드에 정확한 세부 정보를 표시하려면 관리자가 Active Directory 에서 조직 계층을 구성했는지 확인합니다.

참고:

이 기능은 IBM Lotus Notes 서버에서 지원되지 않습니다.

Secure Mail 18.11.1

중요:

다음 문제는 Android 용 Secure Mail 18.11.1 에서 수정되었습니다.

IBM Notes Traveler 9.0.1 SP 10 에 연결된 Android 용 Secure Mail 에서 첨부 파일이 있는 전자 메일이 보낼 편지함에 유지됩니다. [CXM-58962]

Secure Mail 18.11.0

Android 용 Secure Mail

- 하위 폴더 알림. Android 용 Secure Mail 에서 메일 계정의 하위 폴더에서 메일 알림을 받을 수 있습니다. 자세한 내용은 [하위 폴더 알림](#)을 참조하십시오.
- Android 용 Secure Mail** 의 백그라운드 서비스 업데이트. Android 8.0(API 수준 26) 이상을 실행하는 장치에서 Google Play 백그라운드 실행 제한 요구 사항을 충족하기 위해 Secure Mail 백그라운드 서비스가 업그레이드되었습니다. 장치의 메일 동기화 및 알림을 중단 없이 사용하려면 FCM(Firebase Cloud Messaging) 서비스 푸시 알림을 사용하도록 설정합니다. FCM 기반 푸시 알림 사용에 대한 자세한 내용은 [Secure Mail 을 위한 푸시 알림](#)을 참조하십시오.

장치의 Secure Mail 설정에서 메일 알림을 켜야 합니다. 이 업데이트에 대한 자세한 내용은 이 [Support Knowledge Center 문서](#)를 참조하십시오.

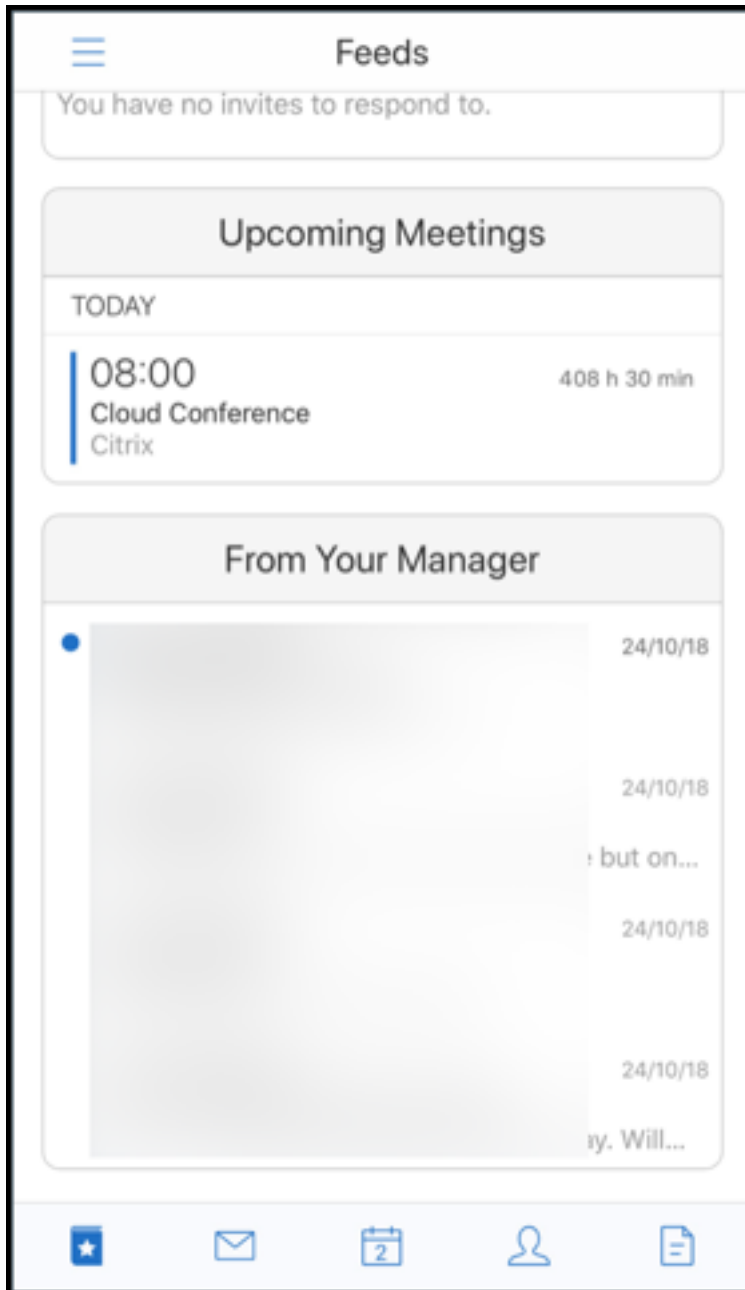
제한 사항:

- FCM 기반 푸시 알림을 사용하도록 설정하지 않은 경우 백그라운드 동기화는 15 분마다 한 번씩 발생합니다. 이 간격은 앱이 백그라운드에서 실행되는지, 아니면 전경에서 실행되는지에 따라 달라집니다.
- 사용자가 장치 설정에서 시간을 수동으로 업데이트하면 일정 위젯의 날짜가 자동으로 업데이트되지 않습니다.

iOS 용 Secure Mail

- iOS 12.1** 에 대한 지원. iOS 용 Secure Mail 은 iOS 버전 12.1 을 지원합니다.
- 풍부한 푸시 알림 실패 메시지에 대한 향상된 기능. iOS 용 Secure Mail에서는 장치의 알림 센터에 알림 실패 유형에 따라 해당하는 푸시 알림 실패 메시지가 나타납니다. 자세한 내용은 [iOS 용 Secure Mail 의 푸시 알림 실패 메시지](#)를 참조하십시오.

- 관리자의 피드. iOS 용 Secure Mail 의 피드 화면에서 관리자의 전자 메일을 볼 수 있습니다. 관리자가 보낸 메일 피드에는 메일 동기화 기간 설정에 따라 최대 5 개의 전자 메일이 나타납니다. 더 많은 관리자 전자 메일을 보려면 모두 보기를 누릅니다.



필수 구성 요소:

Exchange Server 에서 EWS(Exchange 웹 서비스) 가 사용되도록 설정되었는지 확인합니다.

관리자 카드는 Active Directory 에서 가져온 조직 세부 정보 (Outlook 연락처) 를 기반으로 나타냅니다. 관리자 피드에 정확한 세부 정보를 표시하려면 관리자가 Active Directory 에서 조직 계층을 구성했는지 확인합니다.

참고:

이 기능은 IBM Lotus Notes 서버에서 지원되지 않습니다.

Secure Mail 18.10.5

- **Secure Mail**과 **Slack** 통합 (미리 보기): 이제 iOS 또는 Android를 실행하는 장치에서 전자 메일 대화를 Slack 앱으로 보낼 수 있습니다. 자세한 내용은 [Secure Mail과 Slack 통합 \(미리 보기\)](#)를 참조하십시오.
- 피드 폴더의 향상된 기능: iOS용 Secure Mail에서 기존 피드 폴더에 다음과 같은 개선이 이루어졌습니다.
 - 피드 카드에 최대 5개의 예정된 모임이 표시됩니다.
 - 다음 24시간 동안 예정된 모임이 피드 카드에 표시되고 오늘 및 내일 섹션으로 구분됩니다.

Secure Mail 18.10.0

- 메일 및 일정 알림을 위한 **Secure Mail** 알림 채널: Android O 이상을 실행하는 장치에서 알림 채널 설정을 사용하여 이메일 및 일정 알림이 처리되는 방식을 관리할 수 있습니다. 이 기능을 통해 알림을 사용자 지정하고 관리할 수 있습니다. 자세한 내용은 [알림 채널](#)을 참조하십시오.
- 피싱 전자 메일 보고 (전달을 통해): iOS용 Secure Mail에서 피싱으로 보고 기능을 사용하여 피싱으로 의심되는 전자 메일을 전달을 통해 보고할 수 있습니다. 관리자가 정책에서 구성한 전자 메일 주소로 의심스러운 메시지를 전달하면 됩니다. 이 기능을 사용하려면 관리자가 피싱 보고 전자 메일 주소 정책을 구성하고 피싱 보고 메커니즘을 전달을 통해 보고로 설정해야 합니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [피싱 전자 메일 보고](#)를 참조하십시오.

Secure Mail 18.9.0

- “yy.mm.version” 형식의 새로운 버전 번호 지정 체계. 예를 들어 버전 **18.9.0**과 같이 지정됩니다.
- 피싱 전자 메일 보고 (전달을 통해): Android용 Secure Mail에서 피싱으로 보고 기능을 사용하여 피싱으로 의심되는 전자 메일을 전달을 통해 보고할 수 있습니다. 관리자가 구성한 전자 메일 주소로 의심스러운 메시지를 전달하면 됩니다. 이 기능을 사용하려면 관리자가 피싱 보고 전자 메일 주소 정책을 구성하고 피싱 보고 메커니즘을 전달을 통해 보고로 설정해야 합니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [피싱 전자 메일 보고](#)를 참조하십시오.
- 피드 카드의 향상된 기능: Android용 Secure Mail에서는 기존 피드 폴더에 다음과 같은 개선이 이루어졌습니다.
 - 자동으로 동기화된 모든 폴더의 모임 초대가 피드 카드에 표시됩니다.
 - 피드 카드에 최대 5개의 예정된 모임이 표시됩니다.
 - 이제 예정된 모임이 현재 시간으로부터 24시간의 기간을 기준으로 표시됩니다. 이러한 모임 초대는 오늘과 내일로 구분됩니다.이전 릴리스에서는 하루가 끝날 때까지 예정된 모임이 피드에 표시되었습니다.

- **Secure Mail** 일정 이벤트 내보내기: Android 및 iOS 용 Secure Mail 을 사용하여 Secure Mail 일정 이벤트를 장치의 기본 일정 앱으로 내보낼 수 있습니다. 이 기능을 사용하려면 설정을 누른 다음 일정 이벤트 내보내기의 슬라이더를 오른쪽으로 밀니다. 자세한 내용은 [Secure Mail 일정 이벤트 내보내기](#)를 참조하십시오.

Secure Mail 10.8.65

- **iOS 12** 에서 사용 가능: iOS 용 Secure Mail 에서 그룹 알림 기능이 지원됩니다. 이 기능을 사용하면 한 메일 스레드의 대화가 그룹화됩니다. 장치의 잠금 화면에서 그룹화된 알림을 간단히 확인할 수 있습니다. 그룹 알림 설정은 장치에서 기본적으로 사용되도록 설정되어 있습니다.
- iOS 용 Secure Mail 에서 초안 저장 및 초안 삭제 단추가 더 커졌습니다. 이러한 개선을 통해 고객이 두 단추를 더 쉽게 구별할 수 있습니다.
- iOS 용 Secure Mail 의 장치 설정에서 Secure Mail 발신자 ID 를 사용하도록 설정하여 연락처에서 걸려오는 전화를 식별할 수 있습니다. 이러한 설정을 사용하도록 설정하면 전화가 걸려올 때 장치에 해당 앱 이름과 발신자 ID 가 표시됩니다 (예: “Secure Mail 발신자 ID: Joe Jay”). 자세한 내용은 [Secure Mail 발신자 ID](#)를 참조하십시오.

Secure Mail 10.8.60

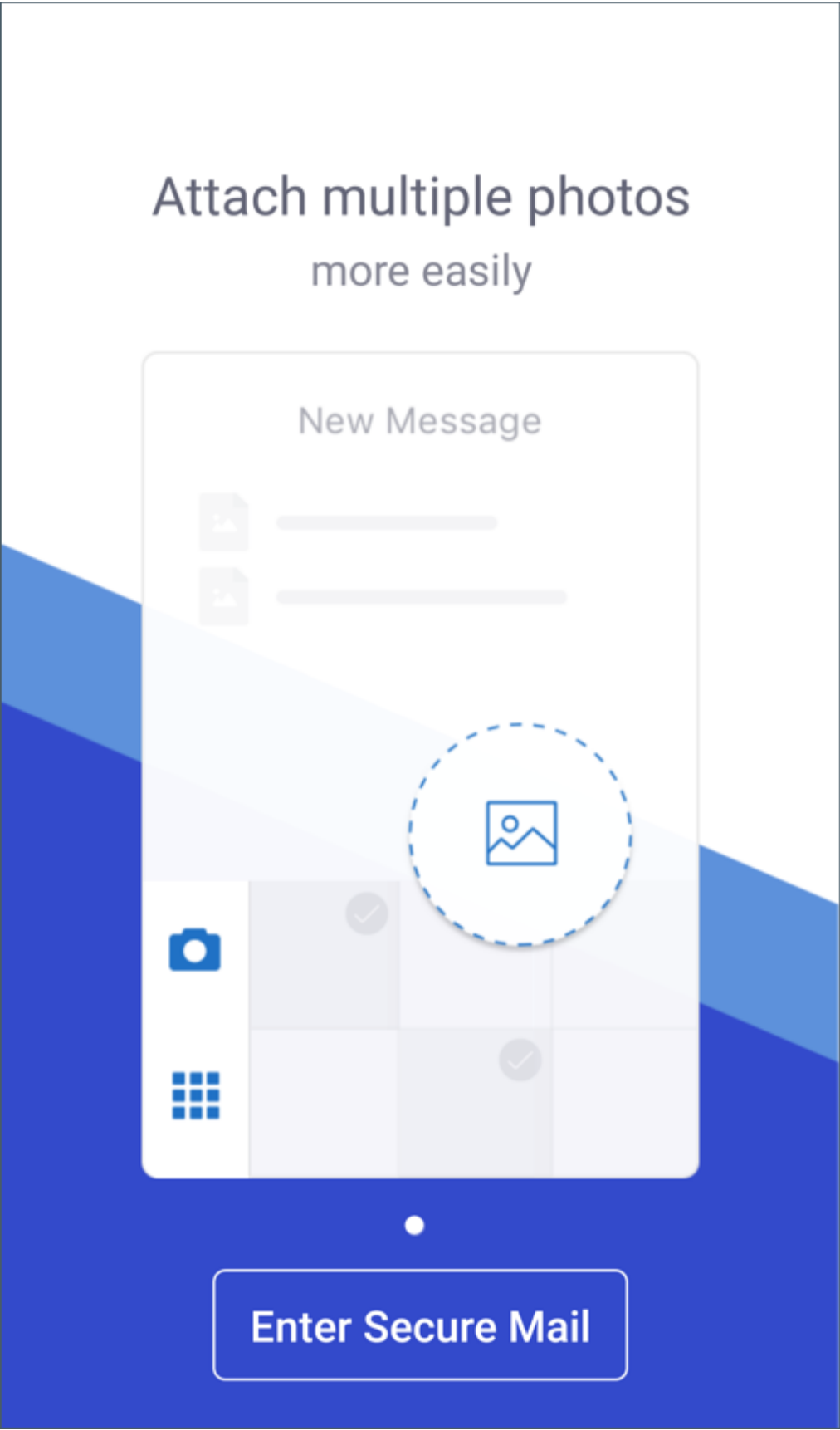
- Secure Mail 이 Android P 를 지원합니다.
- 이제 폴란드어로 Secure Mail 을 사용할 수 있습니다.
- iOS 용 Secure Mail 에서 iOS 의 기본 파일 앱을 사용하여 전자 메일에 파일을 첨부할 수 있습니다. 자세한 내용은 [iOS 기능](#)을 참조하십시오.

Secure Mail 10.8.55

Secure Mail 버전 10.8.55 에는 새로운 기능이 없습니다. 수정된 문제는 [알려진 문제와 수정된 문제](#)를 참조하십시오.

Secure Mail 10.8.50

사진 첨부 개선. iOS 용 Secure Mail 에서 새 갤러리 아이콘을 눌러 사진을 쉽게 첨부할 수 있습니다. 갤러리 아이콘을 누르고 전자 메일에 첨부할 사진을 선택합니다.

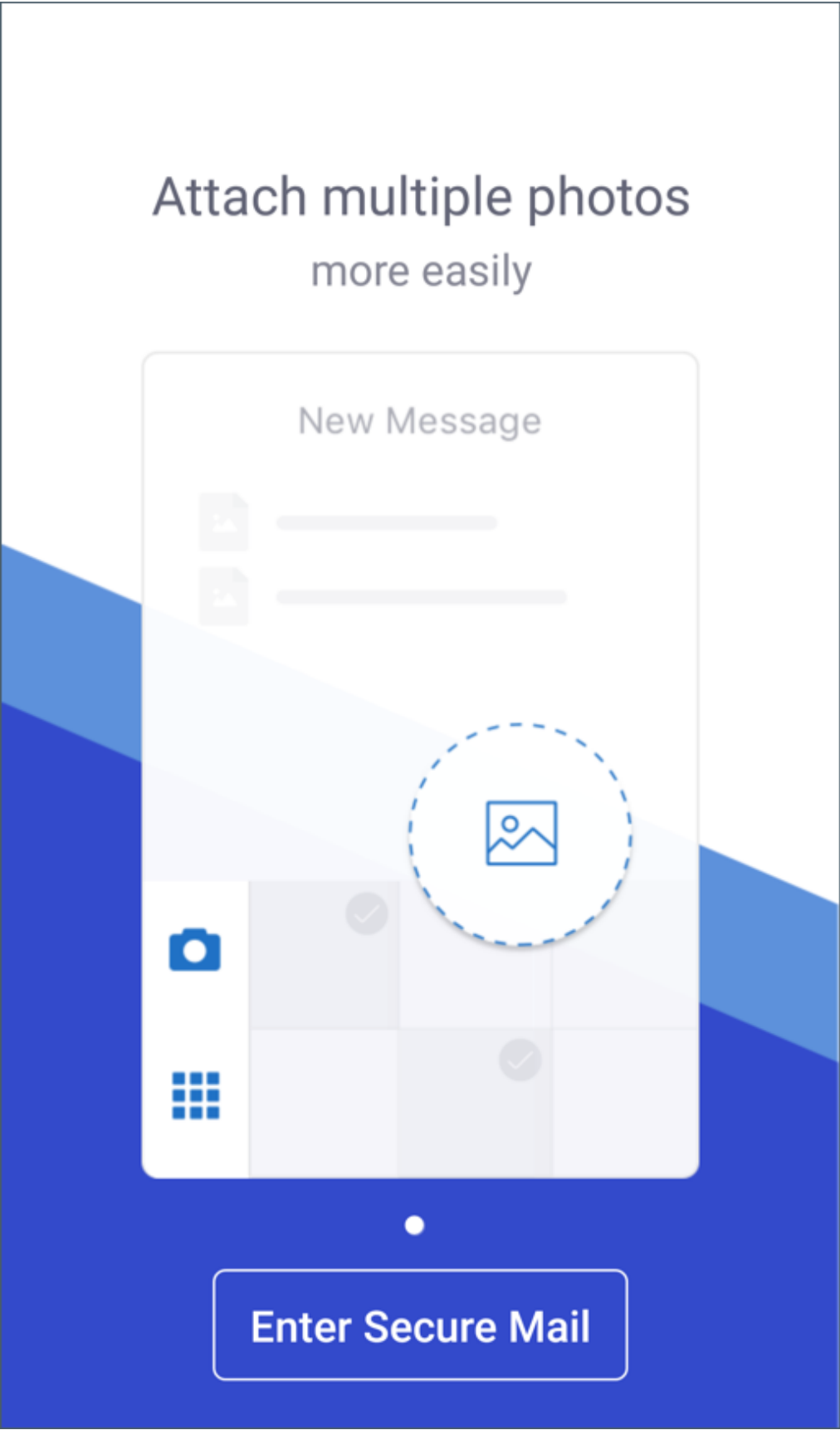


Secure Mail 피드 화면. iOS 및 Android 용 Secure Mail 의 피드 화면에 모든 읽지 않은 전자 메일, 주의가 필요한 모임 초대 및 예정된 모임이 표시됩니다.

Secure Mail 10.8.45

폴더 동기화. iOS 및 Android 용 Secure Mail 에서 동기화 아이콘을 눌러 모든 Secure Mail 콘텐츠를 새로 고칠 수 있습니다. 동기화 아이콘은 사서함, 일정, 연락처, 첨부 파일 등 Secure Mail 의 슬라이드아웃에 표시됩니다. 동기화 아이콘을 누르면 사서함, 일정, 연락처 등 자동 새로 고침을 구성한 폴더가 업데이트됩니다. 동기화 아이콘의 옆에 마지막 동기화의 타임스탬프가 표시됩니다.

사진 첨부 개선. Android 용 Secure Mail 에서 새 갤러리 아이콘을 눌러 사진을 쉽게 첨부할 수 있습니다. 갤러리 아이콘을 누르고 전자 메일에 첨부할 사진을 선택합니다.



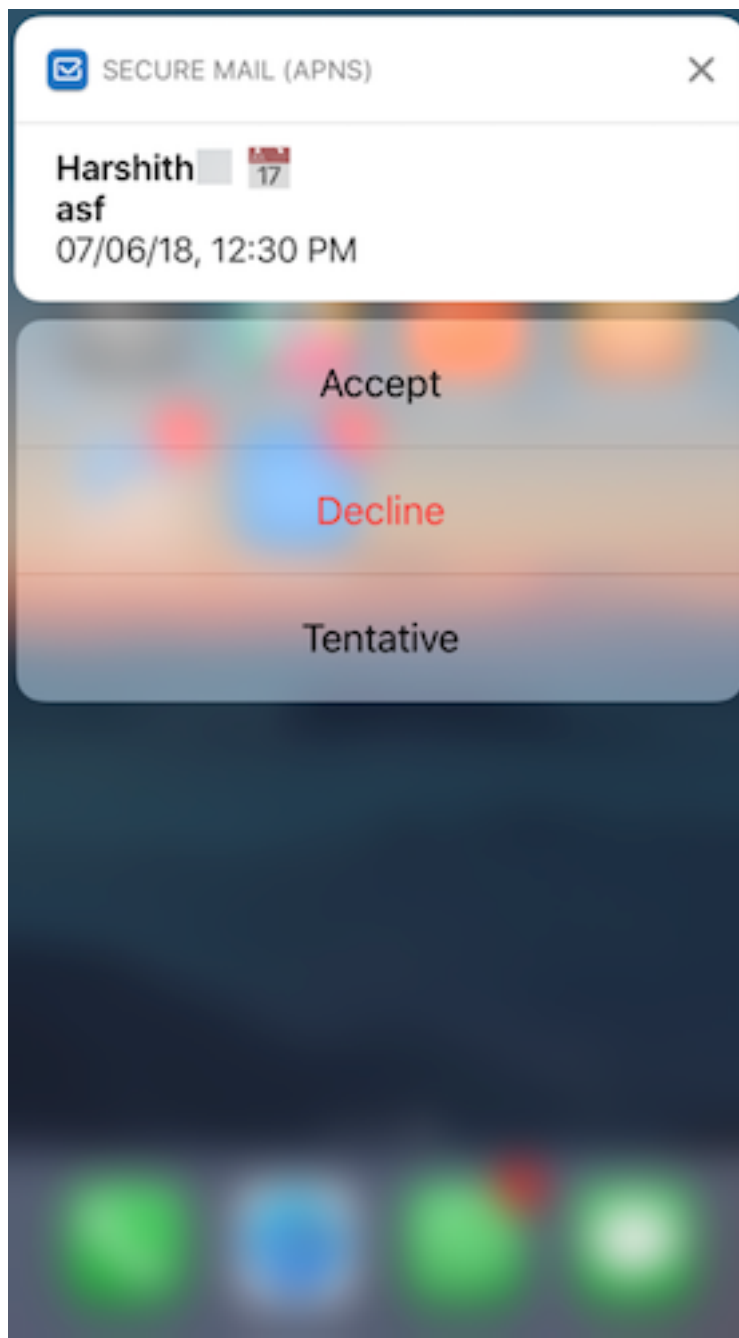
Secure Mail 10.8.40

일정 검색 지원. iOS 용 Secure Mail 에서 일정을 검색하여 이벤트, 참석자 또는 기타 텍스트를 찾을 수 있습니다.

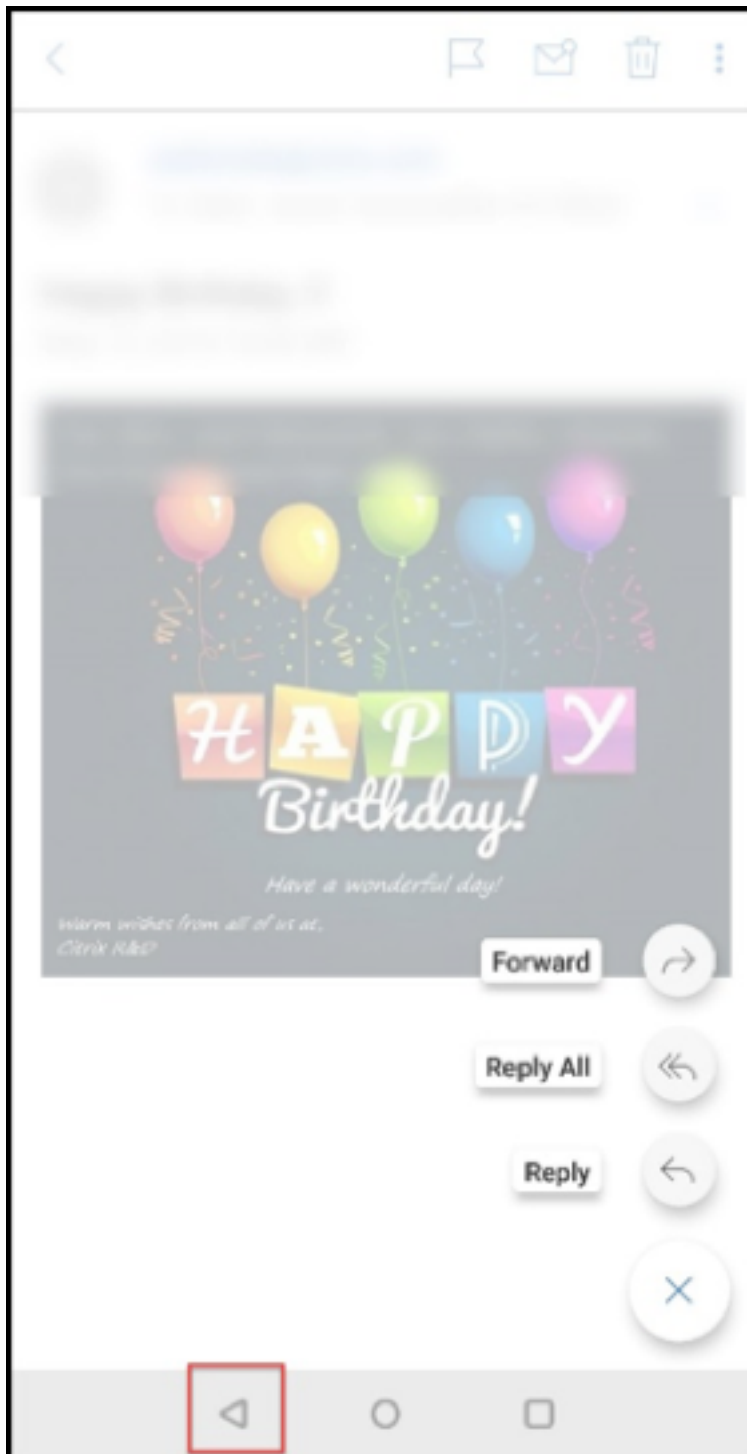
Secure Mail 10.8.35

iOS 용 Secure Mail 버전은 10.8.36 입니다.

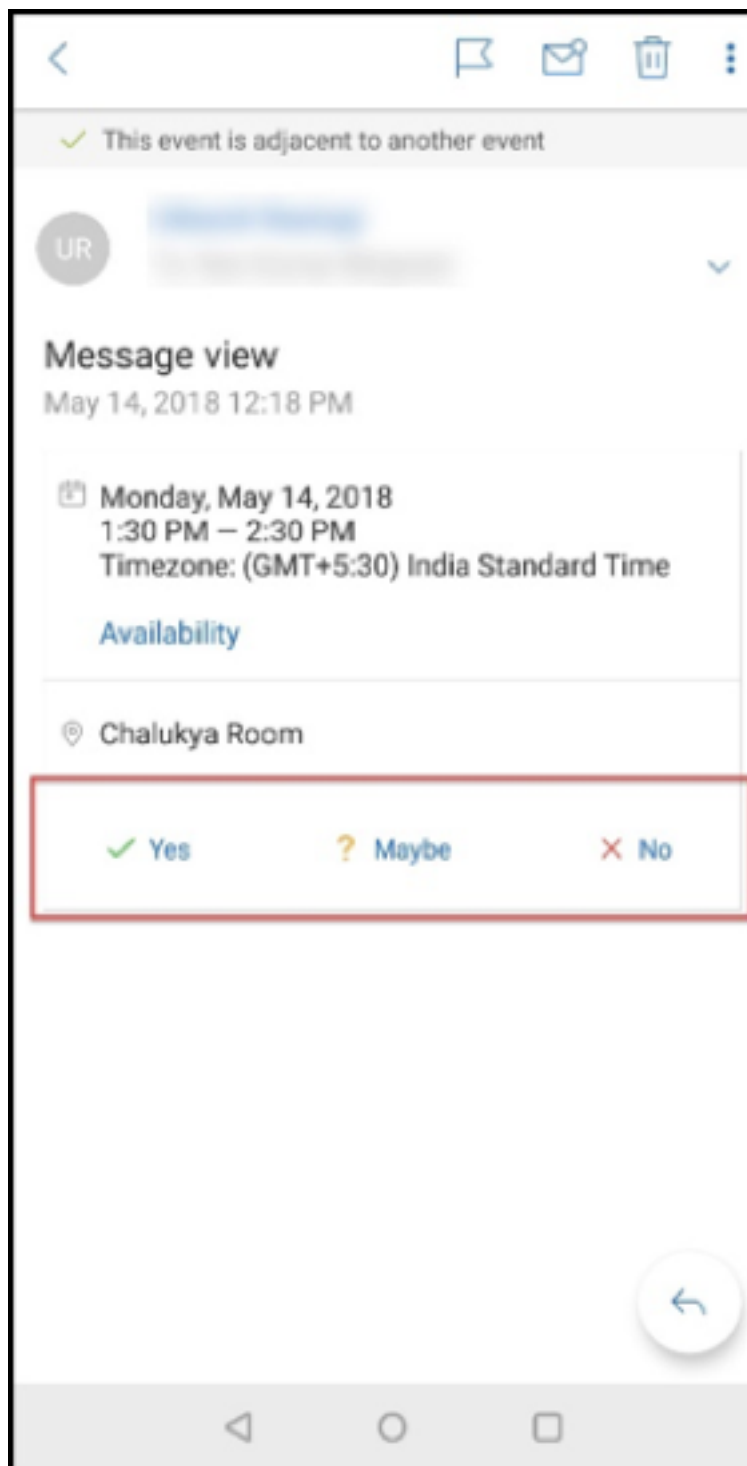
- 알림 응답 옵션. iOS 용 Secure Mail 사용자는 수락, 거부 및 미정을 사용하여 회의 알림에 응답할 수 있습니다. 또한 회신 및 삭제를 사용하여 메시지 알림에 응답할 수 있습니다.



- **Android 용 Secure Mail** 의 향상된 뒤로 단추 기능. Android 용 Secure Mail 사용자는 장치에서 뒤로 단추를 눌러 부동 작업 단추의 확장된 옵션을 해제할 수 있습니다. 부동 작업 단추가 확장된 상태에 있는 경우 장치에서 뒤로 단추를 누르면 응답 옵션이 축소됩니다. 이 작업을 수행하면 메시지 또는 이벤트 세부 정보 보기로 돌아갑니다.



- **Android 용 Secure Mail** 에서 회의 응답 단추가 전자 메일 안에 표시됩니다. 회의 초대에 대한 전자 메일 알림을 받은 경우 다음 옵션 중 하나를 눌러 초대에 응답할 수 있습니다.
 - 예
 - 나중에 결정
 - 아니요



Secure Mail 10.8.25

iOS 용 Secure Mail 에서 파생된 자격 증명에 대한 **S/MIME** 지원: 이 기능을 사용하려면 다음을 수행해야 합니다.

- 파생된 자격 증명을 S/MIME 인증서 원본으로 선택합니다. 자세한 내용은 [iOS 용 파생된 자격 증명](#)을 참조하십시오.

- Citrix Endpoint Management 에서 LDAP Attributes 클라이언트 속성을 추가합니다. 다음 정보를 사용합니다.
 - 키: SEND_LDAP_ATTRIBUTES
 - 값: `userPrincipalName=${ user.userprincipalname } ,sAMAccountName=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`

클라이언트 속성 추가 방법에 대한 단계는 XenMobile Server 의 경우 [클라이언트 속성](#)을 참조하고 Endpoint Management 의 경우 [클라이언트 속성](#)을 참조하십시오.

파생된 자격 증명을 통한 장치 등록 방법에 대한 자세한 내용은 [파생된 자격 증명을 사용하여 장치 등록](#)을 참조하십시오.

1. Endpoint Management 콘솔에서 구성 > 앱으로 이동합니다.
2. **Secure Mail** 을 선택한 다음 편집을 클릭합니다.
3. iOS 플랫폼에서 S/MIME 인증서 원본에 대해 파생된 자격 증명을 선택합니다.

Push notifications region: Americas

S/MIME certificate source: Derived Credential

Enable S/MIME during first Secure Mail startup: OFF

Calendar Web and Audio Options: GoToMeeting and User Entered

S/MIME public certificate source: Exchange

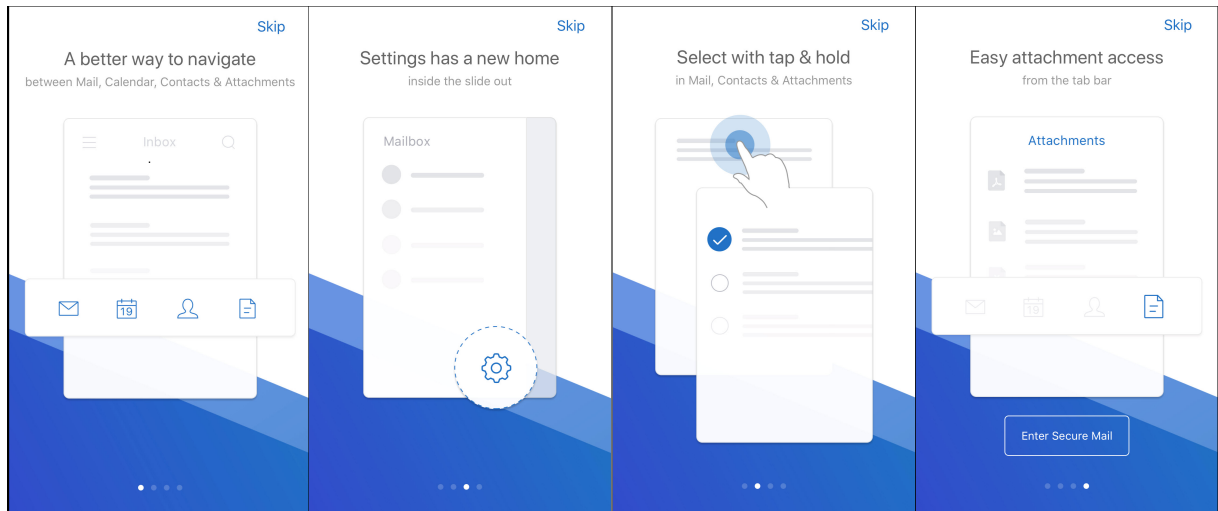
Ldap server address:

Ldap Base DN:

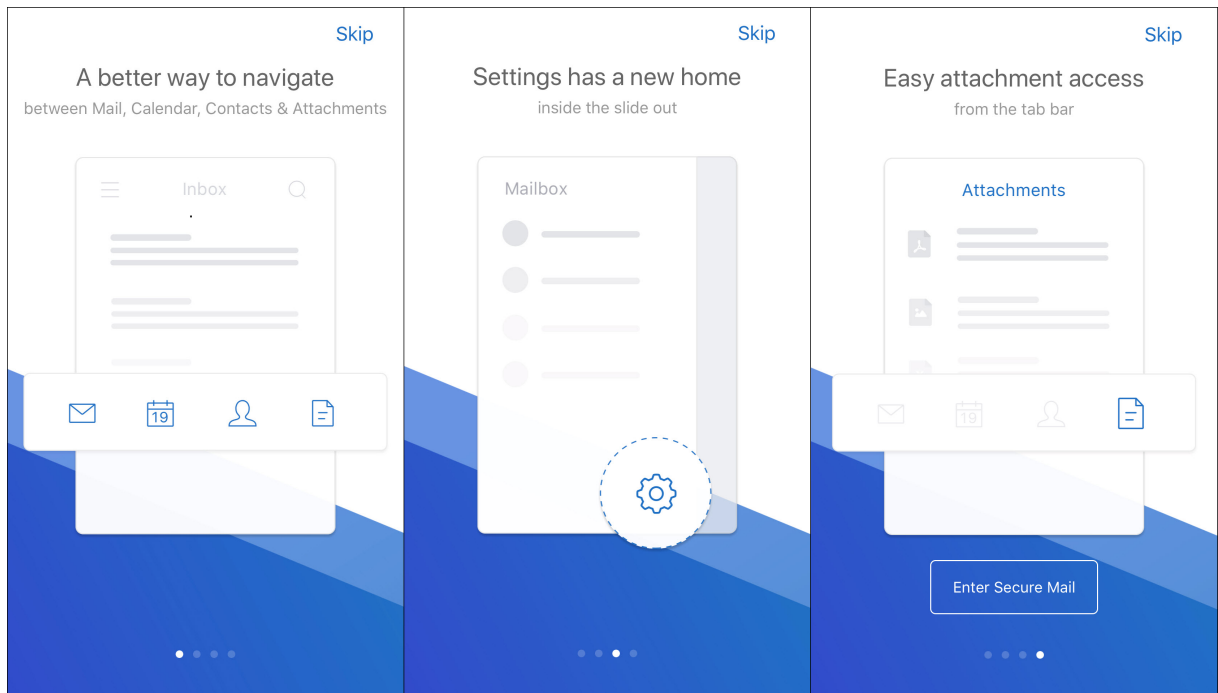
Back Next >

iOS 및 Android 용 Secure Mail 디자인 개선: 사용자 탐색이 더 간편하고 효율적으로 개선되었습니다. 메뉴 및 작업 단추가 탐색 표시줄 형태로 다시 정렬되었습니다.

다음 그림은 iOS 장치의 새로운 탐색 표시줄을 보여 줍니다.

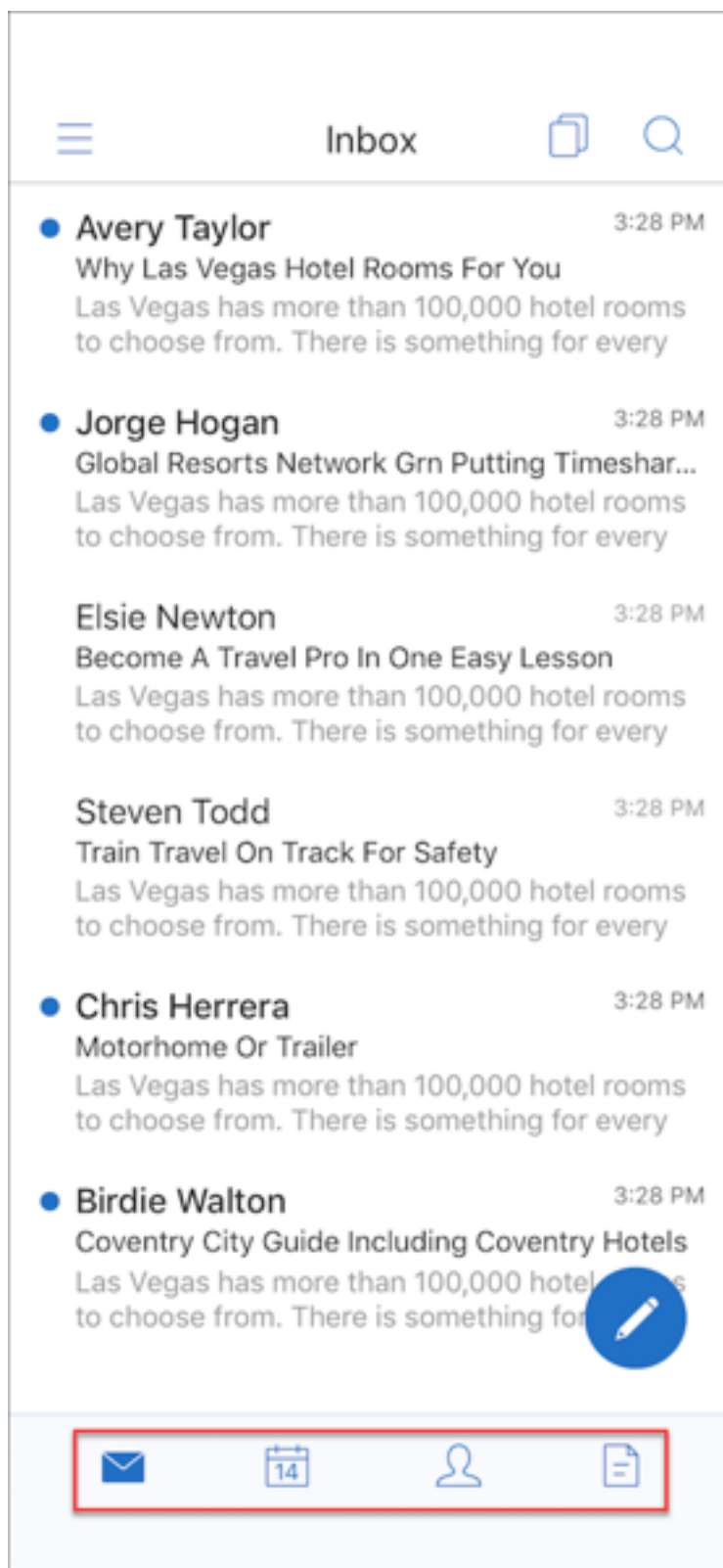


다음 그림은 Android 장치의 새로운 탐색 표시줄을 보여 줍니다.



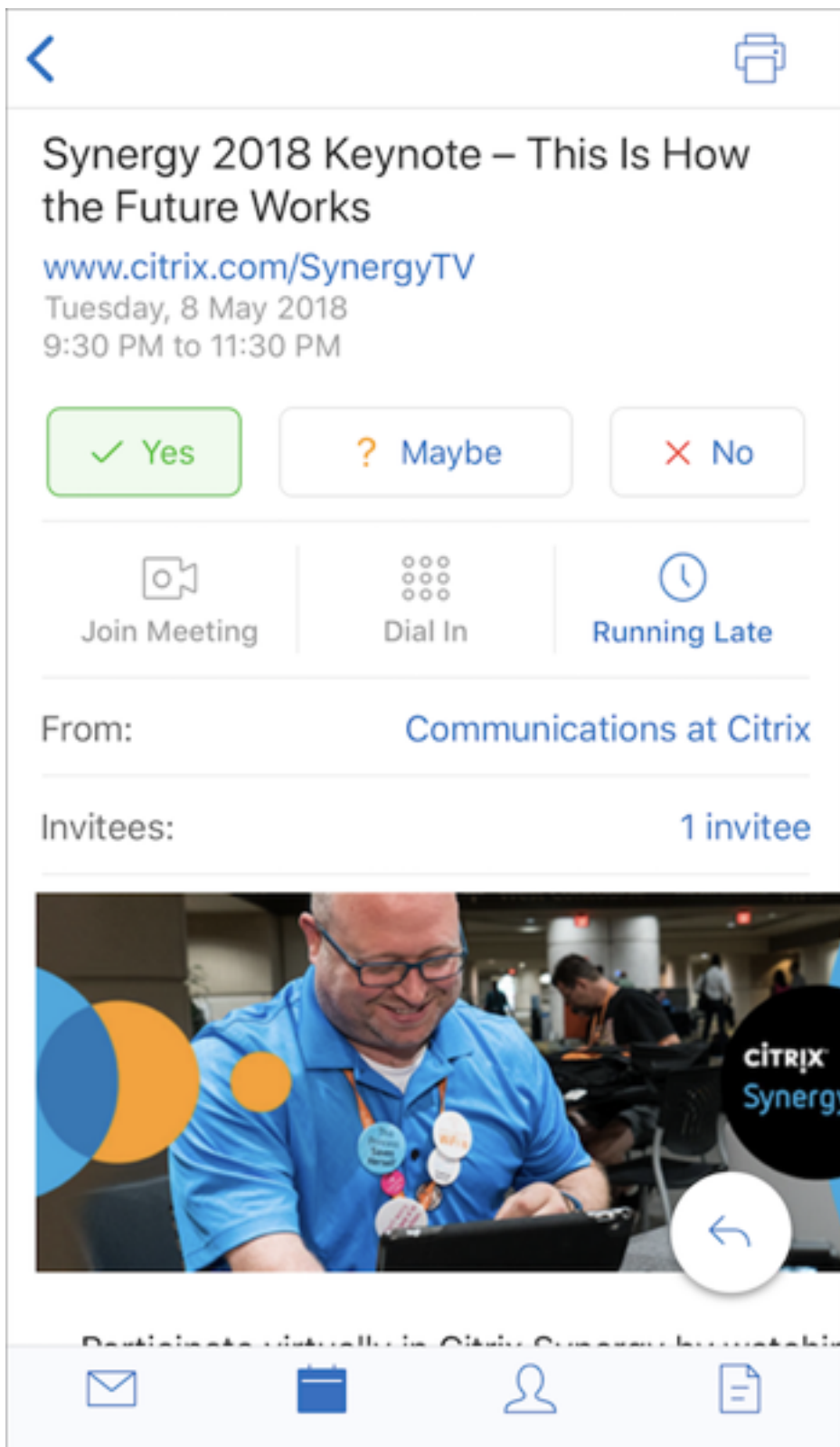
변경 내용:

- 그래버 아이콘이 제거되었습니다. Secure Mail 기능 (예: 메일, 일정, 연락처 및 첨부 파일) 이 이제 바닥글 탭 표시줄의 단추로 제공됩니다. 다음 그림은 이 변경 내용을 보여 줍니다.

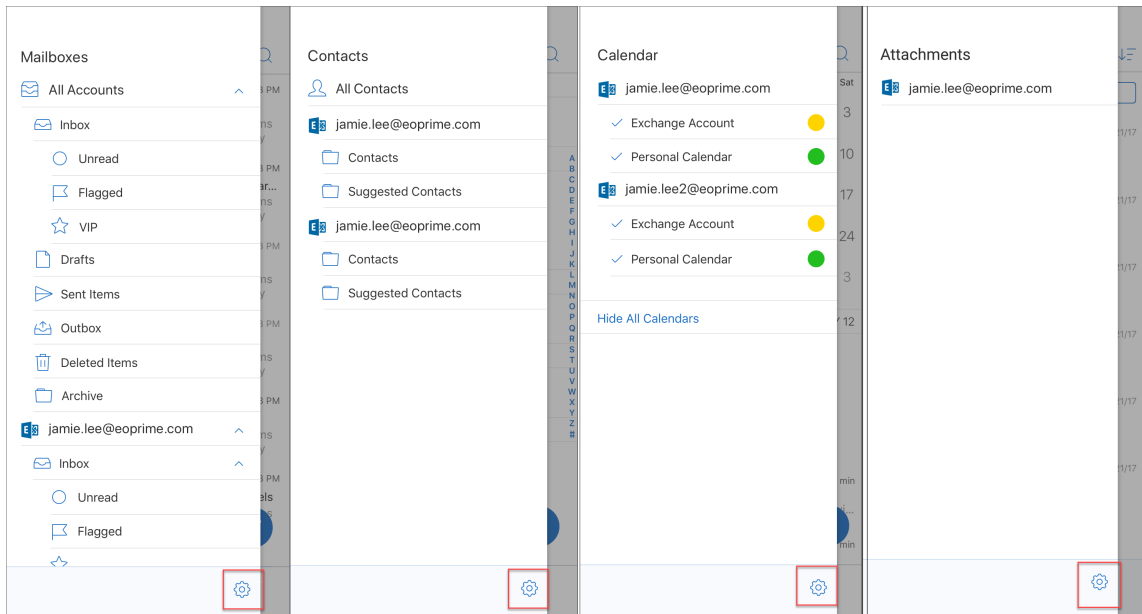


참고:

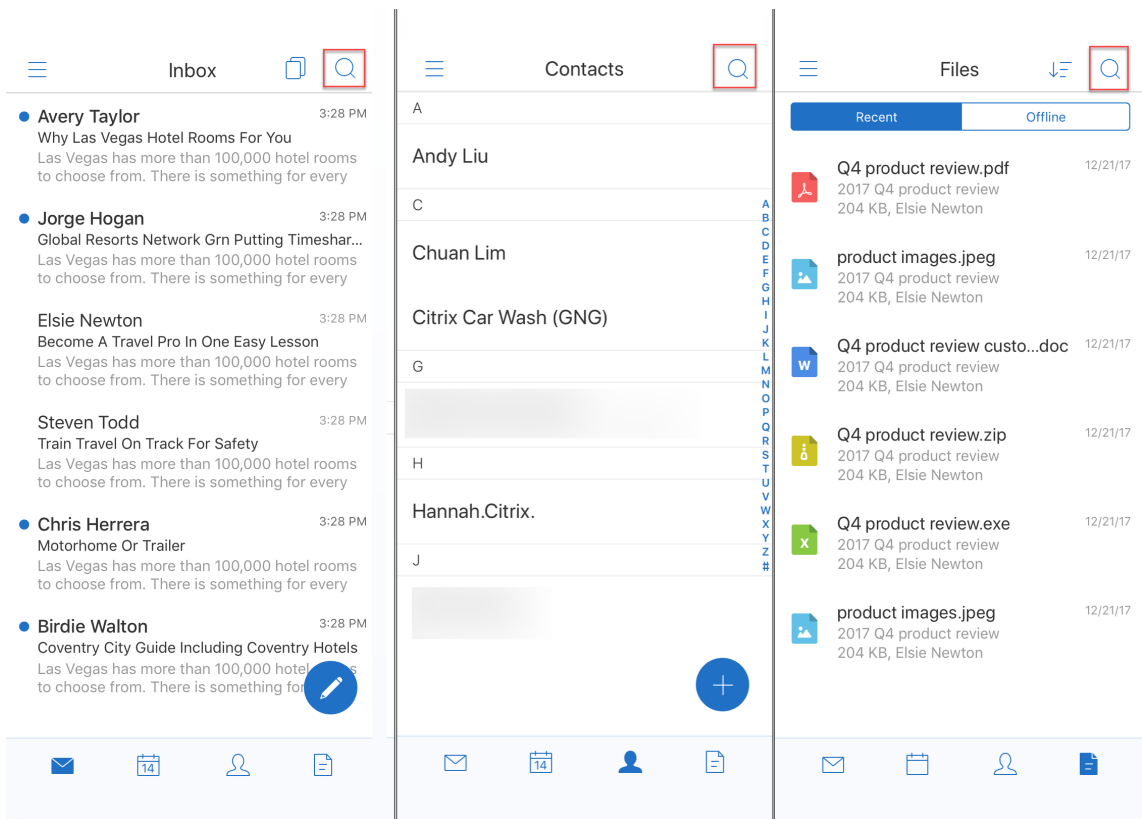
Android 장치에서는 메일 항목을 연 후 바닥글 탭 표시줄을 사용할 수 없습니다. 예를 들어 다음 그림에 표시된 것과 같이 전자 메일 또는 일정 이벤트를 열면 바닥글 탭 표시줄을 사용할 수 없게 됩니다.



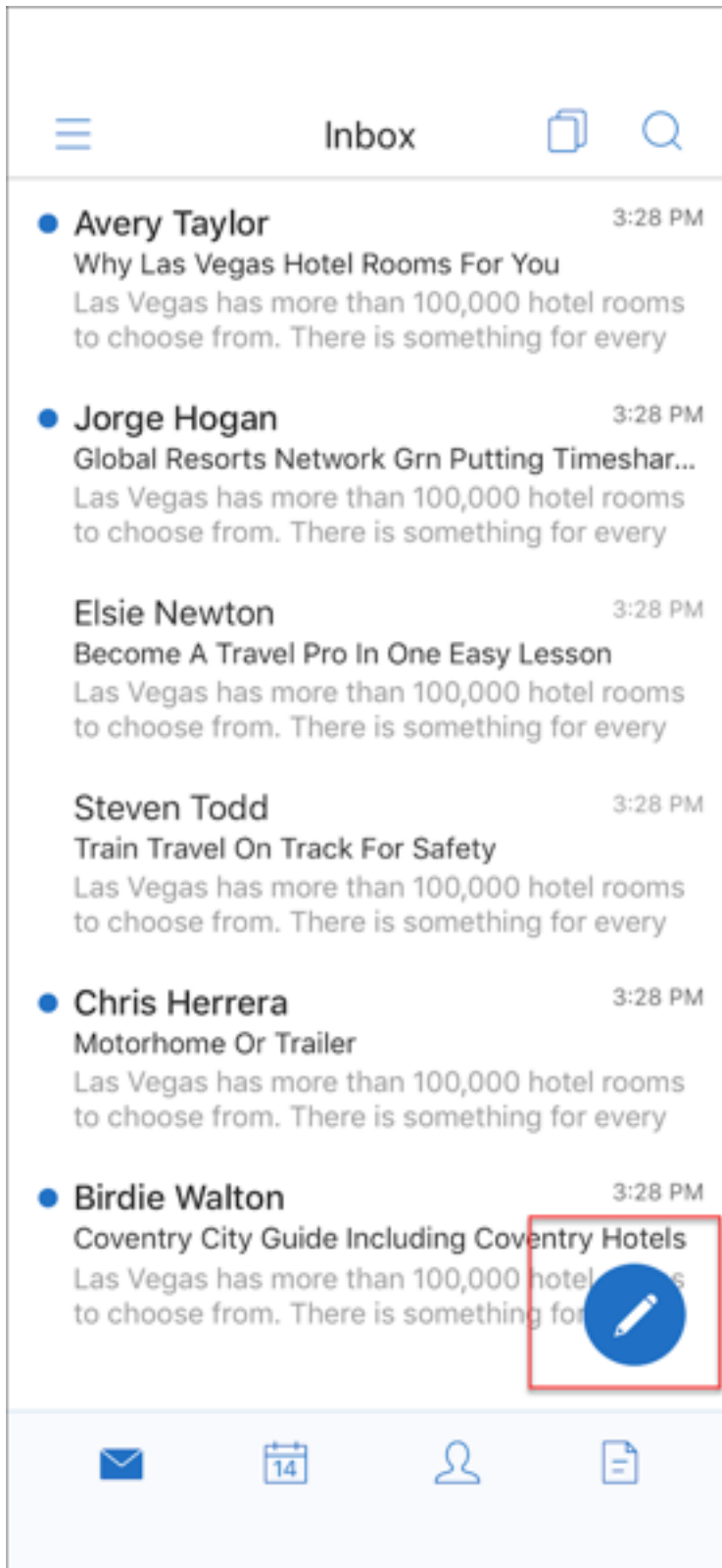
- 설정 메뉴를 모든 메뉴 (예: 메일, 일정, 연락처 및 첨부 파일) 안에서 사용할 수 있습니다. 설정으로 이동하려면 다음 그림에 표시된 것과 같이 햄버거 아이콘을 누른 다음 오른쪽 아래에서 설정 단추를 누릅니다.



- 검색 표시줄이 검색 아이콘으로 대체되고 받은 편지함, 연락처 및 첨부 파일 보기에서 검색 아이콘을 사용할 수 있습니다.



- iOS 장치에서 메일 항목을 길게 눌러 항목을 선택할 수 있습니다.
- 다음 그림에 표시된 것과 같이 작성 부동 작업 단추를 눌러 새 전자 메일을 작성할 수 있습니다.



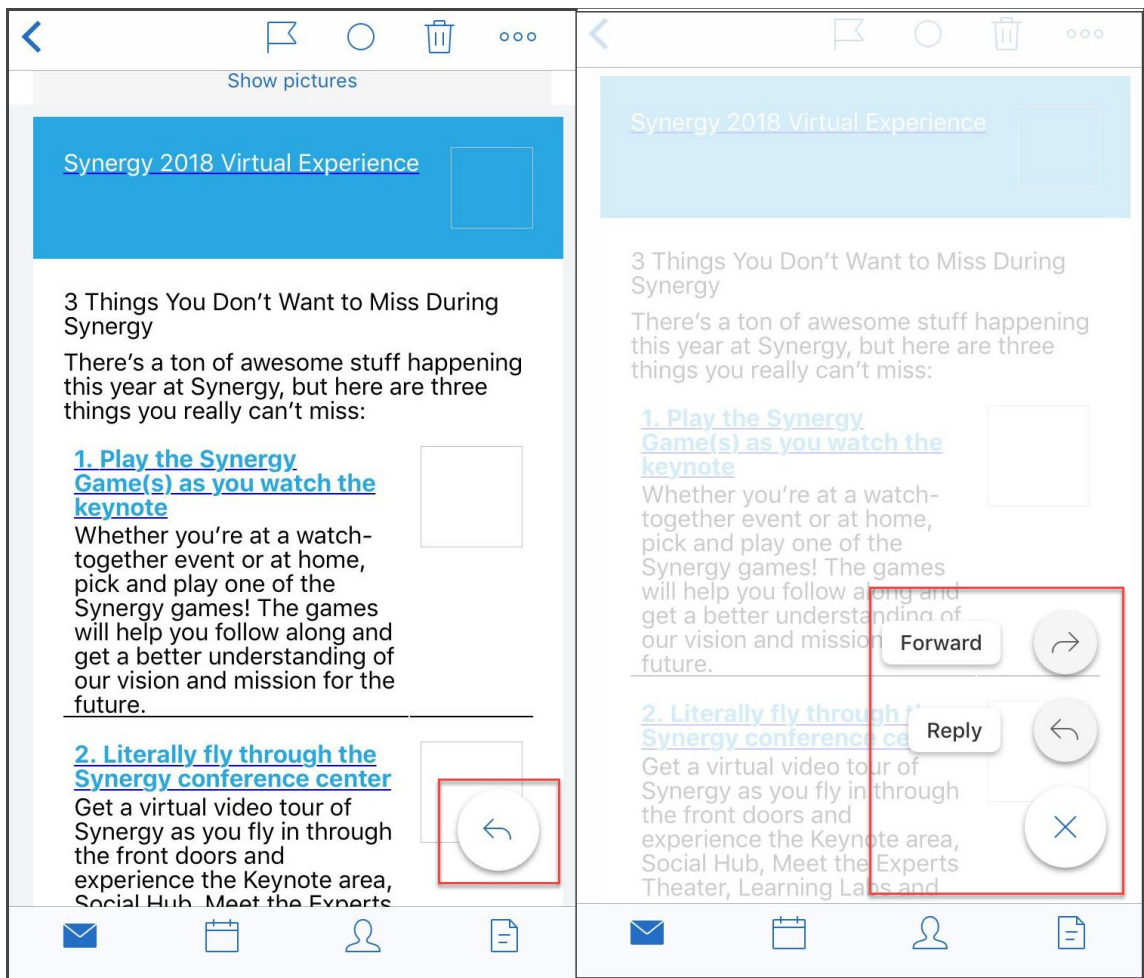
- 이제 화면 오른쪽 위에서 다음 메뉴 옵션을 사용할 수 있습니다.

- 동기화 옵션: 오른쪽 위의 오버플로 아이콘을 누르고 추가 옵션 > 동기화 옵션으로 이동하여 동기화 기본 설정을 변경합니다.

참고:

이 옵션은 Android 장치에서만 사용할 수 있습니다.

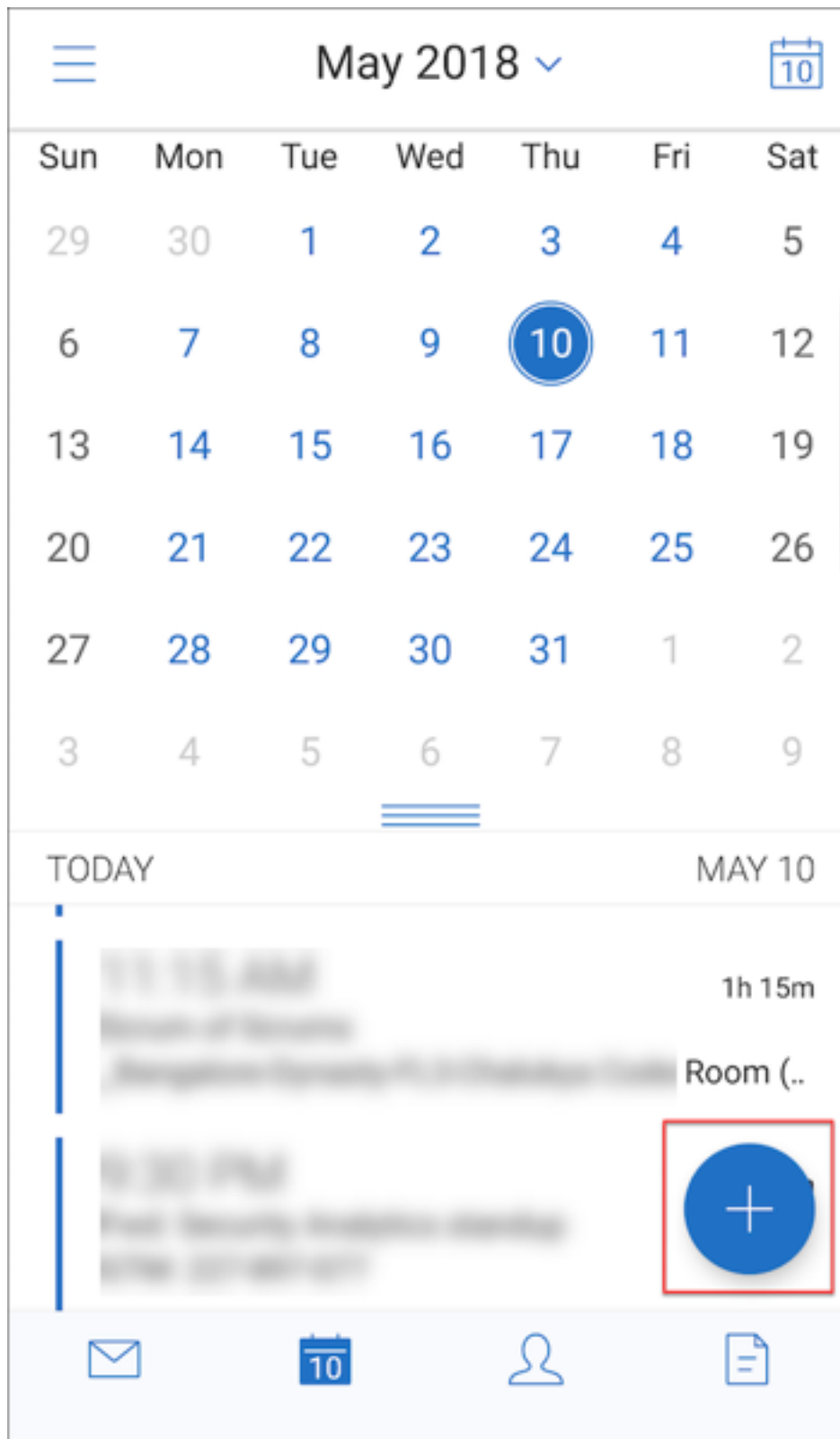
- 검색 아이콘: 눌러서 전자 메일을 검색합니다.
- 분류 보기 아이콘: 눌러서 대화의 분류 보기를 표시합니다.
- 응답 부동 작업 단추: 다음 그림에 표시된 것과 같이 전자 메일을 보는 동안 단추를 눌러 전달, 전체 회신 또는 회신할 수 있습니다.



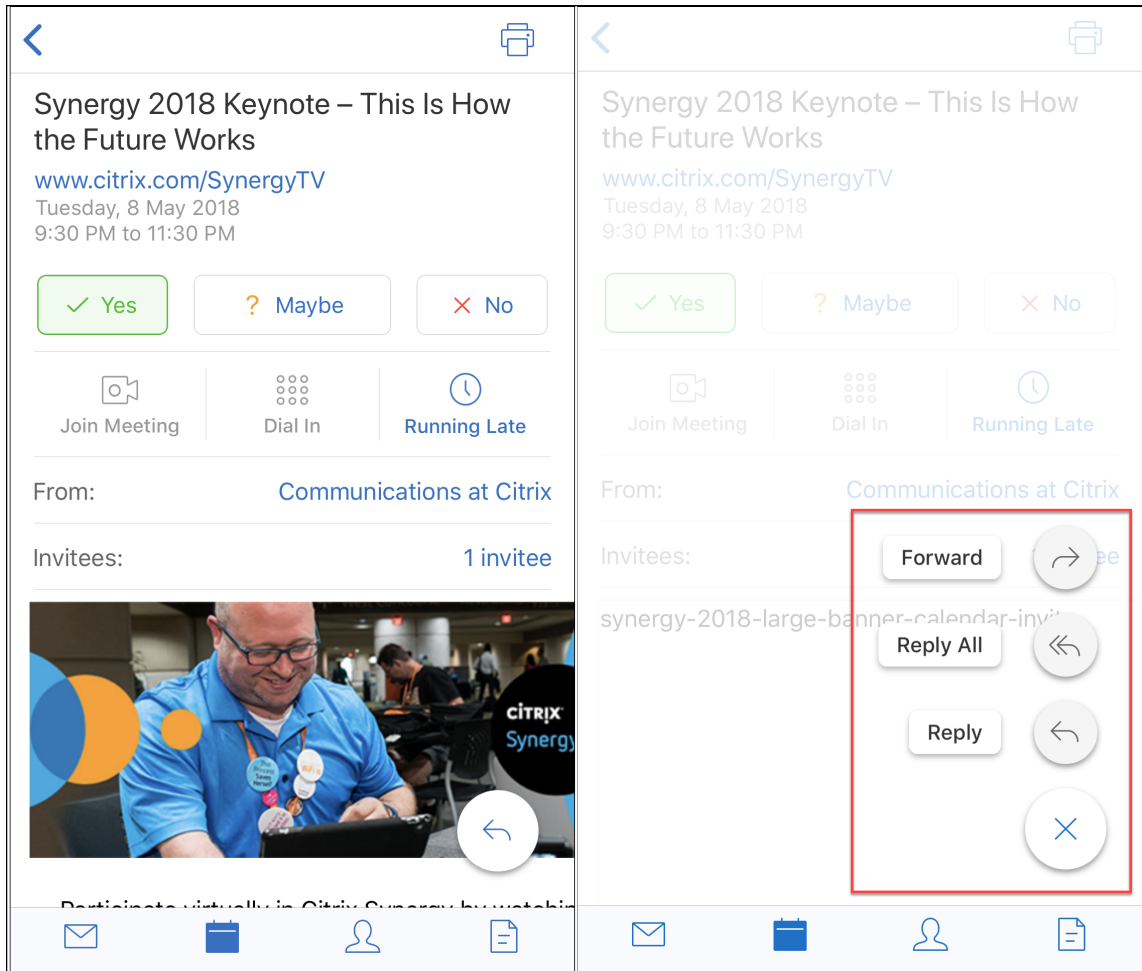
- 전자 메일을 보는 동안 화면 오른쪽 위에서 다음 메뉴 옵션을 사용할 수 있습니다.
 - 플래그: 눌러서 전자 메일에 플래그를 지정합니다.
 - 읽지 않음으로 표시: 눌러서 전자 메일을 읽지 않은 상태로 표시합니다.
 - 삭제: 눌러서 전자 메일을 삭제합니다.
 - 추가 옵션: 오버플로 아이콘을 눌러 사용 가능한 다른 작업 (예: 이동) 을 표시합니다.

일정 변경 내용

- 다음 그림에 표시된 것과 같이 일정에서 이벤트 부동 작업 단추를 눌러 이벤트를 만들 수 있습니다.



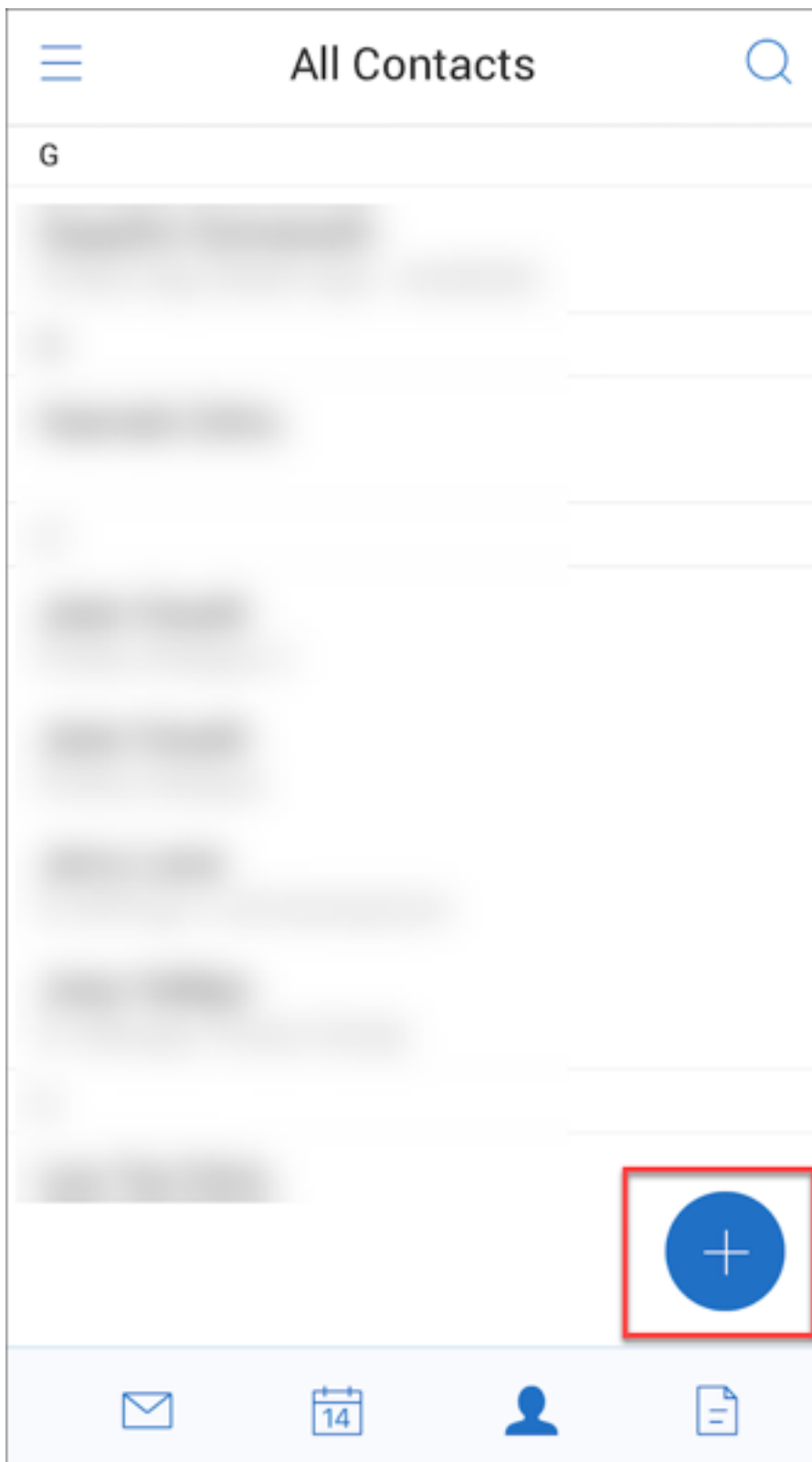
- 이제 화면 오른쪽 위에서 다음 메뉴 옵션을 사용할 수 있습니다.
 - 오늘: 눌러서 오늘의 이벤트를 표시합니다.
 - 검색: 눌러서 이벤트를 검색합니다.
 - 응답 부동 작업 단추: 다음 그림에 표시된 것과 같이 이벤트를 보는 동안 단추를 눌러 전달, 전체 회신 또는 회신할 수 있습니다.



이벤트를 볼 때 예, 나중에 결정 및 아니요 같은 이벤트 응답 작업이 다시 정렬되고 이벤트 세부 정보 아래에 표시됩니다.

연락처 변경 내용

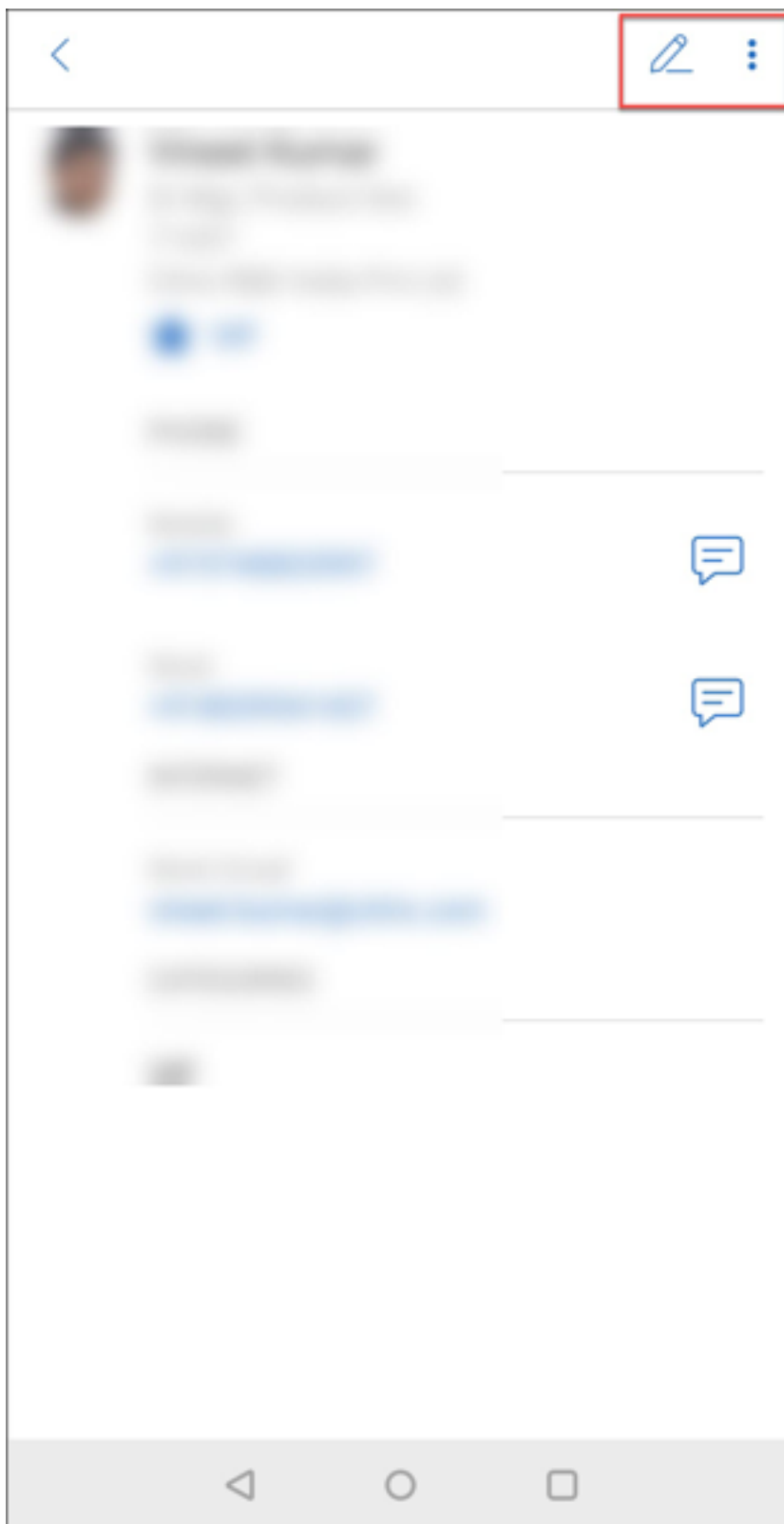
- 다음 그림에 표시된 것과 같이 새 연락처 만들기 부동 작업 단추를 누를 수 있습니다.



- 이제 검색 메뉴 옵션을 화면 오른쪽 위에서 사용할 수 있습니다. 이 옵션을 눌러 연락처를 검색할 수 있습니다.
- 연락처를 보는 동안 화면 오른쪽 위에서 다음 메뉴 옵션을 사용할 수 있습니다.

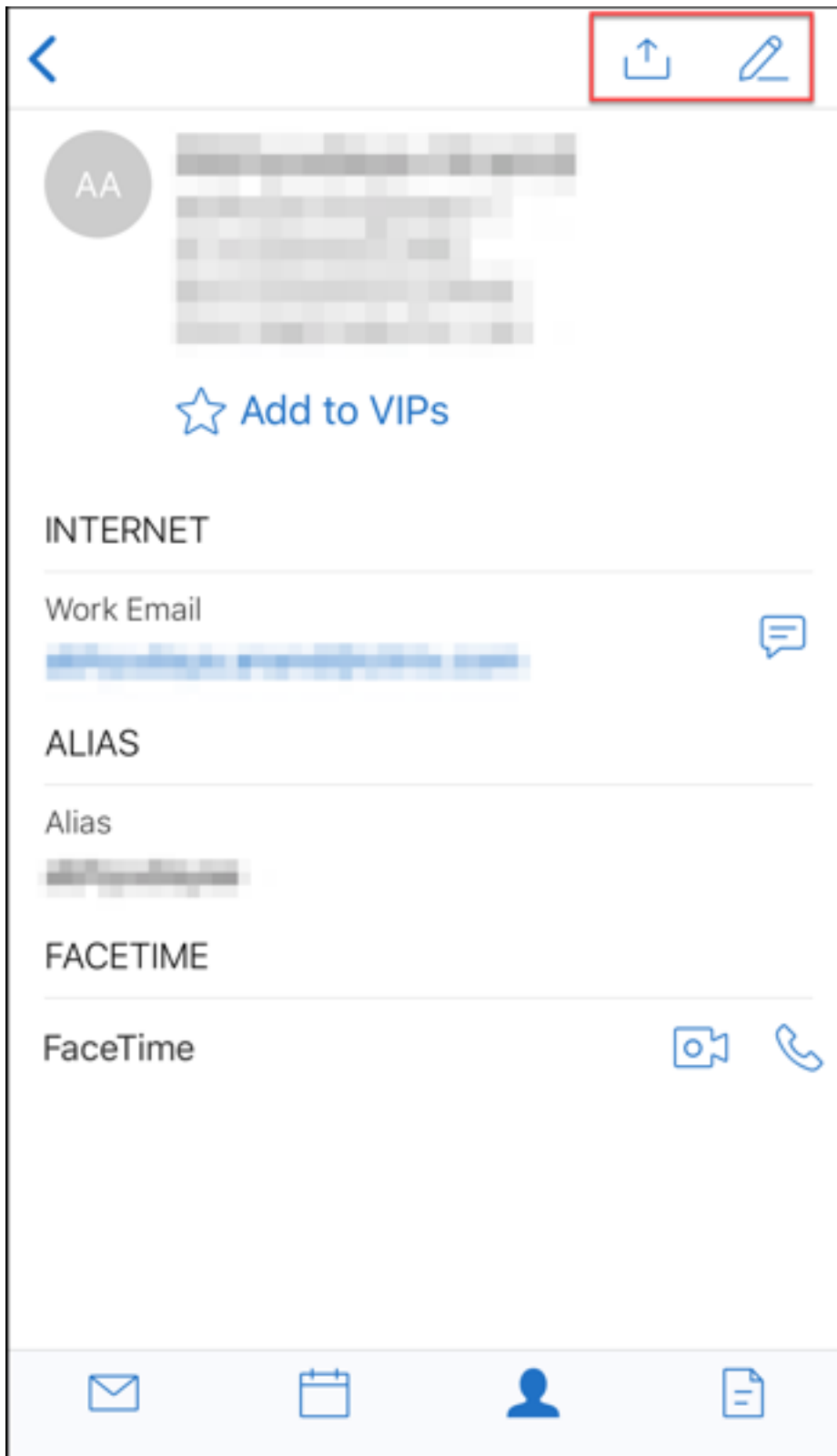
Android 장치의 경우:

- 편집: 눌러서 연락처를 편집합니다.
- 추가 옵션: 편집 아이콘을 눌러 사용 가능한 다른 작업 (예: 메일에 첨부, 공유 및 삭제) 을 표시합니다.







iOS 장치의 경우:

- 편집: 눌러서 연락처를 편집합니다.
- 공유: 공유 아이콘을 눌러 사용 가능한 다른 작업 (예: 연락처 공유 및 메일에 첨부) 을 표시합니다.



참고:

iOS 장치에서 연락처를 삭제하려면 다음 그림에 표시된 것과 같이 연락처를 선택하고 편집을 누른 다음 화면 아래에서 삭제를 누릅니다.

Cancel	Save		
ADDRESS			
Add Address			
COMPANY INFO			
Add Company			
PERSONAL			
Add Personal			
DATES			
Add Date			
NOTES			
Add Note			
Delete Contact			
			

첨부 파일 변경 내용 이제 화면 오른쪽 위에서 다음 첨부 파일 메뉴 옵션을 사용할 수 있습니다.

- 정렬: 정렬 아이콘을 누르고 적절한 필터를 선택하여 첨부 파일을 정렬합니다.
- 검색: 눌러서 첨부 파일을 검색합니다.

Secure Mail 10.8.20

- 이제 iOS 용 Secure Mail 에서 파생된 자격 증명을 등록과 인증에 사용할 수 있습니다. 파생된 자격 증명에 대한 자세한 내용은 [iOS 용 파생된 자격 증명](#)을 참조하십시오.
- iOS 용 Secure Mail 은 다양한 방식의 푸시 알림을 지원합니다. 다양한 방식의 알림을 통해 Secure Mail 이 백그라운드에서 실행 중이지 않을 때에도 받은 편지함에서 잠금 화면 알림을 받을 수 있습니다. 이 기능은 암호 기반 인증과 클라이언트 기반 인증 설정에서 지원됩니다. 자세한 내용은 [다양한 방식의 푸시 알림](#)을 참조하십시오.

참고:

다양한 방식의 푸시 알림 기능을 지원하도록 아키텍처가 변경되어 **VIP** 전용 메일 알림은 더 이상 사용할 수 없습니다.

- 이제 iOS 용 Secure Mail 에서 서식 있는 텍스트 서명이 지원됩니다. 전자 메일 서명에 이미지 또는 링크를 사용할 수 있습니다. 자세한 내용은 [서식 있는 텍스트 서명](#)을 참조하십시오.

Secure Mail 10.8.15

- 이제 **iOS** 용 **Secure Mail** 에서 서식 있는 텍스트 서명이 지원됩니다. 전자 메일 서명에 이미지 또는 링크를 사용할 수 있습니다. 자세한 내용은 [서식 있는 텍스트 서명](#)을 참조하십시오.
- **Secure Mail** 은 **Android Enterprise**(이전 명칭: **Android for Work**) 를 지원합니다. Secure Mail 에서 Android Enterprise 앱을 사용하여 별도의 작업 프로필을 만들 수 있습니다. 자세한 내용은 [Secure Mail 의 Android Enterprise](#)를 참조하십시오.
- 전자 메일을 보는 동안 **Secure Mail** 이 포함된 리소스를 렌더링합니다. 이미지 URL 이 내부 링크인 메일과 같이, 리소스가 내부 네트워크에 있는 경우 Secure Mail 은 내부 네트워크에 연결하여 콘텐츠를 가져오고 렌더링합니다.
- **Secure Mail** 은 최신 인증을 지원합니다. 최신 인증은 사용자 이름 및 암호와 함께 OAuth 토큰 기반 인증을 적용합니다. 이 지원에는 Office 365 의 내부 및 외부 AD FS(Active Directory Federation Services) 또는 IdP(ID 공급자) 지원이 포함됩니다.
- 첨부 파일 저장소 성능이 개선되었습니다. 첨부 파일 저장소를 훨씬 빠르게 스크롤할 수 있게 되었습니다.

Secure Mail 10.8.10

- 첨부 파일 인쇄 지원. iOS 용 Secure Mail 이 첨부 파일 인쇄를 지원합니다.
- **Microsoft Office 365** 를 통한 최신 인증. iOS 용 Secure Mail 이 최신 인증을 지원합니다. 최신 인증은 사용자 이름 및 암호와 함께 OAuth 토큰 기반 인증을 적용합니다. 이 지원에는 Office 365 의 외부 및 내부 AD FS(Active Directory Federation Services) 및 IdP(ID 공급자) 지원이 포함됩니다. 자세한 내용은 [Microsoft Office 365 를 사용한 최신 인증](#)을 참조하십시오.

참고:

이 릴리스는 Microsoft Intune/EMS 와 Endpoint Management 의 통합을 통한 최신 인증을 지원하지 않습니다.

이 릴리스에는 AD FS 를 외부에서 액세스하는 시나리오에 대한 최신 인증이 포함됩니다.

알려진 문제와 수정된 문제

February 27, 2024

Citrix 에서는 이전 두 버전의 모바일 생산성 앱의 업그레이드를 지원합니다.

Secure Mail 24.2.0

iOS 용 Secure Mail 의 수정된 문제

- iOS 용 Secure Mail 에서는 일정 페이지에 추가 단추 (+) 가 표시되지 않아 새 일정 이벤트를 만들지 못할 수 있습니다. [XMHELP-4460]
- Secure Mail 은 네트워크 연결 문제로 인해 iPhone 과 iPad 장치 모두에서 이메일을 동기화할 수 없습니다. [XMHELP-4473]
- iOS 용 Secure Mail 에서 다크 모드를 사용하는 경우 전자 메일 메시지를 읽지 못할 수 있습니다. [XMHELP-4499]

iOS 용 Secure Mail 의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Mail 24.1.0

Android 용 Secure Mail 의 수정된 문제

- 10MB 보다 큰 첨부 파일을 열려고 하면 Android 용 Secure Mail 이 응답하지 않습니다. [XMHELP-4399]
- .docx 형식이고 아랍어 문자나 하이퍼링크가 있는 첨부 파일을 열려고 하면 Android 용 Secure Mail 이 응답하지 않습니다. 이 문제는 Polaris SDK 가 업데이트되지 않은 경우 발생합니다. [XMHELP-4491]

Android 용 Secure Mail 의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Mail 23.10.0

Android 용 Secure Mail 의 수정된 문제

- Secure Mail 에서 첨부 파일을 열면 장치에 **Citrix Files** 앱이 설치되어 있지 않더라도 자세히 (🔍) > 다음으로 열기 옵션에서 **Citrix Files** 에 업로드 옵션을 찾을 수 있습니다. [XMHELP-4437]
- Secure Mail 에서 받은 회의 초대에 첨부된.ics 파일을 미리 보려면.ics 파일 미리 보기에 표시된 회의 시간이 원래 시간보다 한 시간 늦어지는 것을 알 수 있습니다. 이 문제는 서머타임 지역에서 발생합니다. [XMHELP-4429]
- Secure Mail 을 버전 23.8.2 로 업그레이드하고 다크 모드를 활성화하면 첨부 파일을 미리 보는 동안 문제가 발생할 수 있습니다. 줄임표 (...) 버튼을 클릭하면 메뉴 목록이 표시되지 않을 수 있습니다. [CXM-112699]

Android 용 Secure Mail 의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Mail 23.8.2

Android 용 Secure Mail 의 수정된 문제

이 릴리스에는 수정된 문제가 없습니다.

Android 용 Secure Mail 의 알려진 문제

Secure Mail 을 버전 23.8.2 로 업그레이드하고 다크 모드를 활성화하면 첨부 파일을 미리 보는 동안 문제가 발생할 수 있습니다. 줄임표 (...) 버튼을 클릭하면 메뉴 목록이 표시되지 않을 수 있습니다. 이 문제를 해결하려면 Secure Mail 을 라이트 모드로 전환할 수 있습니다. [CXM-112699]

Secure Mail 23.7.0

Android 및 iOS 용 Secure Mail 의 수정된 문제

이 릴리스에는 수정된 문제가 없습니다.

Android 및 iOS 용 Secure Mail 의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Mail 23.8.1

Android 용 Secure Mail 의 수정된 문제

이 릴리스에는 수정된 문제가 없습니다.

Android 용 Secure Mail 의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Mail 23.9.0

iOS 용 Secure Mail 의 수정된 문제

- HCL Domino 11 서버와 함께 iOS 용 Secure Mail 23.2.0 버전을 사용하는 경우 이전에 저장한 초안 이메일을 보내지 못할 수 있습니다. Secure Mail 에 이메일이 성공적으로 전송되었지만 수신자는 이메일을 받지 못했다고 표시됩니다. [XMHELP-4306]

iOS 용 Secure Mail 의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Mail 23.8.0

Android 용 Secure Mail 의 수정된 문제

이 릴리스에는 수정된 문제가 없습니다.

Android 용 Secure Mail 의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Mail 23.7.0

Android 용 Secure Mail 의 수정된 문제

- 일정 이벤트에 대한 알림을 받지 못할 수도 있습니다. 이 문제는 Secure Mail 에 대한 경보 및 알림 권한이 취소될 때 발생합니다. [CXM-109036]

Android 용 Secure Mail 의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Mail 23.6.0

Android 용 Secure Mail 의 수정된 문제

첨부 파일을 볼 때 “라이선스 만료됨” 이라는 워터마크가 표시될 수 있습니다. 이 문제는 Android 용 Secure Mail 버전 23.3.5 이하를 사용하는 경우에 발생합니다. 워터마크 없이 첨부 파일을 보려면 Android 용 Secure Mail 버전 23.6.0 이상으로 업그레이드하십시오. [CXM-110137]

Android 용 Secure Mail 의 알려진 문제

이 릴리스에는 알려진 문제가 없습니다.

Secure Mail 23.5.0

iOS 용 Secure Mail 의 수정된 문제

- 디지털 서명된 전자 메일을 수신하여 Secure Mail 에서 열면 첨부 파일이 나타나지 않을 수 있습니다. [XMHELP-4247]

이전 버전의 알려진 문제 및 수정된 문제

이전 버전의 Secure Mail 에 대한 알려진 문제와 수정된 문제는 [Secure Mail 의 알려진 문제 및 수정된 문제에 대한 기록](#)을 참조하십시오.

Secure Mail 배포

February 27, 2024

Secure Mail 을 Citrix Endpoint Management(이전의 XenMobile) 와 통합하여 배포하려면 다음 일반 단계를 따르십시오.

1. Secure Mail 을 Exchange Server 또는 IBM Notes Traveler 서버와 통합하여 Secure Mail 이 Microsoft Exchange 또는 IBM Notes 와 계속 동기화되도록 할 수 있습니다. IBM Notes 를 사용하는 경우, IBM Notes Traveler 서버를 구성하십시오. 이 구성에서는 Active Directory 자격 증명을 사용하여 Exchange 또는 IBM Notes Traveler 서버에 인증합니다. 자세한 내용은 [Exchange Server 또는 IBM Notes Traveler 서버 통합](#)을 참조하십시오.

중요:

Secure Mail 의 메일을 IBM Notes Traveler(이전의 IBM Lotus Notes Traveler) 와 동기화할 수 없습니다. 이 Lotus Notes 타사 기능은 현재 지원되지 않습니다. 따라서 Secure Mail 에서 모임 응답 메일을 삭제하는 경우 IBM Notes Traveler 서버에서 메일이 삭제되지 않습니다. 사용자가 일정 이벤트를 수락했다가 이후에 설명을 추가하여 이벤트를 거부하거나 설명과 함께 조치를 취하는 경우 설명이 사라집니다. [CXM-47936]

2. 선택적으로 Secure Hub 에서 SSO 가 사용되도록 설정할 수 있습니다. 이를 위해 Endpoint Management 콘솔에서 Citrix Files 계정 정보를 구성하여 Endpoint Management 를 Citrix Files 용 SAML ID 공급자로 사용하도록 설정합니다. 이 구성에서는 Active Directory 자격 증명을 사용하여 Citrix Files 에 인증합니다.

Endpoint Management 콘솔에서 Citrix Files 계정 정보를 구성하는 것은 모든 Citrix 클라이언트, Citrix Files 클라이언트 및 비 MDX Citrix Files 클라이언트에 사용되는 일회용 설정입니다. 자세한 내용은 [To configure Citrix Files account information in Endpoint Management console for SSO\(Endpoint Management 콘솔에서 SSO 에 Citrix Files 계정 정보를 구성하려면\)](#)을 참조하십시오.

3. Citrix 다운로드 사이트에서 Secure Mail .mdx 파일을 다운로드합니다.
4. Secure Mail 을 Endpoint Management 에 추가하고 MDX 정책을 구성합니다. 자세한 내용은 [앱 추가](#)를 참조하십시오.

참고:

Secure Mail 버전 10.6.5 부터 iOS 및 Android 용 Secure Mail 에 대한 새 MDX 분석 정책을 구성할 수 있습니다. Citrix 에서는 제품 품질을 개선하기 위해 분석 데이터를 수집합니다. Google Analytics 세부 수준 정책에서 데이터를 회사 도메인과 연결하지 아니면 익명으로 수집할지를 지정할 수 있습니다. 익명을 선택하면 사용자의 수집된 데이터에 회사 도메인이 포함되지 않습니다. 이러한 새로운 정책은 이전 Google Analytics 정책을 대체합니다.

정책이 익명으로 설정된 경우 다음 유형의 데이터가 수집됩니다. 사용자 식별 정보를 요청하지 않으므로 이 데이터를 개인 사용자나 회사와 연결지을 일은 없습니다. 신원을 확인할 수 있는 정보는 Google 에 전송되지 않습니다.

- 운영 체제 버전, 앱 버전 및 장치 모델과 같은 장치 통계
- ActiveSync 버전 및 Secure Mail 서버 버전과 같은 플랫폼 정보
- APNs 등록, 메일 동기화 및 전송과 첨부 파일 다운로드 및 일정 동기화 같은 제품 품질의 실패 지점.

정책이 전체로 설정되어 있어도 회사 도메인 외 다른 식별 가능한 정보를 수집하지 않습니다. 기본값은 전체입니다.

Secure Mail 구성

November 1, 2023

Secure Mail 에서 다음 기능을 구성하고 통합할 수 있습니다.

- [Office 365 를 통한 최신 인증](#)

- 온-프레미스 Exchange 를 사용한 하이브리드 최신 인증
- Secure Mail 에 대한 백그라운드 서비스
- Exchange Server 또는 IBM Notes Traveler 서버 통합
- Secure Mail 에 대한 S/MIME 구성
- Secure Mail 에 대한 SSO

Microsoft Office 365 를 통한 최신 인증

February 27, 2024

Secure Mail 은 Microsoft Office 365 for AD FS(Active Directory Federation Services) 또는 IDP(ID 공급자) 를 통한 최신 인증을 지원합니다. 최신 인증은 사용자 이름 및 암호와 함께 OAuth 토큰 기반 인증을 적용합니다. iOS 장치가 있는 Secure Mail 사용자는 Office 365 에 연결할 때 인증서 기반 인증을 활용할 수 있습니다. 사용자는 Secure Mail 에 로그인할 때 자격 증명을 입력하는 대신 클라이언트 인증서를 사용하여 인증합니다.

계속하기 전에 다음을 수행하십시오.

1. Microsoft Office 365 용 최신 인증 (OAuth) 을 사용하도록 설정합니다.
2. 최적의 네트워크 연결을 위해 방화벽에서 Office 365 끝점, URL 및 IP 주소 범위를 사용하도록 설정합니다. 자세한 내용은 Microsoft 문서의 [Office 365 URLs and IP address range\(Office 365 URL 및 IP 주소 범위\)](#)를 참조하십시오.

참고:

- 하이브리드 Exchange 사서함 솔루션을 마이그레이션하거나 만들려면 Microsoft 설명서에서 [Exchange 하이브리드 배포를 사용한 Exchange ActiveSync 장치 설정](#)을 참조하십시오.

Citrix Endpoint Management 정책 사전 요구 사항

Citrix Endpoint Management 콘솔에서 다음 정책을 사용하도록 설정합니다.

iOS 를 실행하는 장치:

- **Office 365 인증 메커니즘:** Office 365 에서 계정을 구성하는 동안 인증에 OAuth 메커니즘이 사용됨을 나타내려면 이 정책을 사용합니다. 이 정책에는 다음 값을 구성해야 합니다.
 - **OAuth 사용 안 함:** 계정 구성 시 기본 인증을 적용하려면 이 정책을 사용합니다.
 - 사용자 이름 및 암호와 함께 **OAuth 사용:** 인증 시 OAuth 프로토콜을 적용하려면 이 정책을 사용합니다. 사용자가 사용자 이름 및 암호를 입력하고 선택적으로 OAuth 흐름을 위한 다단계 인증 코드를 제공해야 합니다.
 - 클라이언트 인증서와 함께 사용자 **OAuth:** 인증서 기반 인증을 수행하도록 Office 365 가 구성된 경우 이 정책을 사용합니다. 기본 구성은 **OAuth 사용 안 함**입니다.

Android 를 실행하는 장치:

- **0365** 에 대해 최신 인증 사용: 인증 시 OAuth 프로토콜을 적용하려면 이 정책을 사용합니다.
 - 터널링에 대한 웹 **SSO** 정책: 이 정책을 사용하면 OAuth 트래픽을 터널링하여 터널링됨 - 웹 SSO 를 통과할 수 있습니다. 이 작업을 수행하려면:
 - **Use Web SSO for tunneling**(터널링에 웹 SSO 사용) 정책을 **On**(켜기) 으로 설정합니다.
 - 네트워크 액세스 정책에서 **Tunneled - Web SSO**(터널링됨 - 웹 SSO) 옵션을 선택합니다.
- 참고:
- STA 활성화에 대한 자세한 내용은 [STA 를 통한 메일 서버 연결](#)을 참조하십시오.
- 백그라운드 서비스 정책에서 OAuth 와 관련된 모든 호스트 이름을 제외합니다.

iOS 및 **Android** 장치에 공통된 정책:

- 최신 인증에 대한 사용자 지정 사용자 에이전트: 최신 인증을 위해 기본 사용자 에이전트 문자열을 변경하려면 이 정책을 사용합니다.
- 신뢰할 수 있는 **Exchange Online** 호스트 이름: 계정을 구성하는 동안 인증에 OAuth 메커니즘을 사용하는 신뢰할 수 있는 Exchange Online 호스트 이름 목록을 정의하려면 이 정책을 사용합니다. 이는 `server.company.com`, `server.company.co.uk` 와 같은 심표로 구분된 형식입니다. 이 목록은 기본값 또는 vanity URL 을 포함할 수 있지만 비어 있을 수는 없습니다. 기본값은 **outlook.office365.com** 입니다.
- 신뢰할 수 있는 **AD FS** 호스트 이름: Office 365 OAuth 인증 시 암호가 채워지는 신뢰할 수 있는 AD FS 호스트 이름 목록을 웹 페이지에 대해 정의하려면 이 정책을 사용합니다. 심표로 구분된 형식 (예: `sts.companyname.com`, `sts.company.co.uk`) 을 사용합니다. 이 목록이 비어 있는 경우 Secure Mail 은 암호를 자동으로 채우지 않습니다. Secure Mail 은 목록의 호스트 이름을 Office 365 인증 시 나타나는 웹 페이지의 호스트 이름과 대조하여 해당 페이지가 HTTPS 프로토콜을 사용하는지 확인합니다. 예를 들어 `sts.company.com` 호스트 이름이 나열된 경우 사용자가 `https://sts.company.com`으로 이동할 때 페이지에 암호 필드가 있으면 Secure Mail 이 암호를 채웁니다. 기본값은 `login.microsoftonline.com`입니다.
- **Secure Mail Exchange Server**: Exchange Server 의 주소를 정의하려면 이 정책을 사용합니다. 이 정책을 사용하면 요구 사항에 따라 온프레미스 서버 주소 또는 클라우드 서버 주소를 정의할 수 있습니다.
- **HTTP 451** 리디렉션 구성: 리디렉션을 구성하는 방법에 대한 자세한 내용은 Knowledge Center 문서 [Secure Mail ActiveSync 리디렉션 451](#)을 참조하십시오.

iOS 용 Secure Mail 은 이제 장치에서 정책이 새로 고쳐진 후 최신 인증을 사용하도록 설정되어 있습니다.

제한 사항

- 환경에서 최신 인증을 사용하는 경우 iOS 에 대한 다양한 방식의 푸시 알림 기능을 사용할 수 없습니다. 다양한 방식의 푸시 알림에 대한 자세한 내용은 [Secure Mail 을 위한 푸시 알림](#)을 참조하십시오.
- 인증서 기반 인증을 실행하는 환경에서는 여러 계정이 지원되지 않습니다.

Secure Mail 정책

다음 2 개의 표에는 Exchange 인프라에 따라 필요한 Secure Mail 정책이 나와 있습니다.

Exchange 인프라	Office 365 인증 메커니즘/O365 에 대해 최신 인증 사용	신뢰할 수 있는 AD FS 온라인 호스트 이름	신뢰할 수 있는 Exchange Online 호스트 이름
온-프레미스	꺼짐	해당 없음	해당 없음
하이브리드 *	켜짐	AD FS/IDP	Outlook.office365.com 또는 Vanity URL
Exchange Online	켜짐	AD FS/IDP	Outlook.office365.com 또는 Vanity URL

Exchange 인프라	Secure Mail Exchange Server	백그라운드 네트워크 서비스 (iOS)	백그라운드 네트워크 서비스 (Android)
온-프레미스	Exchange 온-프레미스 호스트 이름	온-프레미스	온-프레미스
하이브리드 *	온-프레미스, Exchange Online 호스트 이름	온-프레미스, Exchange 온-프레미스 호스트 이름	온-프레미스, Exchange 온-프레미스 호스트 이름, AD FS/IDP(내부 전용)
Exchange Online	Outlook.office365.com	Exchange Online 호스트 이름	Exchange 온-프레미스 호스트 이름, AD FS, IDP

*Secure Mail 은 마이그레이션된 사서함과 함께 하이브리드 Exchange 인프라를 지원합니다.

온-프레미스 사용자의 사서함이 Exchange Online 으로 마이그레이션되는 경우, Secure Mail 이 자동으로 이 변경을 탐지하여 최신 인증을 사용할 것인지 묻는 메시지를 사용자에게 표시하므로 계정을 재구성할 필요가 없습니다.

Secure Mail 및 OAuth 지원 매트릭스

다음 표에는 iOS 및 Android 장치에서의 Secure Mail OAuth 지원 매트릭스가 나와 있습니다.

인증 유형	IDP/외부 AD FS	IDP/내부 AD FS	Azure AD	Intune
사용자 이름 및 암호	예	예	예	예

인증 유형	IDP/외부 AD FS	IDP/내부 AD FS	Azure AD	Intune
클라이언트 인증서	예	Android 전용	아니요	아니요

iOS 및 Android 용 온-프레미스 Exchange 를 사용한 하이브리드 최신 인증

November 1, 2023

하이브리드 최신 인증 (HMA) 은 보다 안전한 사용자 인증 및 권한 부여 방법을 사용하는 사용자 ID 관리 솔루션입니다. 이제 Exchange 서버 온-프레미스 하이브리드 배포에 사용할 수 있습니다.

HMA 는 사용자 이름과 암호를 사용하는 OAuth 토큰 기반 인증입니다. 온-프레미스 사서함 사용자는 OAuth 토큰을 사용하여 온-프레미스 Exchange 에 액세스할 수 있습니다. OAuth 토큰은 클라우드에서 가져옵니다. 최신 인증을 사용하여 사용자 ID 를 관리하면 관리자는 리소스 보안에 다양한 도구를 사용할 수 있으며 온-프레미스 Exchange 에서 보다 안전하게 ID 를 관리할 수 있습니다.

HMA 에 대한 자세한 내용은 [Exchange 온-프레미스용 하이브리드 최신 인증 발표](#)를 참조하십시오.

MDX 정책에 필요한 변경

HMA 가 Secure Mail iOS 및 Android 에서 작동하도록 하려면 **Office 365** 용 **OAuth** 지원 섹션에서 MDX 정책을 다음과 같이 변경하십시오.

- Android 의 경우 **O365** 용 최신 인증 사용 옵션을 활성화합니다.
iOS 의 경우 **Office 365** 인증 메커니즘을 사용자 이름 및 암호와 함께 **OAuth** 사용으로 설정합니다.
- 신뢰할 수 있는 **Exchange** 온라인 호스트 이름 텍스트 필드에 고객의 온-프레미스 Exchange URL 을 입력합니다.
- Office 365 Exchange Server** 텍스트 필드에 고객의 온-프레미스 Exchange URL 을 입력합니다.
- 다음을 클릭합니다.

참고: 위에서 언급한 MDX 정책 변경을 수행하기 전에 Exchange 에서 HMA 설정이 활성화되었는지 확인하십시오. 그렇지 않으면 **O365** 용 최신 인증 사용 옵션을 비활성화합니다.

Android 의 **Office 365** 에 대한 **OAuth** 지원 섹션:

Secure Mail

OAuth Support for Office 365

Use Modern authentication for O365

ON

Trusted Exchange Online Hostnames

outlook.office365.com

Trusted AD FS Hostnames

login.microsoftonline.com

Office 365 Exchange Server

outlook.office365.com

Custom user agent for modern authentication

Custom Client Id for OAuth Authentication

Use Web SSO for tunneling

ON

Slack integration

Enable Slack

OFF

Slack workspace name

Widgets

Allow Calendar Agenda widget

ON

Deployment Rules

Store Configuration

Back

Next >

iOS 의 Office 365 에 대한 OAuth 지원 섹션:

OAuth Support for Office 365

Office 365 authentication mechanism

Use OAuth with Username and Password

Trusted Exchange Online Hostnames

outlook.office365.com

Trusted AD FS Hostnames

login.microsoftonline.com

Office 365 Exchange Server

outlook.office365.com

Custom user agent for modern authentication

Mail Redirection

Mail Redirection

Secure Mail

Slack integration

Enable Slack

ON

Slack workspace name

Default Slack App

Slack

Deployment Rules

Store Configuration

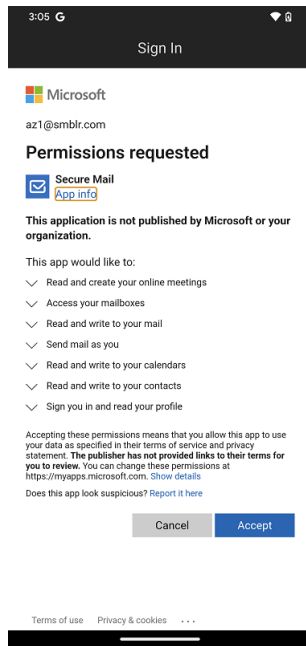
Volume purchase

Back

Next >

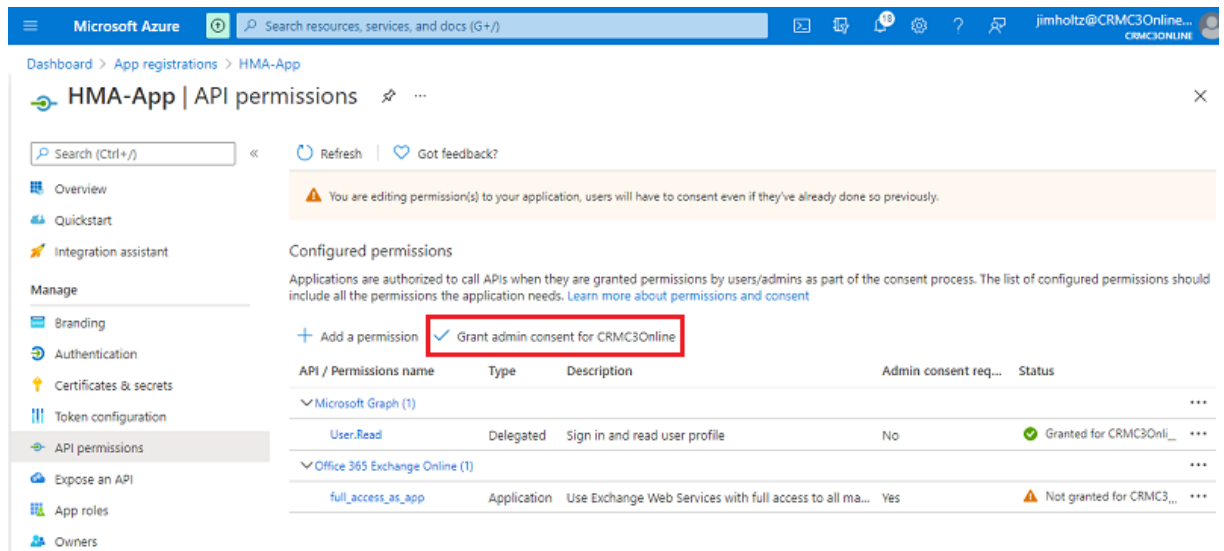
다음 동의 페이지는 사용자가 처음으로 로그인에 성공한 후에 나타납니다. 수락을 클릭합니다.

Secure Mail



선택 사항: 이 동의 페이지를 더 이상 표시하지 않으려면 다음 단계를 수행하십시오.

- Microsoft Azure 포털을 엽니다.
- 대시보드에서 앱 등록 > **HMA-App** 으로 이동합니다.
- 구성된 권한 섹션에서 **CRMC3Online** 에 대한 관리자 동의 부여 옵션을 활성화합니다.



제한 사항

- HMA 에서 기본 인증으로 전환하려면 Secure Mail 에서 기존 계정을 삭제하고 새 계정을 다시 만들어야 합니다.
- MDX 정책과 Exchange 정책이 일치하지 않는 경우 사용자는 Secure Mail 에 로그인할 수 없습니다.

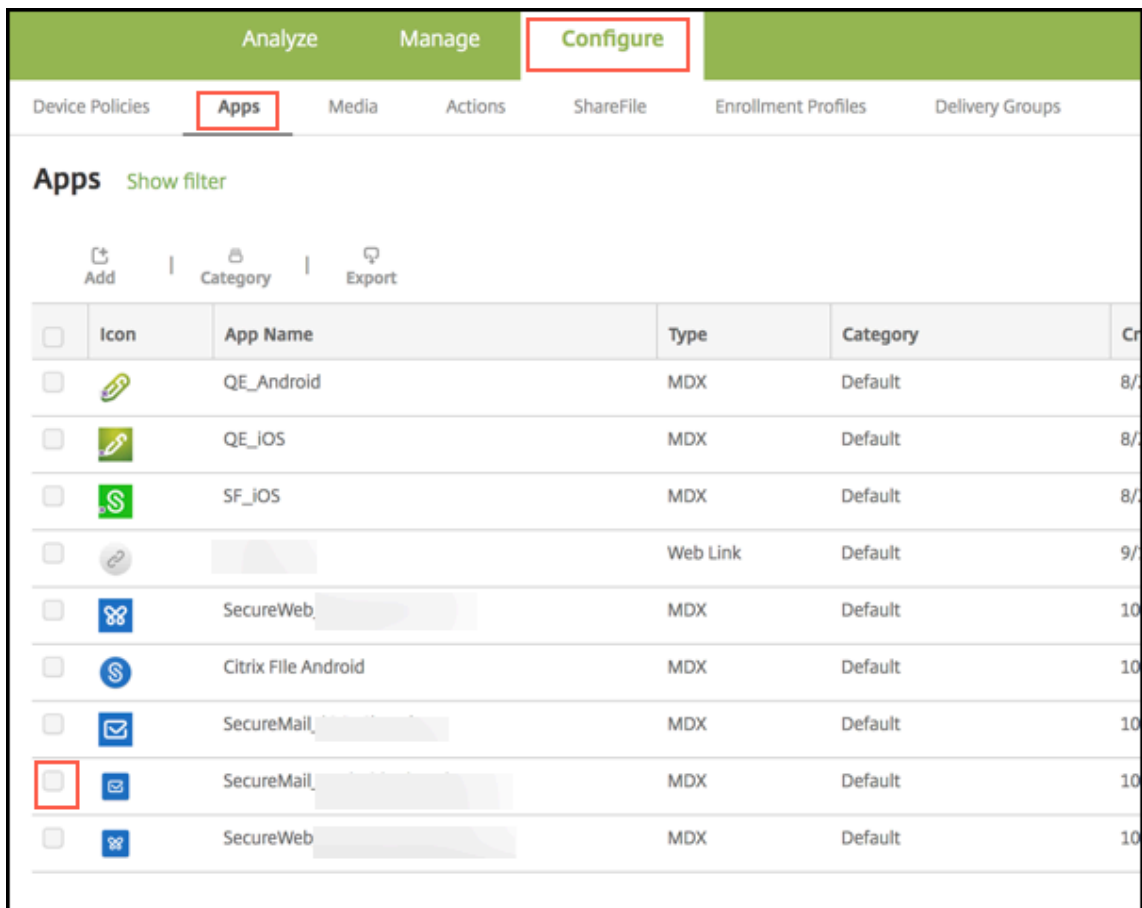
Secure Mail에 대한 백그라운드 서비스

February 27, 2024

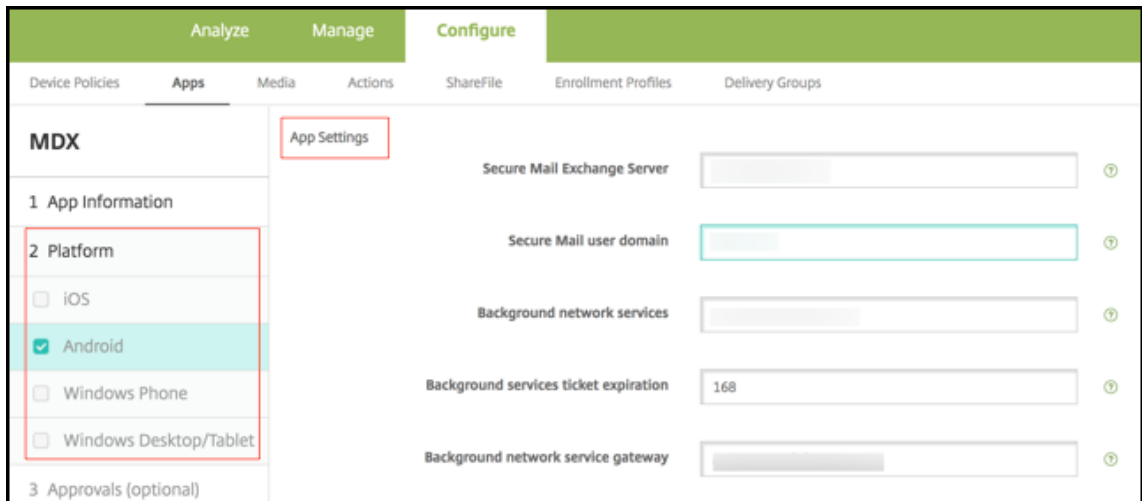
Citrix Gateway를 통해 메일 서버에 액세스하려면 Secure Mail에 대한 백그라운드 서비스를 구성해야 합니다. Secure Mail을 Citrix Endpoint Management(이전 명칭: XenMobile)에 추가하는 경우 MDX 앱 정책 설정에서 백그라운드 서비스를 구성합니다.

Secure Mail에 대한 백그라운드 서비스를 구성하려면

1. 관리자 자격 증명을 사용하여 Endpoint Management 콘솔에 로그인합니다.
2. 콘솔에서 구성 탭을 클릭하고 앱을 클릭한 후 Secure Mail 앱을 선택하고 편집을 클릭합니다.



3. **MDX policy settings(MDX 정책 설정)** 페이지의 플랫폼 섹션에서 필요에 따라 iOS 또는 Android 플랫폼을 선택합니다.
4. 앱 설정 섹션에서 정책을 구성합니다.

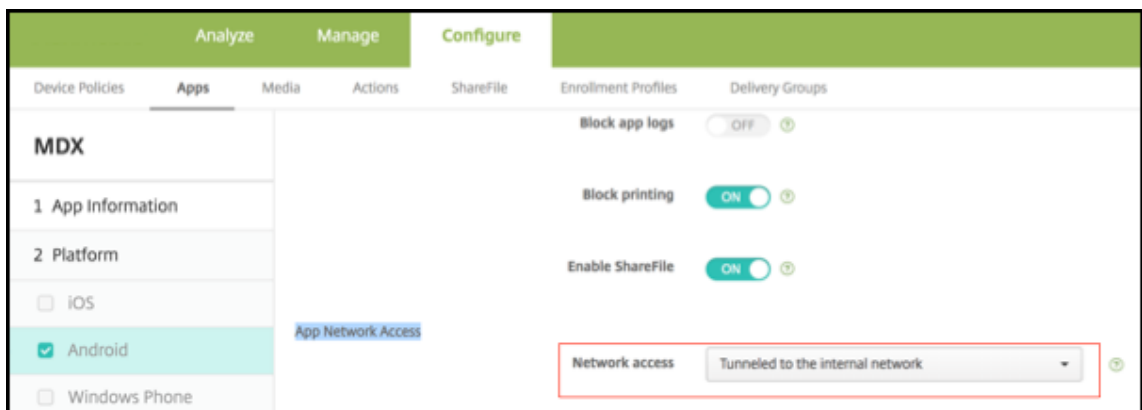


백그라운드 서비스 구성을 위한 MDX 앱 정책

다음 MDX 앱 정책은 Citrix Gateway, Citrix Endpoint Management 서버, STA(Secure Ticket Authority) 서버 및 메일 서버와 Secure Mail의 통신에 영향을 미칩니다.

네트워크 액세스: 네트워크 액세스 정책은 Secure Mail이 VPN을 사용해야 백그라운드 네트워크 서비스에 액세스할 수 있는지 아니면 모든 트래픽이 인터넷을 통해 제한 없이 전송되는지를 지정합니다.

- 네트워크 액세스 정책이 내부 네트워크로 터널링됨으로 설정된 경우 백그라운드 네트워크 서비스에 나열된 URL만 Citrix Gateway를 통과하며, 나머지 트래픽은 인터넷을 통해 제한 없이 전송됩니다. 기본적으로 Secure Mail 액세스는 내부 네트워크로 터널링됨으로 설정되어 있습니다.
- 네트워크 액세스 정책이 제한 없음으로 설정된 경우 Secure Mail에서 시작된 모든 트래픽이 인터넷을 통해 제한 없이 전송되며, 백그라운드 서비스에 액세스하는 데 VPN이 사용되지 않습니다.



Secure Mail Exchange Server: Secure Mail Exchange Server 정책을 Exchange Server 또는 메일 서버의 FQDN(정규화된 도메인 이름)으로 설정합니다.

백그라운드 네트워크 서비스: 백그라운드 네트워크 서비스 정책은 Citrix Gateway를 통해 액세스하도록 허용된 메일 서버의 목록을 지정합니다. 호스트 이름 및 포트 번호를 심볼로 구분된 값으로 나열합니다. 값 사이에 선행 및 후행 공백이 없어야 합니다.

메일 서버 주소의 경우 `hostnameFQDN:portnumber`를 포함하십시오. 예: `mail1.example.com:443`, `mail2.example.com:443`(쉼표 사이 공백 없음).

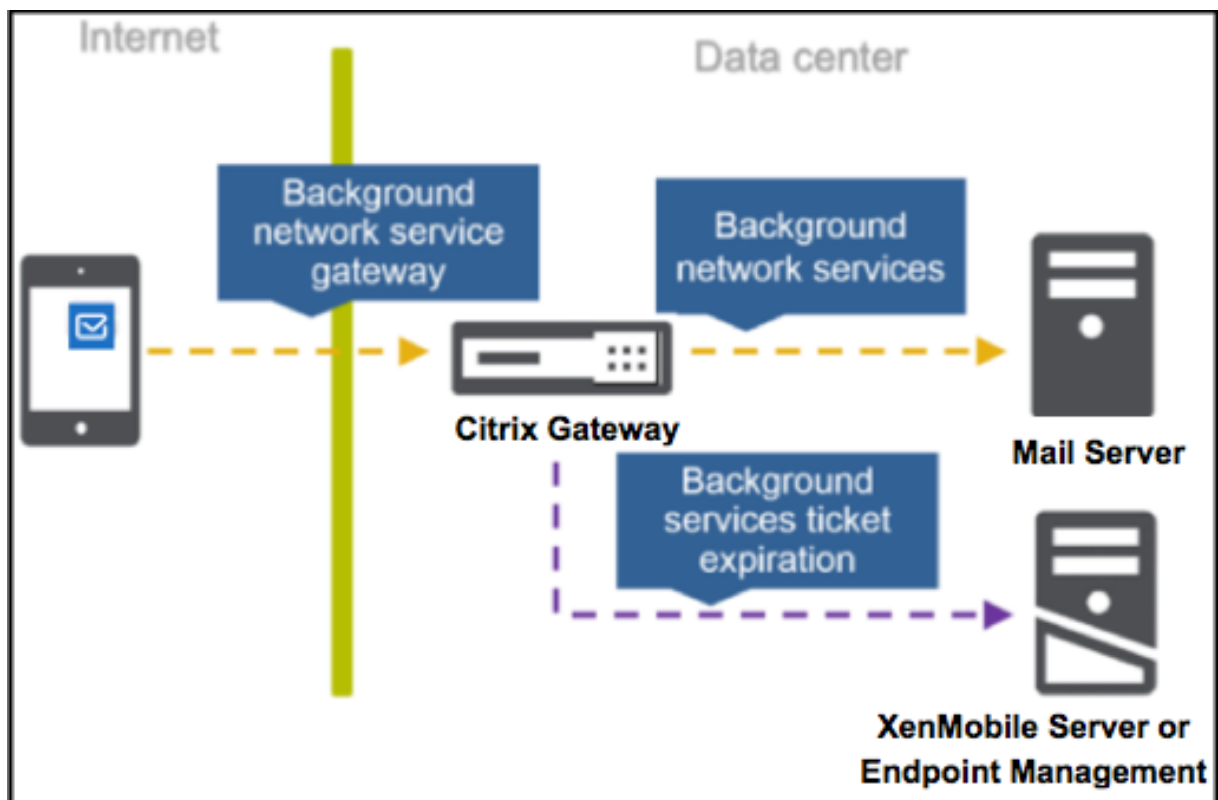
백그라운드 네트워크 서비스 게이트웨이: 백그라운드 네트워크 서비스 게이트웨이 정책은 메일 서버에 연결하기 위해 Secure Mail 이 사용하는 Citrix Gateway 를 지정합니다. Citrix Gateway 주소의 경우 `citrixgatewayFQDN:portnumber`를 포함하십시오. 예: `gateway3.example.com:443`.

백그라운드 서비스 티켓 만료: 이 정책은 백그라운드 네트워크 서비스 티켓의 유효 기간을 지정합니다. Secure Mail 이 Citrix Gateway 를 통해 메일 서버에 연결하는 경우 Citrix Endpoint Management 에서 내부 메일 서버에 연결하는 데 사용할 토큰을 발급합니다. 이 설정은 Secure Mail 에서 이 토큰을 사용할 수 있는 기간을 결정합니다. 토큰이 활성 상태인 경우 메일 서버에 대한 인증 및 연결을 위한 새 토큰이 필요 없습니다. 시간 제한이 만료되면 사용자가 다시 로그인해야 새 토큰이 생성됩니다. 토큰의 기본값은 168 시간 (7 일) 입니다.

백그라운드 서비스를 위한 MDX 앱 정책에 대한 자세한 내용은 다음을 참조하십시오.

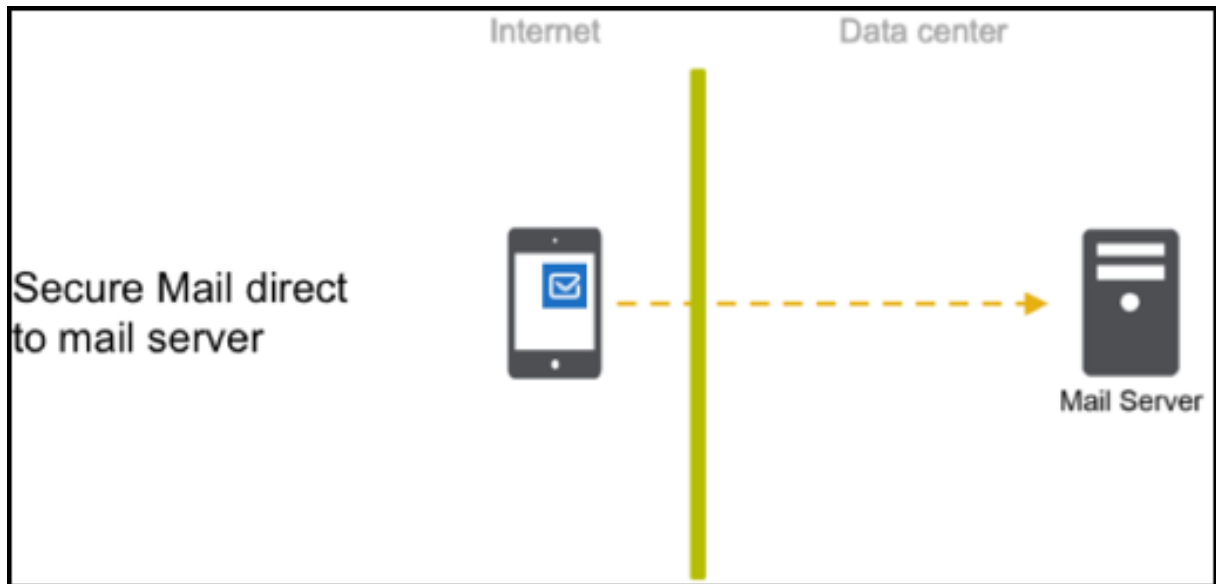
- [Android 에 대한 Secure Mail 앱 설정 정책](#)
- [iOS 에 대한 Secure Mail 앱 설정 정책](#)

다음 그림에서는 통신 흐름 및 이러한 정책이 적용되는 곳을 보여 줍니다.



다음 그림은 메일 서버로의 Secure Mail 연결 유형을 보여 줍니다. 각 그림 뒤에는 관련된 정책 설정의 목록이 나와 있습니다.

메일 서버로의 직접 연결



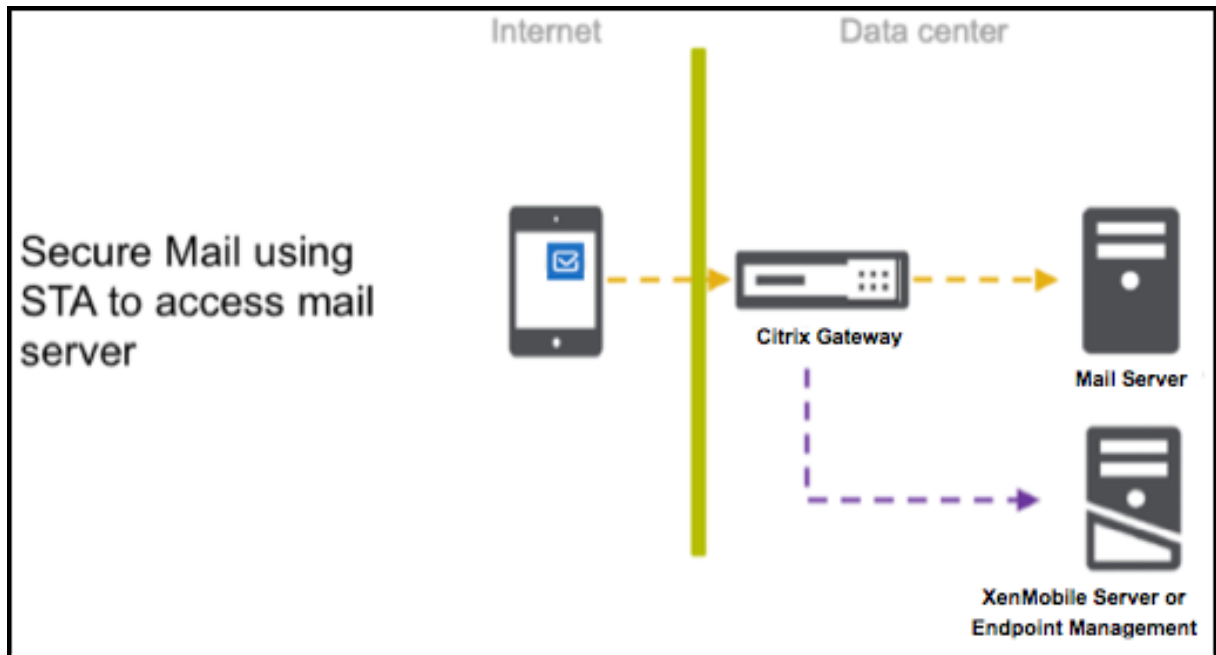
메일 서버로의 직접 연결에 대한 정책:

- 네트워크 액세스: 제한 없음

네트워크 액세스가 제한된 경우 다음 정책이 적용되지 않습니다.

- 백그라운드 네트워크 서비스: 해당 없음
- 백그라운드 서비스 티켓 만료: 해당 없음
- 백그라운드 네트워크 서비스 게이트웨이: 해당 없음

STA 를 통한 메일 서버로의 연결



STA 를 통해 메일 서버에 연결하기 위한 정책:

- 네트워크 액세스: 터널링됨 - 웹 **SSO**
- 백그라운드 네트워크 서비스: `mail.example.com:443`, `mail1.example1.com:443`, `outlook.office365.com:443` or vanity URL:443
- 백그라운드 서비스 티켓 만료: **168**
- 백그라운드 네트워크 서비스 게이트웨이: `gateway3.example.com:443`

참고:

STA 연결은 장시간 세션 연결을 지원하므로 Citrix 에서는 Secure Mail 에 STA 연결을 사용하도록 권장합니다.

STA 에 대한 자세한 내용은 이 [Citrix Knowledge Center 문서](#)를 참조하십시오.

Exchange Server 또는 IBM Notes Traveler 서버 통합

February 27, 2024

Secure Mail 이 메일 서버와 계속 동기화되도록 하려면 내부 네트워크에 있거나 Citrix Gateway 뒤에 있는 Exchange Server 또는 IBM Notes Traveler 서버와 Secure Mail 을 통합합니다.

- Secure Mail 에 대한 백그라운드 서비스를 구성하려면 [Secure Mail 에 대한 백그라운드 서비스](#)를 참조하십시오.
- Secure Mail 에 대한 IBM Notes Traveler 서버를 구성하려면 [Secure Mail 을 위한 IBM Notes Traveler 서버 구성](#)을 참조하십시오.

중요:

Secure Mail 의 메일을 IBM Notes Traveler(이전의 IBM Lotus Notes Traveler) 와 동기화할 수 없습니다. 이 Lotus Notes 타사 기능은 현재 지원되지 않습니다. 따라서 예를 들어 Secure Mail 에서 회의 메일을 삭제하는 경우 IBM Notes Traveler 서버에서 메일이 삭제되지 않습니다. [CXM-47936]

동기화는 Secure Notes 와 Secure Tasks 에 대해서도 가능합니다. 그러나 Secure Notes 및 Secure Tasks 는 2018 년 12 월 31 일에 EOL(수명 종료) 상태에 도달했습니다. 자세한 내용은 [EOL 및 사용되지 않는 앱](#) 을 참조하십시오.

- iOS 용 Secure Notes 를 동기화하려면 iOS 용 Secure Notes 를 Exchange Server 와 통합합니다.
- Secure Notes 와 Android 용 Secure Tasks 를 동기화하려면 Android 용 Secure Mail 계정을 사용합니다.

Secure Mail, Secure Notes 및 Secure Tasks 를 Citrix Endpoint Management(이전의 XenMobile) 에 추가하는 경우 [백그라운드 서비스 구성에 대한 MDX 앱 정책](#) 에 설명된 대로 MDX 정책을 구성합니다.

참고:

Android 및 iOS 용 Secure Mail 은 Notes Traveler 서버에 지정된 전체 경로를 지원합니다. 예: <https://mail.example.com/traveler/Microsoft-Server-ActiveSync>.

이제 Traveler 서버를 위한 웹 사이트 대체 규칙으로 Domino 디렉터리를 구성하지 않아도 됩니다.

Secure Mail 을 위한 IBM Notes Traveler 서버 구성

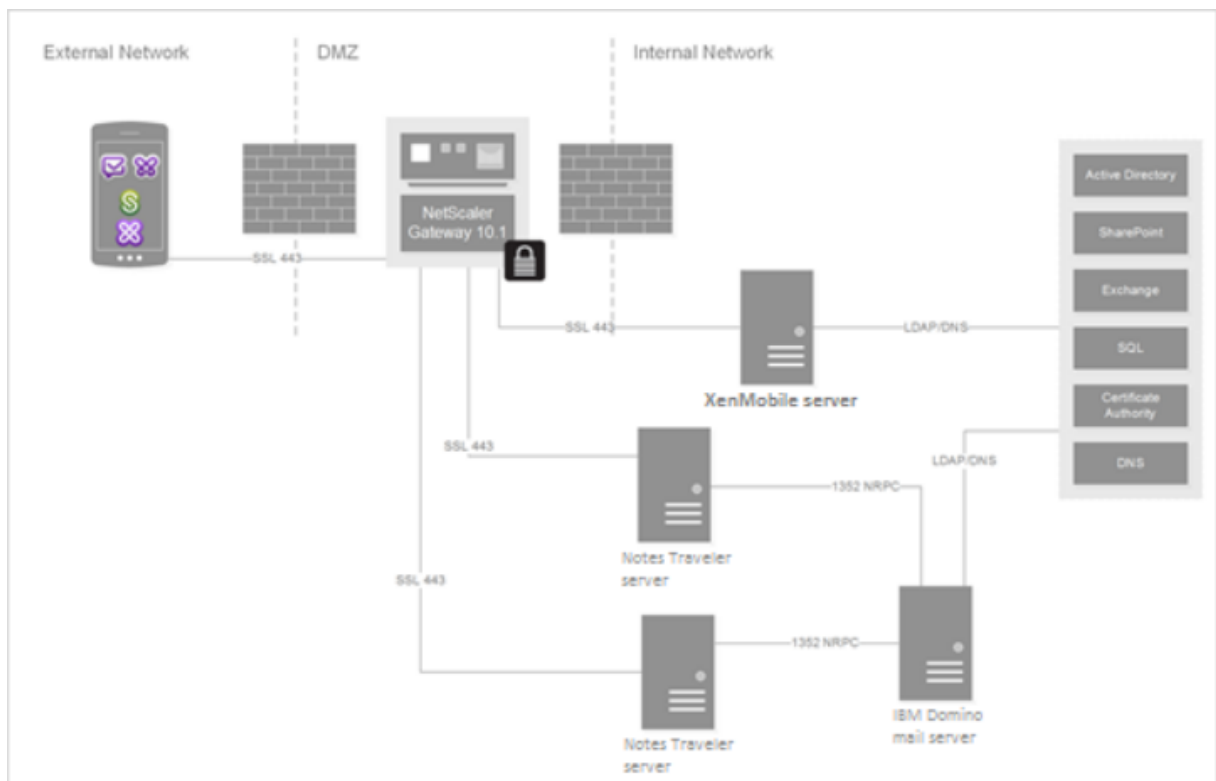
IBM Notes 환경에서는 Secure Mail 을 배포하기 전에 IBM Notes Traveler 서버를 구성해야 합니다. 이 섹션에서는 이 구성에 대한 배포 이미지 및 시스템 요구 사항을 보여 줍니다.

중요:

Notes Traveler 서버에서 SSL 3.0 을 사용하는 경우, SSL 3.0 에는 SSL 3.0 을 사용하여 서버에 연결하는 앱에 영향을 미치는 메시지 가로채기 (man-in-the-middle) 공격의 일종인 POODLE(Padding Oracle On Downgraded Legacy Encryption) 공격이라고 하는 취약점이 있다는 것에 유의하십시오. POODLE 공격으로 인한 취약점을 해결하기 위해 Secure Mail 은 기본적으로 SSL 3.0 연결이 사용되지 않도록 설정하고 TLS 1.0 을 사용하여 서버에 연결합니다. 따라서 Secure Mail 은 SSL 3.0 을 사용하는 Notes Traveler 서버에 연결할 수 없습니다. 권장되는 해결 방법에 대한 자세한 내용은 [Exchange Server 또는 IBM Notes Traveler 서버 통합](#) 에서 SSL/TLS 보안 수준 구성 섹션을 참조하십시오.

IBM Notes 환경에서는 Secure Mail 을 배포하기 전에 IBM Notes Traveler 서버를 구성해야 합니다.

다음 다이어그램은 샘플 배포에서의 IBM Notes Traveler 서버 및 IBM Domino 메일 서버의 네트워크 배치를 보여 줍니다.



시스템 요구 사항

인프라 서버 요구 사항

- IBM Domino Mail Server 9.0.1
- IBM Notes Traveler 9.0.1

인증 프로토콜

- Domino 데이터베이스
- Lotus Notes 인증 프로토콜
- Lightweight Directory 인증 프로토콜

포트 요구 사항

- Exchange: 기본 SSL 포트는 443입니다.
- IBM Notes: SSL 은 포트 443 에서 지원됩니다. 비 SSL 은 기본적으로 포트 80 에서 지원됩니다.

SSL/TLS 보안 수준 구성

Citrix 는 위의 중요 참고 사항에서 설명된 POODLE 공격으로 인한 취약점을 해결하기 위해 Secure Mail 을 수정했습니다. Notes Traveler 서버가 SSL 3.0 을 사용하는 경우 연결이 사용되도록 하려면 IBM Notes Traveler 서버 9.0 에서 TLS 1.2 를 사용하여 문제를 해결하는 것이 좋습니다.

IBM 은 Notes Traveler 의 서버 간 보안 통신에서 SSL 3.0 이 사용되는 것을 방지하기 위한 패치를 제공합니다. 2014 년 11 월에 릴리스된 이 패치는 Notes Traveler 서버 버전 9.0.1 IF7, 9.0.0.1 IF8 및 8.5.3 업그레이드 팩 2 IF8 에 임시 픽스 업데이트로 포함되어 있으며, 향후의 모든 릴리스에 포함될 예정입니다.

또 다른 해결 방법은 Secure Mail 을 Endpoint Management 에 추가할 때 연결 보안 수준 정책을 **SSLv3** 및 **TLS** 로 변경하는 것입니다. 이 문제에 대한 최신 정보는 [SSLv3 Connections Disabled by Default on Secure Mail 10.0.3\(Secure Mail 10.0.3 에서 기본적으로 사용 안 함으로 설정되는 SSLv3 연결\)](#)을 참조하십시오.

다음 표에는 Secure Mail 에서 지원하는 프로토콜이 연결 보안 수준 정책 값에 따라 운영 체제별로 나와 있습니다. 또한 메일 서버는 프로토콜을 협상할 수 있어야 합니다.

다음 표에 연결 보안 수준이 SSLv3 및 TLS 인 경우 Secure Mail 에 대해 지원되는 프로토콜이 나와 있습니다.

운영 체제 유형	SSLv3	TLS
iOS 9 이상	아니요	예
Android M 이전	예	예
Android M 및 Android N	예	예
Android O	아니요	예

다음 표에는 연결 보안 수준이 TLS 인 경우에 Secure Mail 에 대해 지원되는 프로토콜이 나와 있습니다.

운영 체제 유형	SSLv3	TLS
iOS 9 이상	아니요	예
Android M 이전	아니요	예
Android M 및 Android N	아니요	예
Android O	아니요	예

Notes Traveler 서버 구성

다음 정보는 IBM Domino Administrator 클라이언트의 구성 페이지에 관한 것입니다.

- 보안: 인터넷 인증은 Fewer name variations with higher security(보안 강화를 위해 이름 변형을 거의 허용 안 함) 으로 설정되어 있습니다. 이 설정은 LDAP 인증 프로토콜에서 UID 를 AD 사용자 ID 에 매핑하는 데 사용됩니다.

- **NOTES.INI** 설정: **NTS_AS_ENFORCE_POLICY=false** 를 추가합니다. 이렇게 하면 Secure Mail 정책을 Traveler 대신 Endpoint Management 에서 관리할 수 있습니다. 이 설정은 현재의 고객 측 배포와 충돌할 수 있지만, Endpoint Management 배포에서의 장치 관리를 간소화합니다.
- 동기화 프로토콜: IBM Notes 의 SyncML 및 모바일 장치 동기화는 현재 Secure Mail 에서 지원되지 않습니다. Secure Mail 동기화는 Traveler 서버에 내장된 Microsoft ActiveSync 프로토콜을 통해 메일, 일정 및 연락처 항목을 동기화합니다. SyncML 이 기본 프로토콜로 적용되는 경우 Secure Mail 은 Traveler 인프라를 통해 다시 연결할 수 없습니다.
- **Domino** 디렉터리 구성 - 웹 인터넷 사이트: Traveler 에서 양식 기반 인증이 사용되지 않도록 세션 인증을 재정의합니다.

Secure Mail 에 대한 S/MIME 구성

February 27, 2024

Secure Mail 은 S/MIME(Secure/Multipurpose Internet Mail Extensions) 을 지원하여 보안 강화를 위해 사용자가 메시지에 서명하고 메시지를 암호화할 수 있게 합니다. 서명은 메시지를 보낸 식별된 사람이 사칭자가 아님을 받는 사람에게 확인시켜 줍니다. 암호화는 호환되는 인증서를 가진 받는 사람만 메시지를 열 수 있게 합니다.

S/MIME 에 대한 자세한 내용은 Microsoft TechNet 를 참조하십시오.

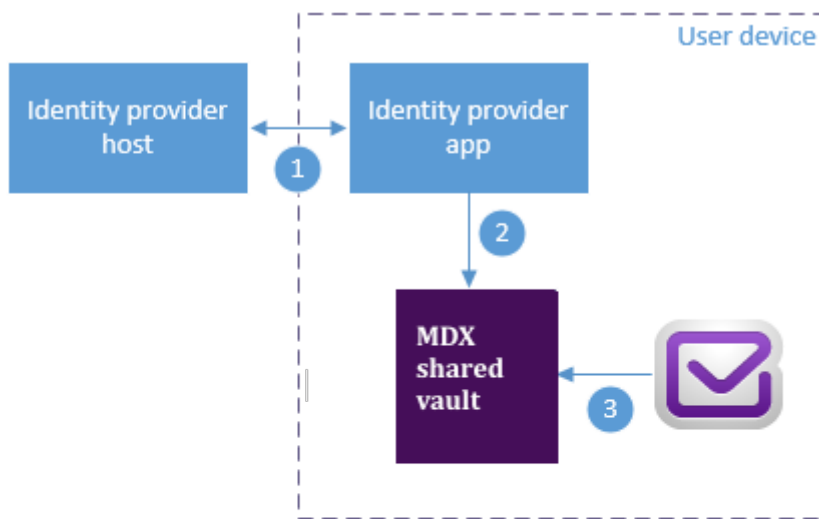
다음 표에서 X 는 장치 OS 에서 Secure Mail 이 S/MIME 기능을 지원함을 나타냅니다.

S/MIME 기능	iOS	Android
디지털 ID 공급자 통합: Secure Mail 을 지원되는 타사 디지털 ID 공급자와 통합할 수 있습니다. ID 공급자 호스트는 사용자 장치의 ID 공급자 앱에 인증서를 공급합니다. 이 앱은 민감한 앱 데이터의 보안 스토리지 영역인 Endpoint Management 공유 저장소로 인증서를 보냅니다. Secure Mail 은 공유 저장소에서 인증서를 얻습니다. 자세한 내용은 디지털 ID 공급자와의 통합 섹션을 참조하십시오.	X	

S/MIME 기능	iOS	Android
파생된 자격 증명 지원	Secure Mail 이 파생된 자격 증명을 인증서 원본으로 지원합니다. 파생된 자격 증명에 대한 자세한 내용은 Citrix Endpoint Management 설명서의 iOS 용 파생된 자격 증명 문서를 참조하십시오.	
전자 메일에 의한 인증서 배포: 전자 메일로 인증서를 배포하려면 인증서 템플릿을 생성한 후에 템플릿을 사용하여 사용자 인증서를 요청해야 합니다. 인증서를 설치하고 유효성 검사를 수행한 후에 사용자 인증서를 내보내고 전자 메일로 사용자에게 보냅니다. 그러면 사용자가 Secure Mail 에서 전자 메일을 열고 인증서를 가져옵니다. 자세한 내용은 전자 메일로 인증서 배포 섹션을 참조하십시오.	X	X
단일 용도 인증서 자동으로 가져오기: Secure Mail 은 서명 또는 암호화 전용 인증서인지 감지한 후에 자동으로 인증서를 가져오고 사용자에게 알려 줍니다. 인증서가 두 가지 용도로 사용되는 경우 해당 인증서를 가져오라는 메시지가 사용자에게 표시됩니다.	X	

디지털 ID 공급자와의 통합

다음 다이어그램은 디지털 ID 공급자 호스트에서 Secure Mail 로 인증서가 이동하는 경로를 보여 줍니다. 이러한 작업은 Secure Mail 을 지원되는 타사 디지털 ID 공급자 서비스와 통합할 때 이루어집니다.



- 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

MDX 공유 저장소는 인증서 같은 민감한 앱 데이터를 위한 보안 스토리지 영역입니다. Endpoint Management 에서 사용하도록 설정된 앱만 공유 저장소에 액세스할 수 있습니다.

사전 요구 사항

Secure Mail 은 Entrust IdentityGuard 와의 통합을 지원합니다.

통합 구성

1. ID 공급자 앱을 준비하여 사용자에게 제공합니다.

- Entrust 에 연락하여 .ipa 가 래핑되도록 합니다.
- MDX Toolkit 을 사용하여 앱을 래핑합니다.

Endpoint Management 환경 외부에서 이 앱의 다른 버전을 이미 보유하고 있는 사용자에게 앱을 배포할 경우 이 앱에 대해 고유한 앱 ID 를 사용하십시오. 이 앱 및 Secure Mail 에 대해 동일한 프로비전 프로필을 사용하십시오.

- 이 앱을 Endpoint Management 에 추가하고 Endpoint Management 앱 스토어에 게시합니다.
- ID 공급자 앱을 Secure Hub 로부터 설치해야 한다는 점을 사용자에게 알려 줍니다. 필요에 따라 설치 이후 단계에 대한 지침을 제공합니다.

다음 단계에서 Secure Mail에 대해 S/MIME 정책을 구성하는 방식에 따라, 인증서를 설치하거나 Secure Mail 설정에서 S/MIME이 사용하도록 설정하라는 메시지가 표시될 수 있습니다. 두 절차의 단계는 [iOS용 Secure Mail에서 S/MIME을 사용하도록 설정](#)에 나와 있습니다.

2. Secure Mail을 Endpoint Management에 추가할 경우, 다음 정책을 구성해야 합니다.

- S/MIME 인증서 출처 정책을 공유 저장소로 설정합니다. 그러면 Secure Mail이 디지털 ID 공급자에 의해 공유 저장소에 저장된 인증서를 사용합니다.
- Secure Mail 초기 시작 중에 S/MIME을 사용하도록 설정하려면 처음 Secure Mail 시작 시 S/MIME 사용 정책을 구성합니다. 이 정책은 공유 저장소에 인증서가 있을 경우 Secure Mail이 S/MIME을 사용하도록 설정할지 여부를 결정합니다. 사용 가능한 인증서가 없으면 인증서를 가져오라는 메시지가 Secure Mail에서 사용자에게 표시됩니다. 이 정책이 사용되도록 설정하지 않은 경우, 사용자가 Secure Mail 설정에서 S/MIME을 사용하도록 설정할 수 있습니다. 기본적으로 Secure Mail은 S/MIME를 사용하지 않으므로 사용자가 Secure Mail 설정에서 S/MIME를 사용 설정해야 합니다.

파생된 자격 증명 사용

디지털 ID 공급자와 통합하는 대신 파생된 자격 증명을 사용할 수 있습니다.

Secure Mail을 Endpoint Management에 추가할 때 S/MIME 인증서 원본 정책을 파생된 자격 증명으로 구성합니다. 파생된 자격 증명에 대한 자세한 내용은 [iOS용 파생된 자격 증명](#)을 참조하십시오.

전자 메일로 인증서 배포

디지털 ID 공급자와 통합하거나 파생된 자격 증명을 사용하는 대신, 인증서를 전자 메일로 사용자에게 배포할 수 있습니다. 이 옵션에서는 이 섹션에 자세히 설명된 다음과 같은 일반 단계가 필요합니다.

1. Server Manager를 사용하여 Microsoft Certificate Services를 위한 웹 등록이 사용되도록 설정하고 IIS에서의 인증 설정을 확인합니다.
2. 전자 메일 메시지 서명 및 암호화를 위한 인증서 템플릿을 생성합니다. 이러한 템플릿을 사용하여 사용자 인증서를 요청합니다.
3. 인증서를 설치하고 유효성 검사를 수행한 후에 사용자 인증서를 내보내고 전자 메일로 사용자에게 보냅니다.
4. 사용자는 Secure Mail에서 전자 메일을 열고 인증서를 가져옵니다. 이렇게 하면 Secure Mail에서만 인증서를 사용할 수 있습니다. S/MIME을 위한 iOS 프로필에는 인증서가 나타나지 않습니다.

사전 요구 사항

이 섹션에 있는 지침은 다음 구성 요소를 기반으로 합니다.

- XenMobile Server 10 이상

- 지원되는 버전의 Citrix Gateway(이전 명칭: NetScaler Gateway)
- iOS 용 Secure Mail(버전 10.8.10 이상), Android 장치용 Secure Mail(버전 10.8.10 이상)
- 루트 CA(인증 기관) 역할을 하는 Microsoft Certificate Services 를 포함하는 Microsoft Windows Server 2008 R2 이상
- Microsoft Exchange:
 - Exchange Server 2016 누적 업데이트 4
 - Exchange Server 2013 누적 업데이트 15
 - Exchange Server 2010 SP3 업데이트 롤업 16

S/MIME 을 구성하기 전에 다음과 같은 사전 요구 사항을 완료하십시오.

- 루트 및 중간 인증서를 수동으로 또는 Endpoint Management 에서의 자격 증명 장치 정책을 통해 모바일 장치에 배포합니다. 자세한 내용은 [자격 증명 장치 정책](#) 을 참조하십시오.
- Exchange Server 로의 ActiveSync 트래픽을 보안하기 위해 사설 서버 인증서를 사용하는 경우, 다음을 수행하십시오. 모든 루트 및 중간 인증서를 모바일 장치에 설치합니다.

Microsoft Certificate Services 를 위한 웹 등록이 사용되도록 설정

1. 관리 도구로 이동하고 서버 관리자를 선택합니다.
2. **Active Directory** 인증서 서비스 아래에서 인증 기관 웹 등록이 설치되어 있는지 확인합니다.
3. 필요하면 역할 서비스 추가를 선택하여 인증 기관 웹 등록을 설치합니다.
4. 인증 기관 웹 등록을 선택하고 다음을 클릭합니다.
5. 설치가 완료되면 닫기 또는 마침을 클릭합니다.

IIS 에서의 인증 설정 확인

- 사용자 인증서를 요청하는 데 사용되는 웹 등록 사이트 (예: <https://ad.domain.com/certsrv/>) 가 HTTPS 서버 인증서 (개인 또는 공용) 로 보안되는지 확인합니다.
 - 웹 등록 사이트는 HTTPS 를 통해 액세스되어야 합니다.
1. 관리 도구로 이동하고 서버 관리자를 선택합니다.
 2. 웹 서버 (**IIS**) 에서 역할 서비스 아래를 살펴봅니다. 클라이언트 인증서 매핑 인증 및 IIS 클라이언트 인증서 매핑 인증이 설치되어 있는지 확인합니다. 그렇지 않으면 해당 역할 서비스를 설치합니다.
 3. 관리 도구로 이동하여 **IIS(인터넷 정보 서비스)** 관리자를 선택합니다.
 4. **IIS** 관리자 창의 왼쪽에서 웹 등록을 위해 IIS 인스턴스를 실행하고 있는 서버를 선택합니다.
 5. 인증을 클릭합니다.
 6. **Active Directory** 클라이언트 인증서 인증이 사용으로 설정되어 있는지 확인합니다.
 7. 오른쪽 창에서 사이트 > **Default site for Microsoft Internet Information Services(Microsoft Internet Information Services 기본 사이트)** > 바인딩을 클릭합니다.
 8. HTTPS 바인딩이 없으면 이 바인딩을 추가합니다.

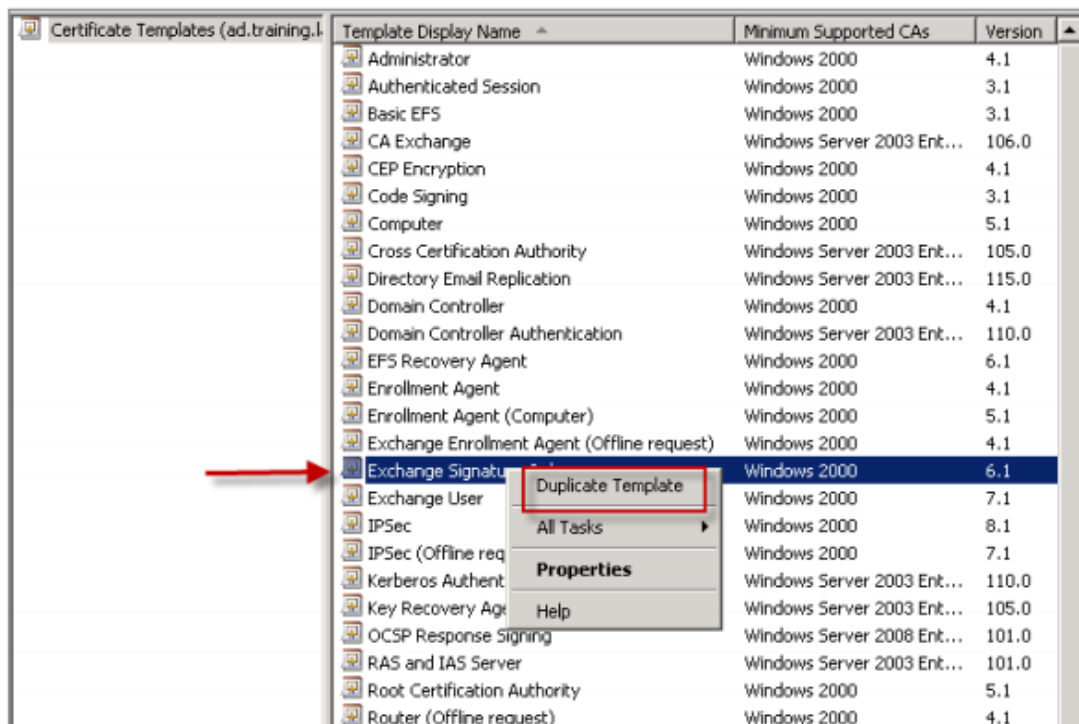
9. 기본 웹 사이트 홈으로 이동합니다.
10. **SSL** 설정을 클릭하고 클라이언트 인증서에 대해 수락을 클릭합니다.

새 인증서 템플릿 생성

Citrix 에서는 전자 메일 메시지 서명 및 암호화를 수행하기 위해 Microsoft Active Directory 인증서 서비스에서 인증서를 생성하도록 권장합니다. 동일한 인증서를 두 가지 용도로 사용하고 암호화 인증서를 보관하는 경우, 서명 인증서를 복구하고 가장 을 허용할 수 있습니다.

다음 절차는 CA(인증 기관) 서버에서 인증서 템플릿을 복제합니다.

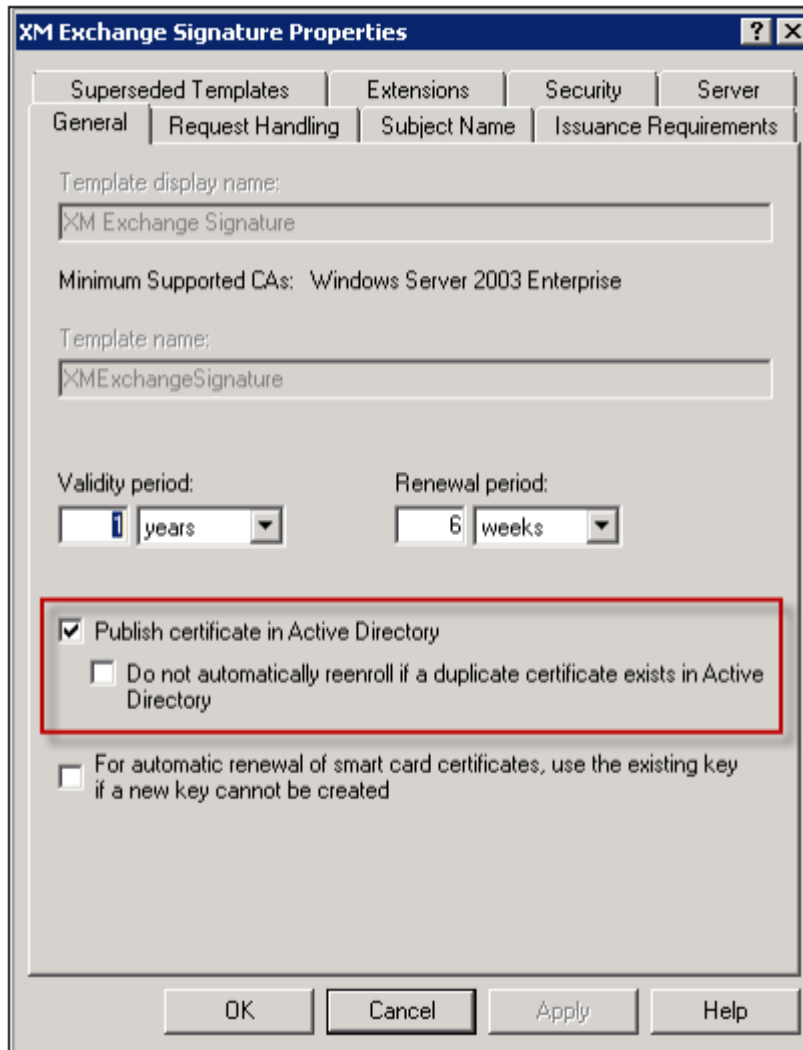
- Exchange 서명만 (서명용)
 - Exchange 사용자 (암호화용)
1. 인증 기관 스냅인을 엽니다.
 2. CA 를 확장하고 인증서 템플릿으로 이동합니다.
 3. 마우스 오른쪽 버튼을 클릭하고 관리를 클릭합니다.
 4. Exchange 서명만 템플릿을 검색하고 템플릿을 마우스 오른쪽 버튼으로 클릭한 후 템플릿 복제를 클릭합니다.



5. 이름을 할당합니다.
6. **Active Directory** 에 인증서 게시 확인란을 선택합니다.

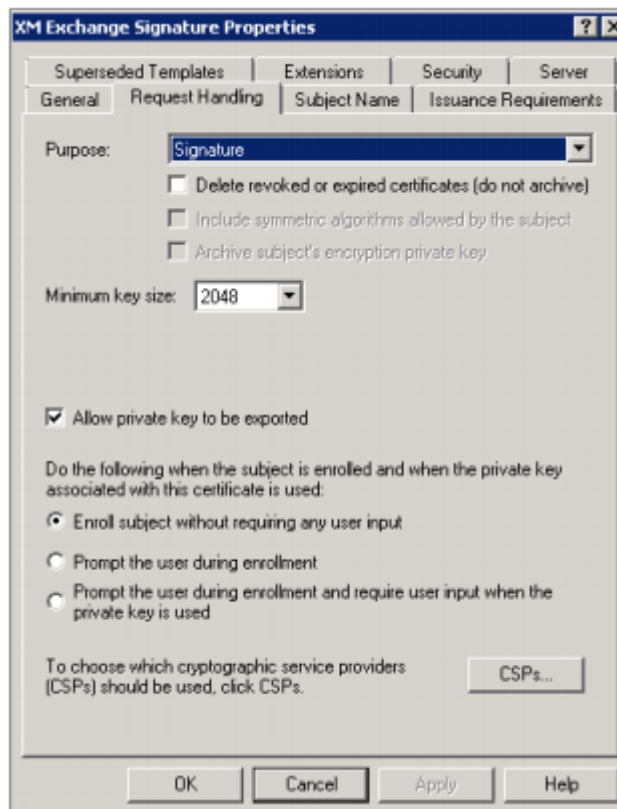
참고:

Active Directory에 인증서 게시 확인란을 선택하지 않으면 사용자가 수동으로 사용자 인증서 (서명 및 암호화 용도)를 게시해야 합니다. 이 작업은 **Outlook** 메일 클라이언트 > 보안 센터 > 전자 메일 보안 > **GAL**(전체 주소 목록)에 게시를 통해 수행할 수 있습니다.

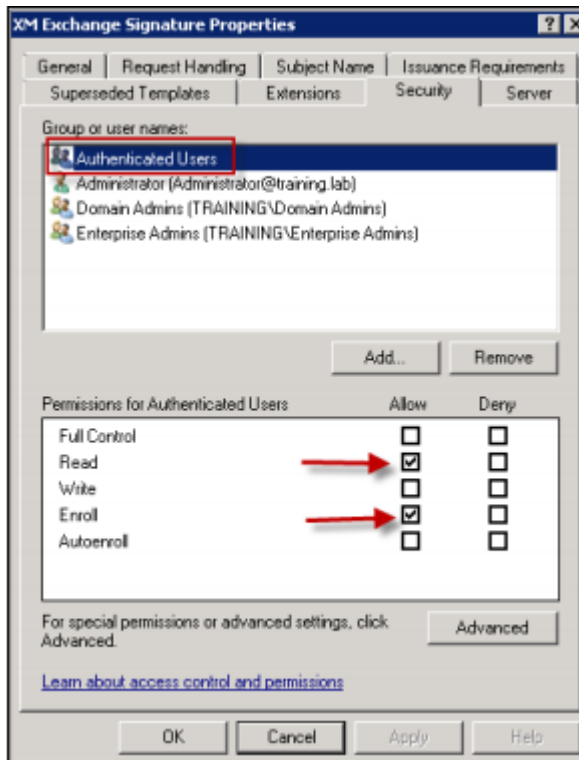


7. 요청 처리 탭을 클릭한 후 다음 매개 변수를 설정합니다.

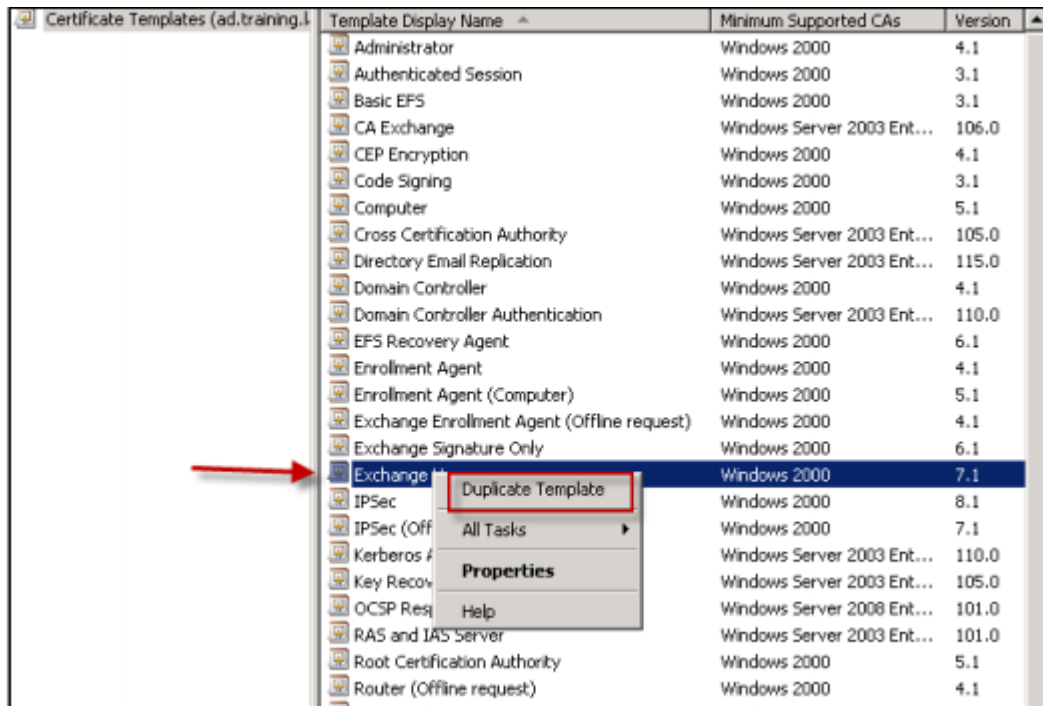
- 용도: 서명
- 최소 키 크기: 2048
- 개인 키를 내보낼 수 있음 확인란: 선택됨
- 사용자 입력 요청 없이 주체 등록 확인란: 선택됨



8. 보안 탭을 클릭하고 그룹 또는 사용자 이름 아래에서 인증된 사용자 또는 원하는 도메인 보안 그룹이 추가되어 있는지 확인합니다. 또한 인증된 사용자의 권한 아래에서 읽기 및 등록 확인란이 허용으로 선택되어 있는지 확인합니다.



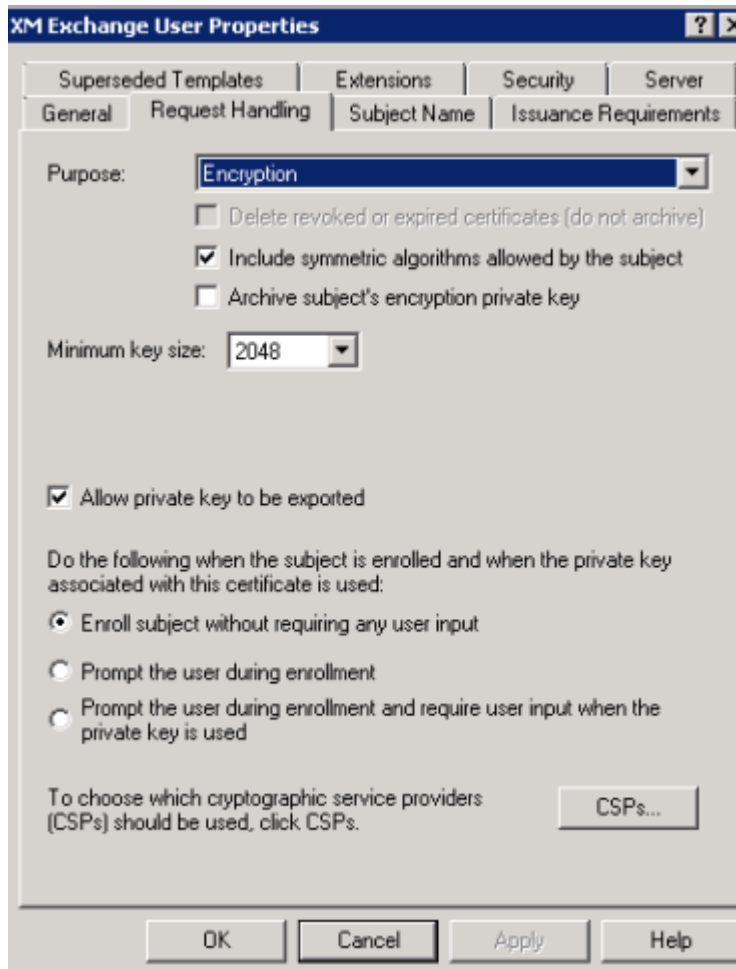
9. 다른 모든 탭과 설정은 기본 설정을 그대로 유지합니다.
10. 인증서 템플릿에서 **Exchange** 사용자를 클릭한 후 4 단계부터 9 단계까지 반복합니다.

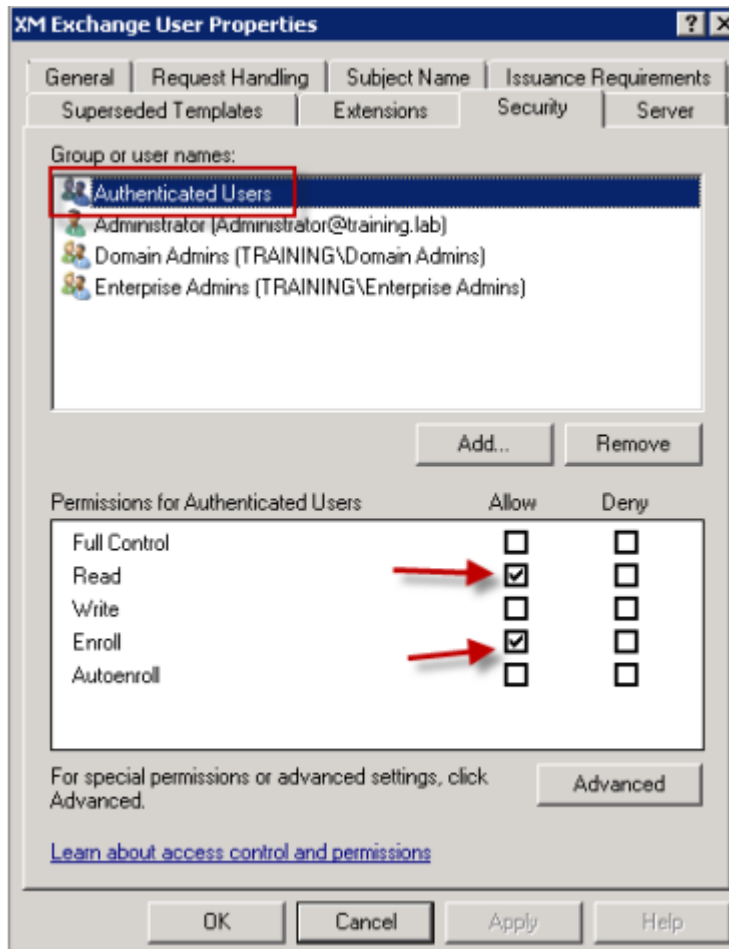


새 Exchange 사용자 템플릿에 대해 원본 템플릿과 동일한 기본 설정을 사용합니다.

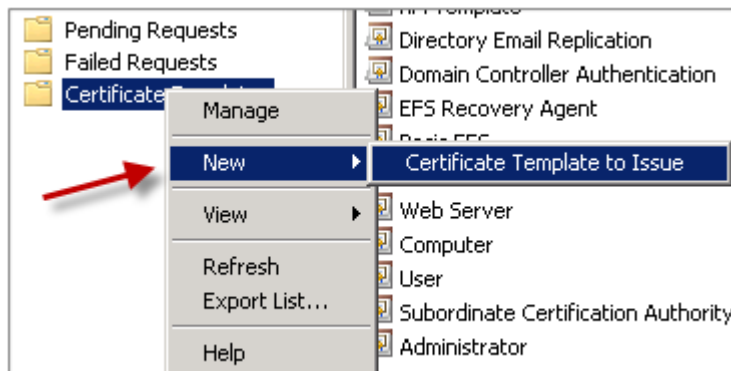
11. 요청 처리 탭을 클릭한 후 다음 매개 변수를 설정합니다.

- 용도: 암호화
- 최소 키 크기: 2048
- 개인 키를 내보낼 수 있음 확인란: 선택됨
- 사용자 입력 요청 없이 주체 등록 확인란: 선택됨





12. 두 템플릿이 생성되면 두 인증서 템플릿을 발급해야 합니다. 새로 만들기를 클릭한 후 발급할 인증서 템플릿을 클릭합니다.



사용자 인증서 요청

이 절차에서는 “user1” 을 사용하여 웹 등록 페이지 (예: <https://ad.domain.com/certsrv/>) 를 탐색합니다. 절차를 수행하려면 보안 전자 메일을 위한 새 사용자 인증서 2 개, 즉 서명용 인증서 1 개 및 암호화용 인증서 1 개가 필요합니다. Secure Mail 을 통해 S/MIME 을 사용할 필요가 있는 다른 도메인 사용자에게 대해서도 동일한 절차를 반복할 수 있습니다.

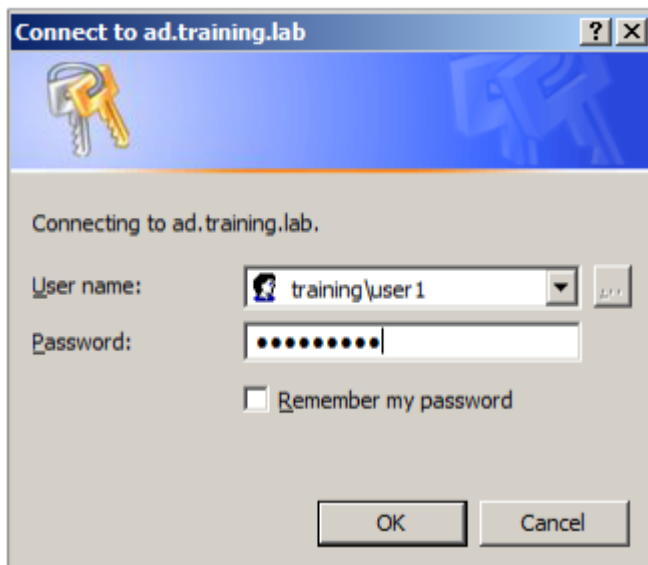
다.

서명 및 암호화용으로 사용자 인증서를 생성하기 위해 Microsoft Certificate Services 에서 웹 등록 사이트 (예: <https://ad.domain.com/certsrv/>) 를 통해 수동 등록이 사용됩니다. 다른 방법은 이 기능을 사용할 사용자 그룹에 대해 그룹 정책을 통해 자동 등록을 구성하는 것입니다.

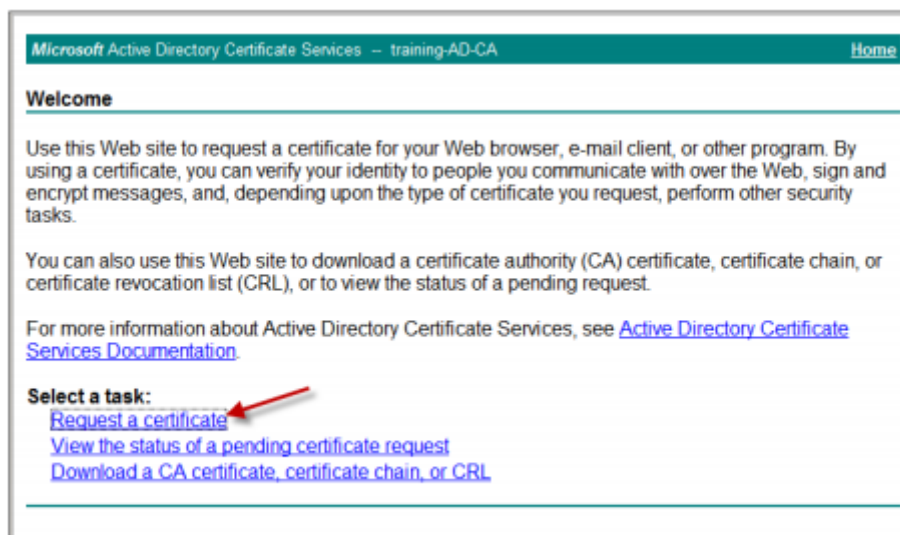
1. Windows 기반 컴퓨터에서 Internet Explorer 를 열고 웹 등록 사이트로 이동하여 새 사용자 인증서를 요청합니다.

참고:

인증서를 요청하려면 올바른 도메인 사용자로 로그인해야 합니다.



2. 로그인한 상태에서 인증서 요청을 클릭합니다.



3. 고급 인증서 요청을 클릭합니다.

- 이 **CA** 에 요청을 만들어 제출합니다를 클릭합니다.
- 서명용 사용자 인증서를 생성합니다. 적절한 템플릿 이름을 선택하고 사용자 설정을 입력한 후 요청 형식으로 이동하여 **PKCS10** 을 선택합니다.

요청이 제출되었습니다.

Microsoft Active Directory Certificate Services -- training-AD-CA [Home](#)

Advanced Certificate Request

Certificate Template:

XM Exchange Signature

Identifying Information For Offline Template:

Name: user1

E-Mail: user1@training.lab

Company: Citrix

Department: Support Readiness

City: FTL

State: FL

Country/Region: US

Key Options:

☒ Create new key set ☐ Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0

Key Usage: ☒ Signature

Key Size: 2048 (Min: 2048, Max: 10384, common key sizes: 2048 4096 8192 10384)

☒ Automatic key container name ☐ User specified key container name

☒ Mark keys as exportable

☐ Enable strong private key protection

Additional Options:

Request Format: ☐ CMC ☒ PKCS10

Hash Algorithm: sha1

Only used to sign request.

☐ Save request

- 이 인증서 설치를 클릭합니다.
- 인증서가 성공적으로 설치되었는지 확인합니다.

Microsoft Active Directory Certificate Services -- training-AD-CA

Certificate Installed

Your new certificate has been successfully installed.

- 이제는 전자 메일 메시지 암호화를 위해 동일한 절차를 반복합니다. 동일한 사용자로 웹 등록 사이트에 로그인한 상태에서 홈 링크로 이동하여 새 인증서를 요청합니다.
- 새 암호화 템플릿을 선택한 후 5 단계에서 입력한 동일한 사용자 설정을 입력합니다.

Microsoft Active Directory Certificate Services -- training-AD-CA [Home](#)

Advanced Certificate Request

Certificate Template:

XM Exchange User

Identifying Information For Offline Template:

Name: user1
 E-Mail: user1@training.lab
 Company: Citrix
 Department: Support Readiness
 City: FTL
 State: FL
 Country/Region: US

Key Options:

☒ Create new key set ☐ Use existing key set
 CSP: Microsoft Enhanced Cryptographic Provider v1.0
 Key Usage: ☒ Exchange
 Key Size: 2048 (Min: 2048 Max: 16384 (common key sizes: 2048 4096 8192 16384))
☒ Automatic key container name ☐ User specified key container name
☒ Mark keys as exportable
☐ Enable strong private key protection

Additional Options:

Request Format: ☐ CMC ☒ PKCS10
 Hash Algorithm: sha1
Only used to sign request.
☐ Save request

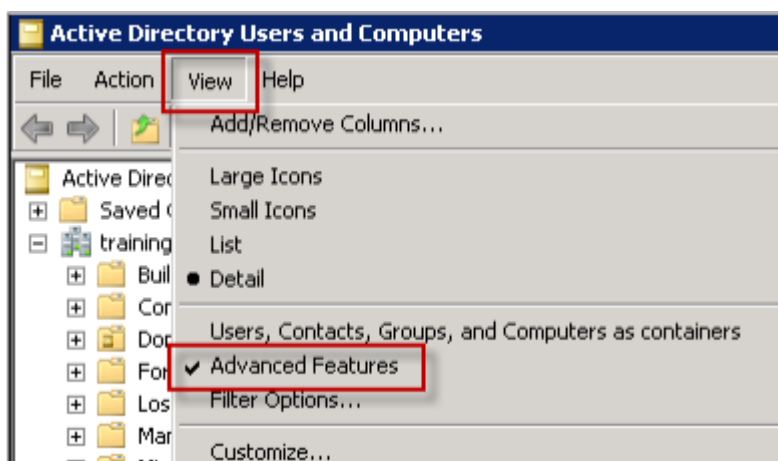
10. 인증서를 올바르게 설치했는지 확인하고 동일한 절차를 반복하여 다른 도메인 사용자를 위해 한 쌍의 사용자 인증서를 생성합니다. 이 예제에서는 동일한 절차를 따르고 “User2”를 위해 한 쌍의 인증서를 생성합니다.

참고:

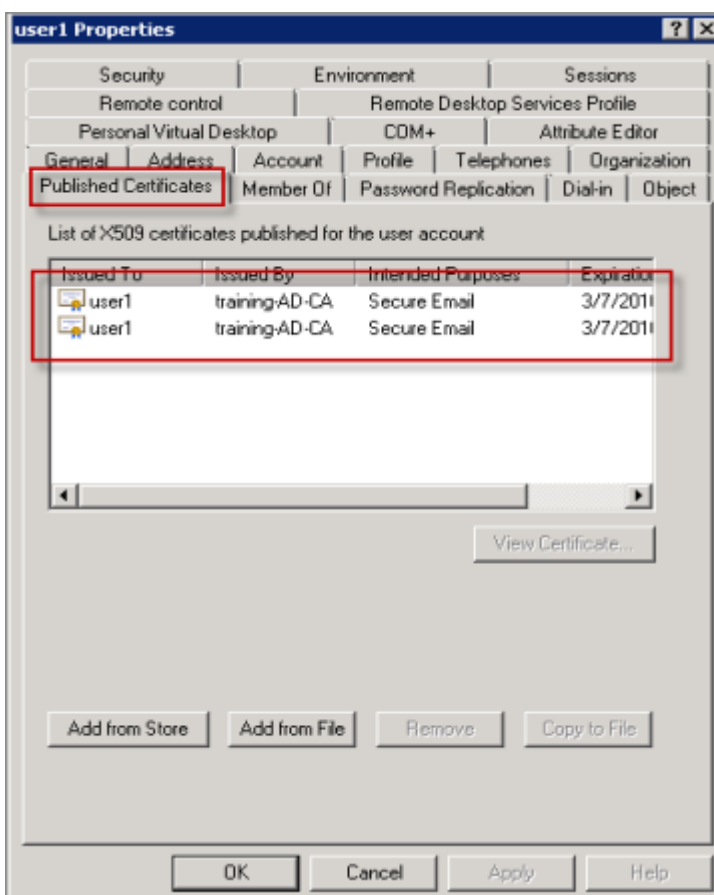
이 절차에서는 동일한 Windows 기반 컴퓨터를 사용하여 “User2”를 위한 두 번째 인증서 쌍을 요청합니다.

게시된 인증서 유효성 검사

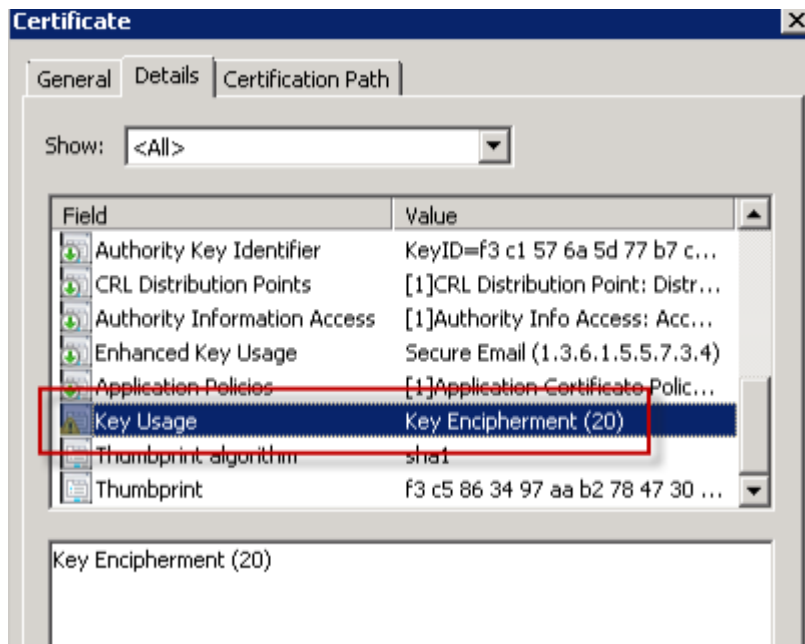
1. 인증서가 도메인 사용자 프로필에 올바르게 설치되었는지 확인하려면 **Active Directory** 사용자 및 컴퓨터 > 보기 > 고급 기능으로 이동합니다.



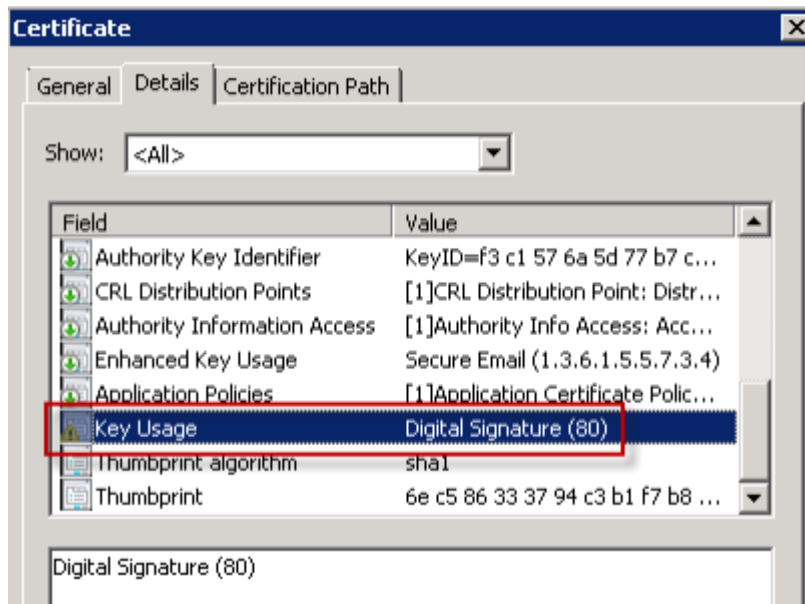
2. 사용자 (이 예제에서는 User1)의 속성으로 이동한 후 게시된 인증서 탭을 클릭합니다. 두 인증서를 사용할 수 있는지 확인합니다. 인증서별로 특정 용도가 있는지도 확인할 수 있습니다.



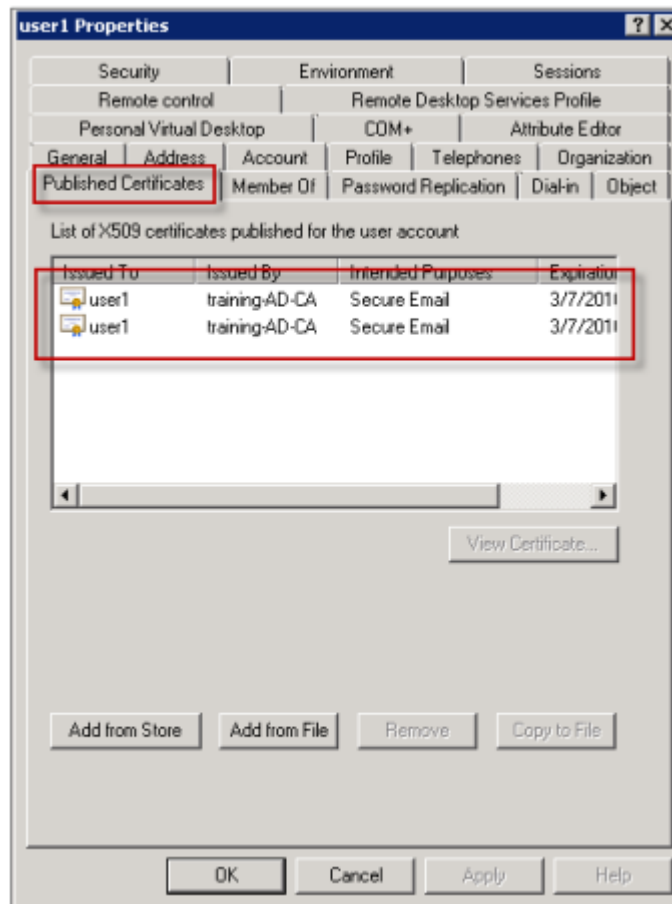
이 그림은 전자 메일 메시지 암호화를 위한 인증서를 보여 줍니다.



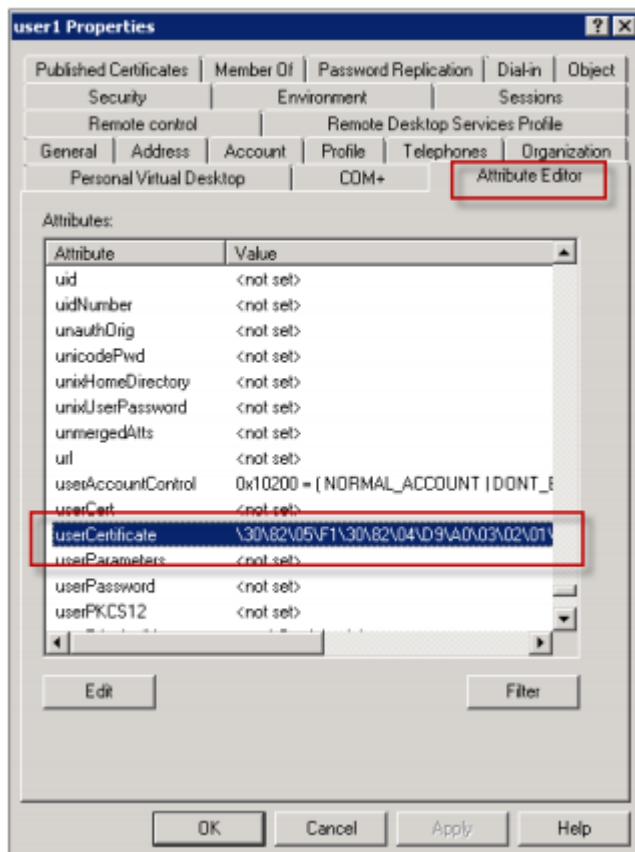
이 그림은 전자 메일 메시지 서명을 위한 인증서를 보여 줍니다.



암호화된 올바른 인증서가 사용자에게 할당되어 있는지 확인합니다. 이 정보는 **Active Directory** 사용자 및 컴퓨터 > 사용자 속성에서 확인할 수 있습니다.



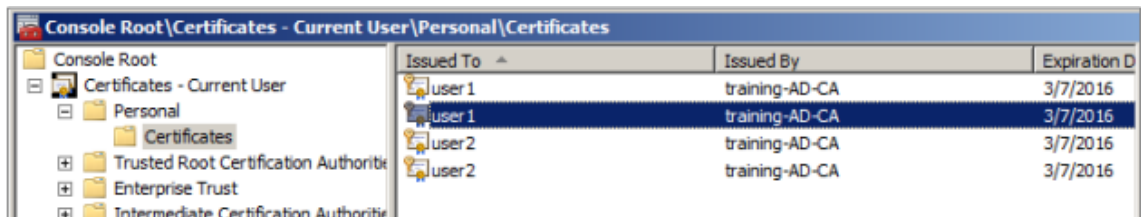
Secure Mail 은 LDAP 쿼리를 통해 사용자 개체 특성 `userCertificate` 를 확인하는 방식으로 작동합니다. 이 값은 특성 편집기 탭에서 읽을 수 있습니다. 이 필드가 비어 있거나 암호화된 사용자 인증서가 올바르게 없으면 Secure Mail 이 메시지를 암호화하거나 해독할 수 없습니다.



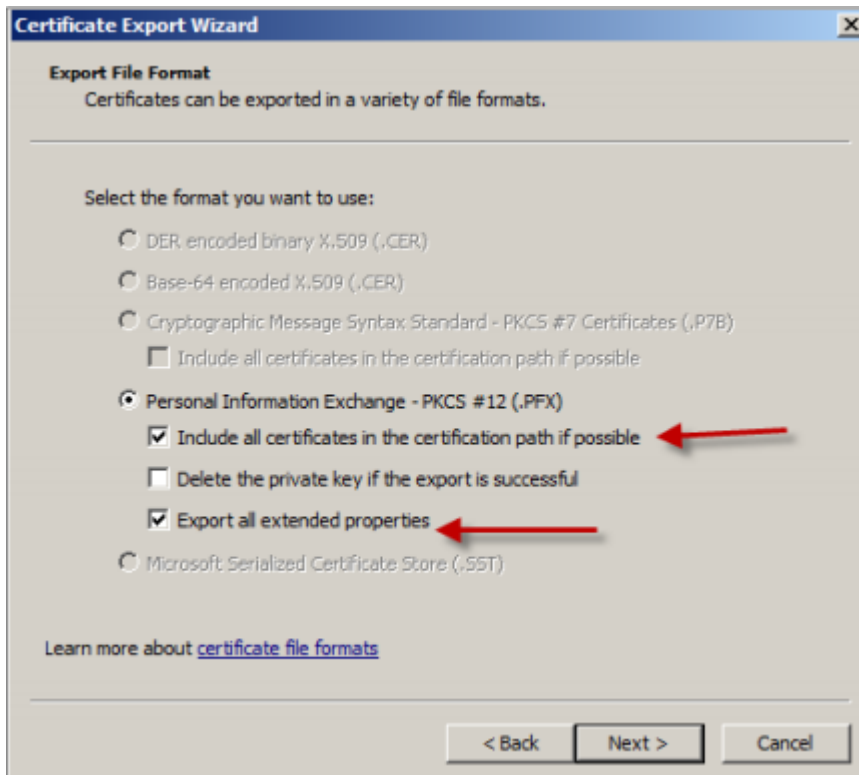
사용자 인증서 내보내기

이 절차에서는 “User1” 및 “User2” 인증서 쌍을.PFX(PKCS#12) 형식으로 개인 키와 함께 내보냅니다. 내보낼 때 인증서는 OWA(Outlook Web Access) 를 사용하여 전자 메일을 통해 사용자에게 보내집니다.

1. MMC 콘솔을 열고 인증서 - 현재 사용자 스냅인으로 이동합니다. “User1” 및 User2” 인증서 쌍이 모두 표시됩니다.



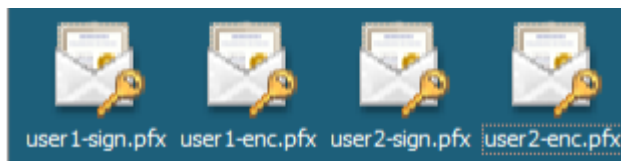
2. 인증서를 마우스 오른쪽 버튼으로 클릭하고 모든 작업 > 내보내기를 클릭합니다.
3. 예, 개인 키를 내보냅니다를 선택하여 개인 키를 내보냅니다.
4. 가능하면 인증 경로에 있는 인증서 모두 포함 및 확장 속성 모두 내보내기 확인란을 선택합니다.



5. 첫 번째 인증서를 내보냈으면 사용자의 나머지 인증서에 대해 동일한 절차를 반복합니다.

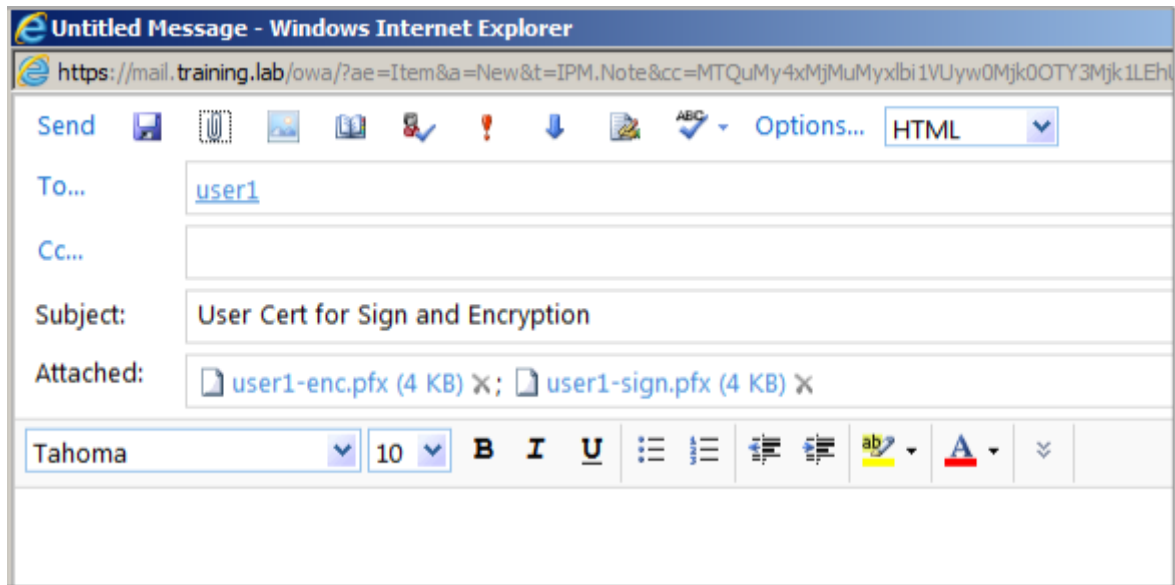
참고:

참고: 어떤 인증서가 서명 인증서이고 어떤 인증서가 암호화 인증서인지 명확히 구분되도록 레이블을 지정합니다. 이 예에서 인증서는 userX-sign.pfx 및 “userX-enc.pfx” 로 레이블이 지정됩니다.



전자 메일을 통해 인증서 보내기

모든 인증서가 PFX 형식으로 내보내진 경우, OWA(Outlook Web Access) 를 사용하여 전자 메일을 통해 인증서를 보낼 수 있습니다. 이 예에서 로그인 이름은 User1 이고 보낸 전자 메일에는 두 인증서가 포함됩니다.



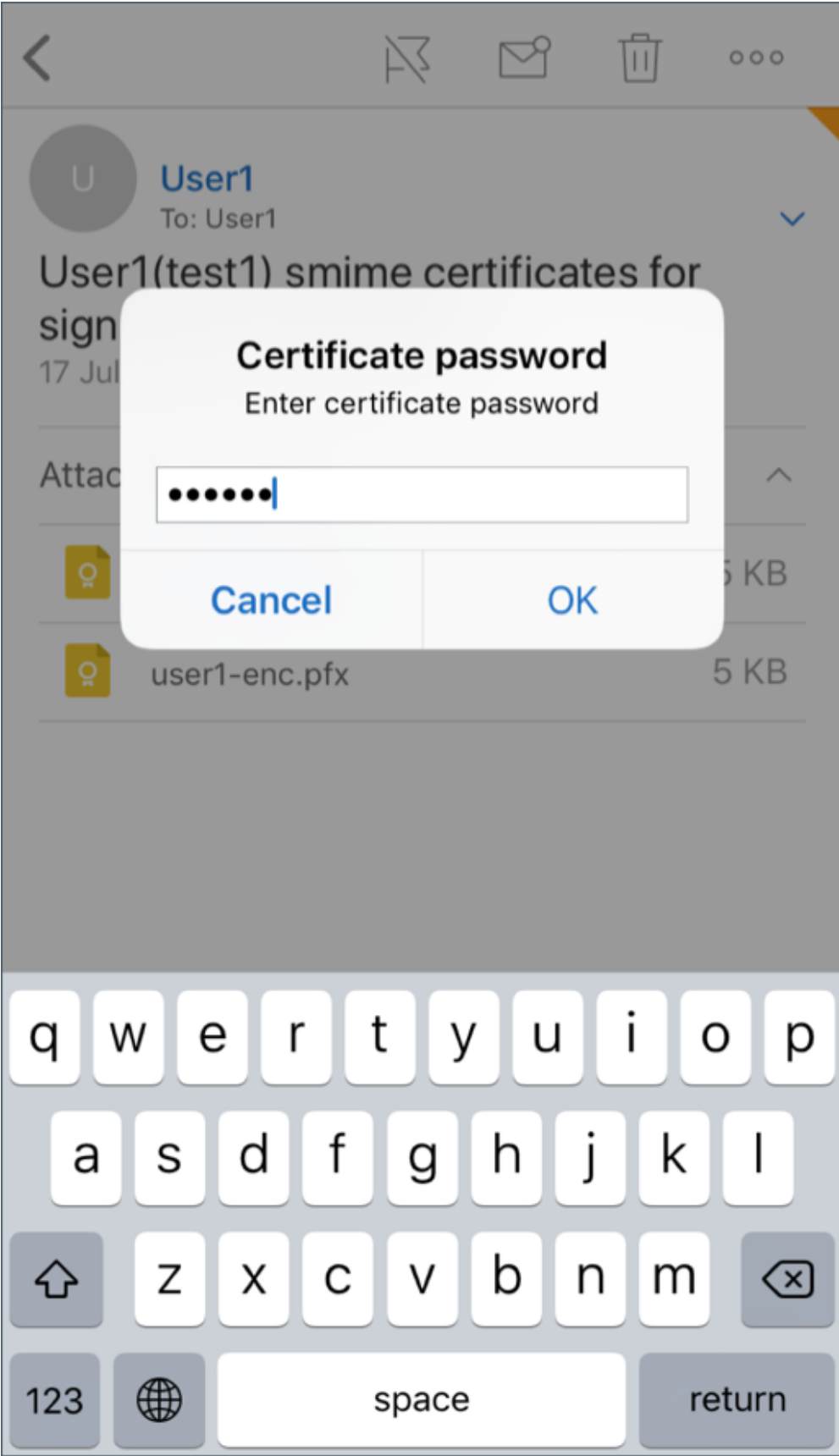
User2 또는 도메인의 다른 사용자에게 대해 동일한 절차를 반복합니다.

iOS 및 Android 용 Secure Mail 에서 S/MIME 이 사용되도록 설정

전자 메일이 전달된 후 다음 단계로 Secure Mail 을 사용하여 메시지를 열고 적절한 서명 및 암호화용 인증서로 S/MIME 이 사용되도록 설정합니다.

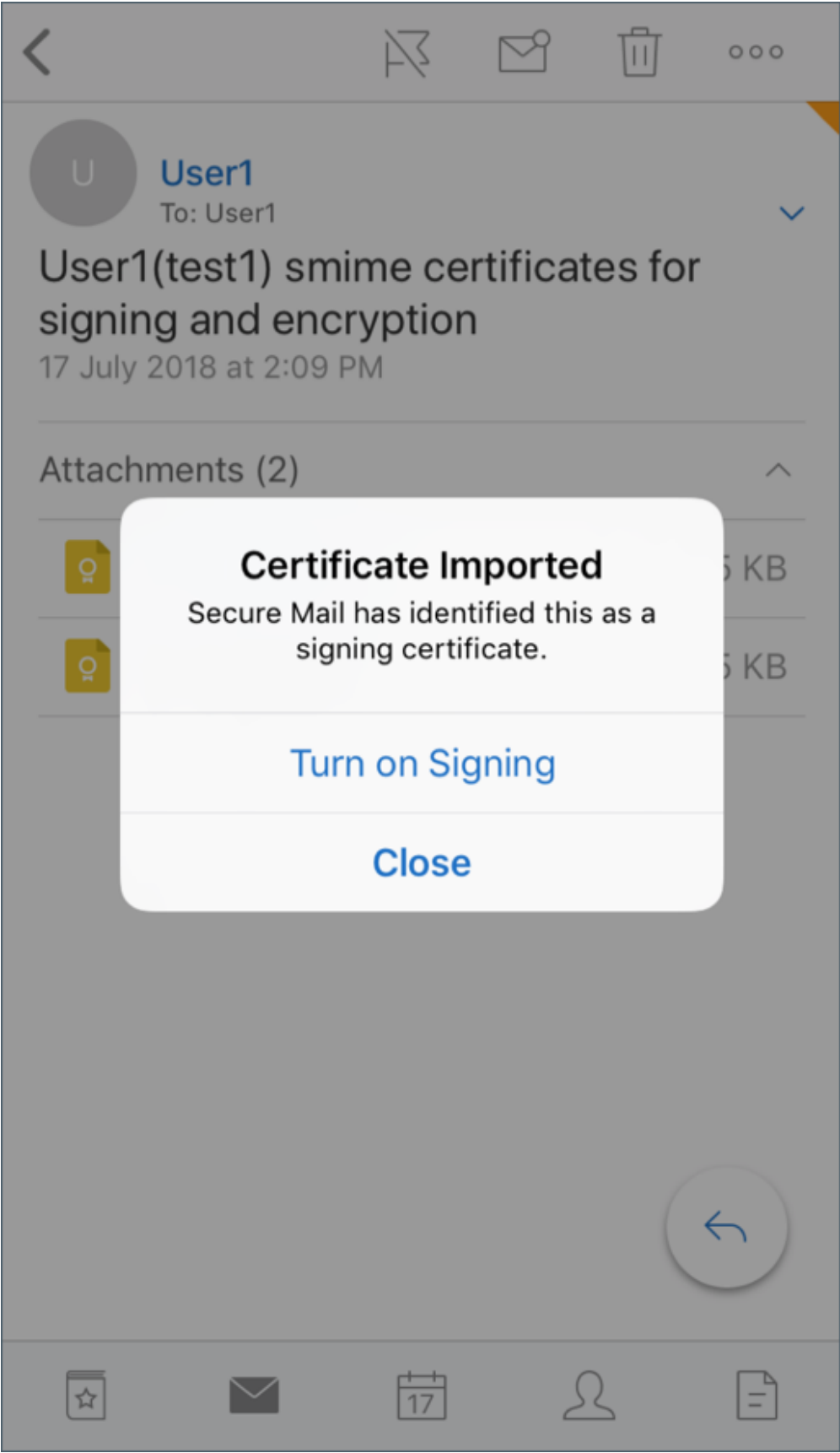
개별 서명 및 암호화 인증서와 함께 **S/MIME** 를 사용하도록 설정하려면

1. Secure Mail 을 열고 S/MIME 인증서가 포함된 전자 메일로 이동합니다.
2. 다운로드하여 가져올 서명 인증서를 누릅니다.
3. 서명 인증서를 서버에서 내보낼 때 개인 키에 할당된 암호를 입력합니다.








이제 인증서를 가져왔습니다.

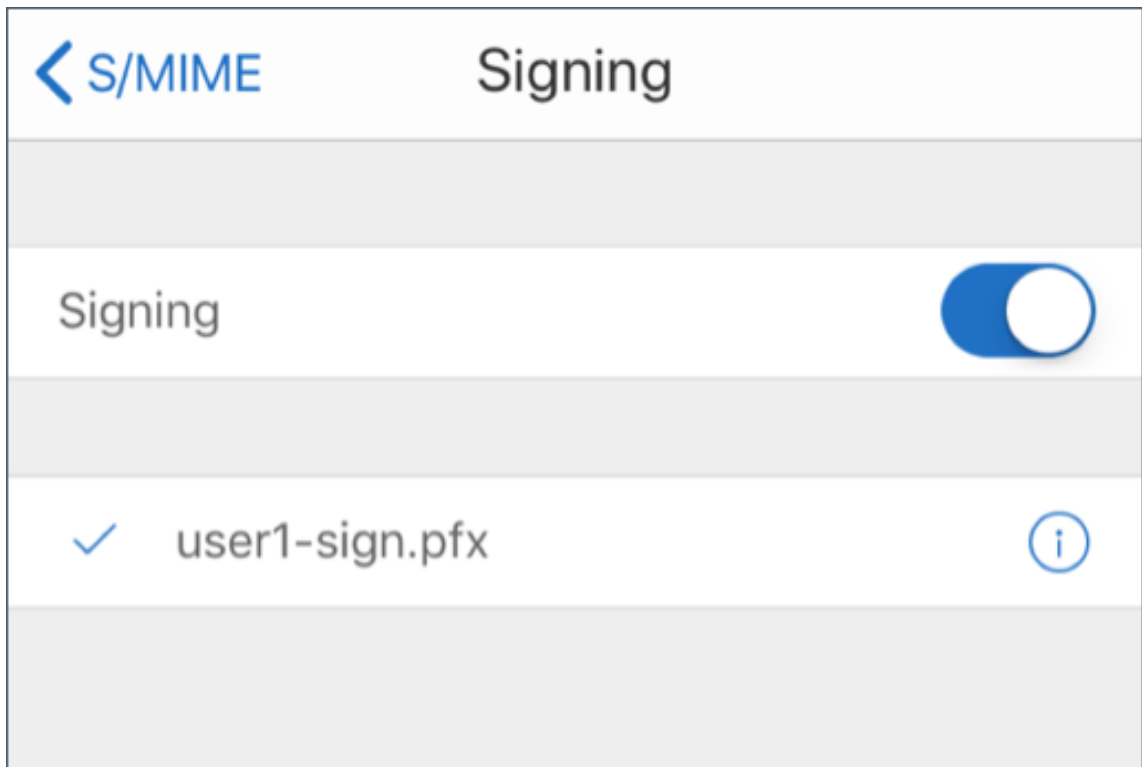
4. 서명 켜기를 누릅니다.



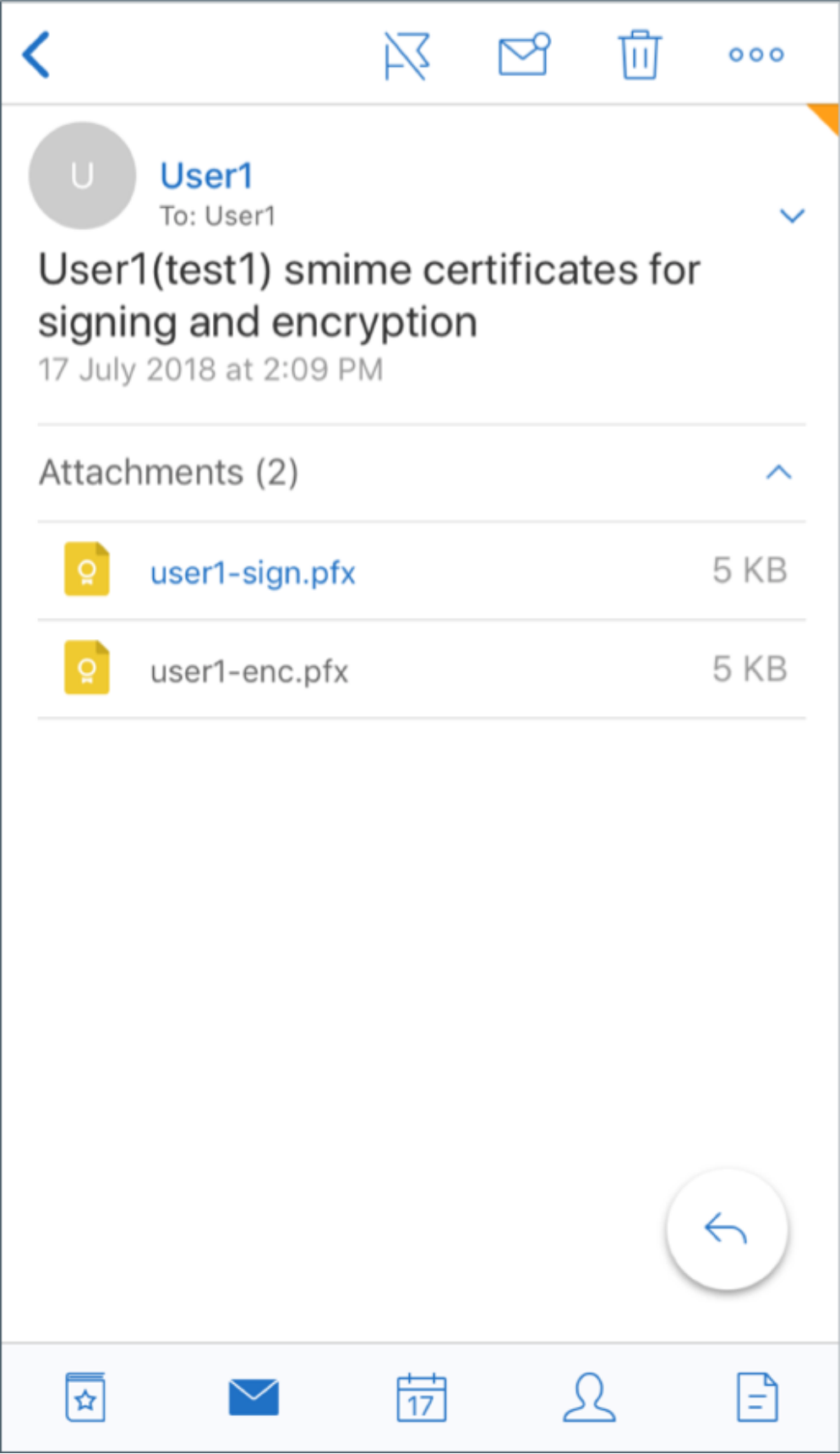
5. 또는 설정 > **S/MIME** 로 이동하여 서명 인증서를 설정할 S/MIME 를 누릅니다.

Settings	Done
Out of Office	Off
MAIL	
Ask Before Deleting	
Organize by Conversation	
Load Attachments on WiFi	
Show Pictures	
Sync Mail Period	3 days
Check Spelling	
S/MIME	>
Offline Files	0 MB
Signature	
Swipe Options	>
Preview Lines	1 Line
CALENDAR	

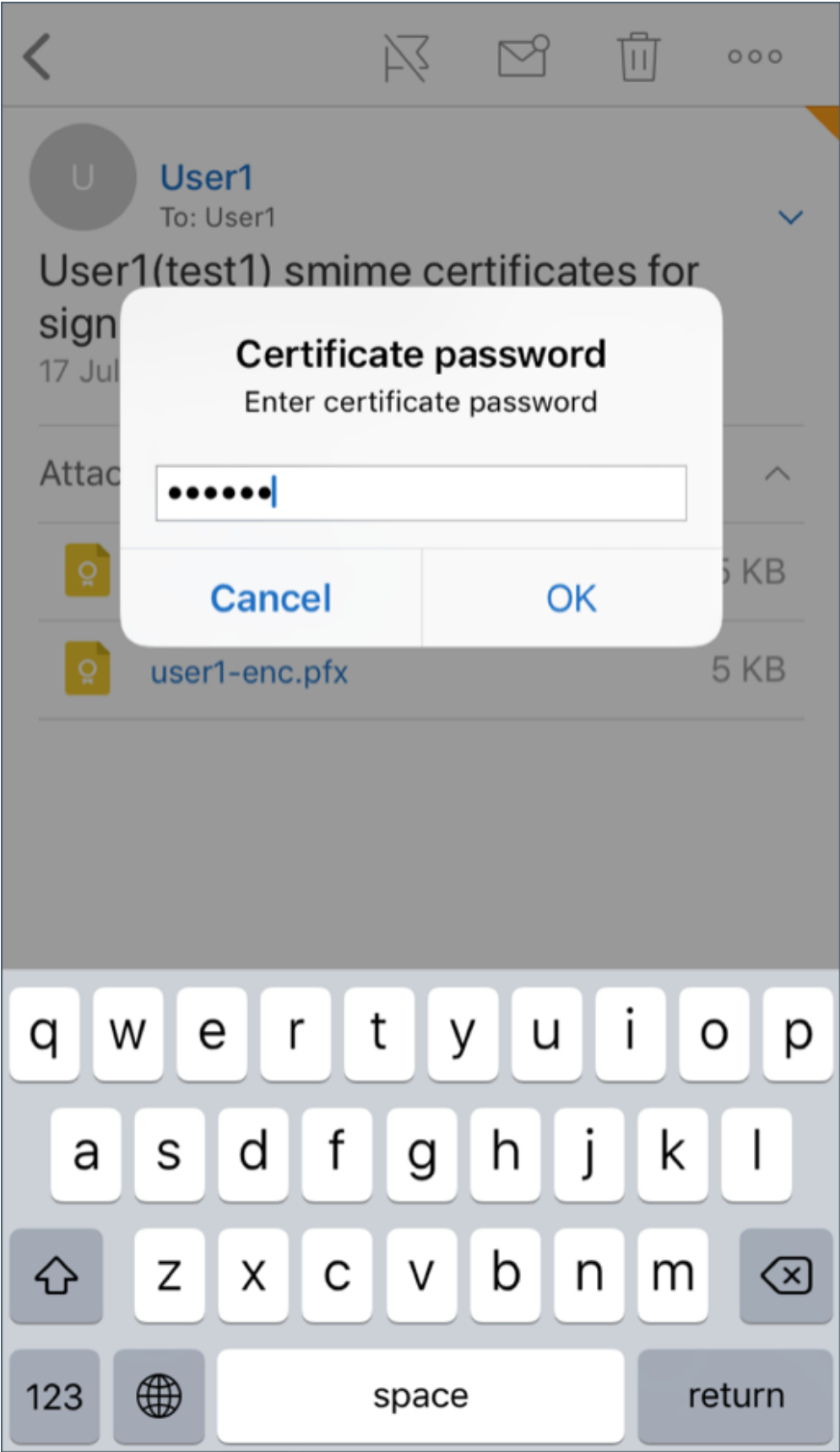
6. 서명 화면에서 올바른 서명 인증서를 가져왔는지 확인합니다.



7. 전자 메일 메시지로 돌아가서 다운로드하고 가져올 암호화 인증서를 누릅니다.

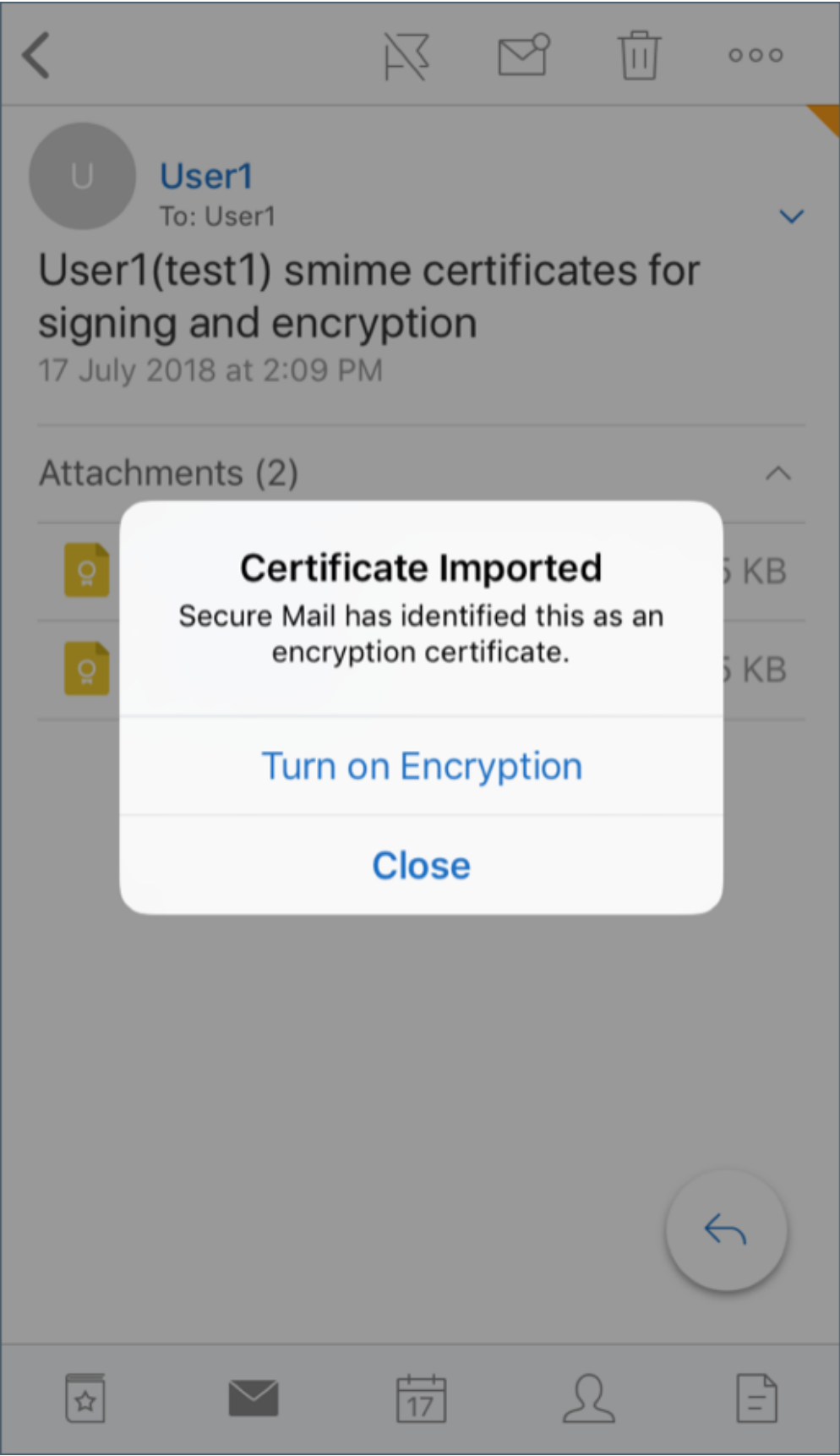


8. 암호화 인증서를 서버에서 내보낼 때 개인 키에 할당된 암호를 입력합니다.

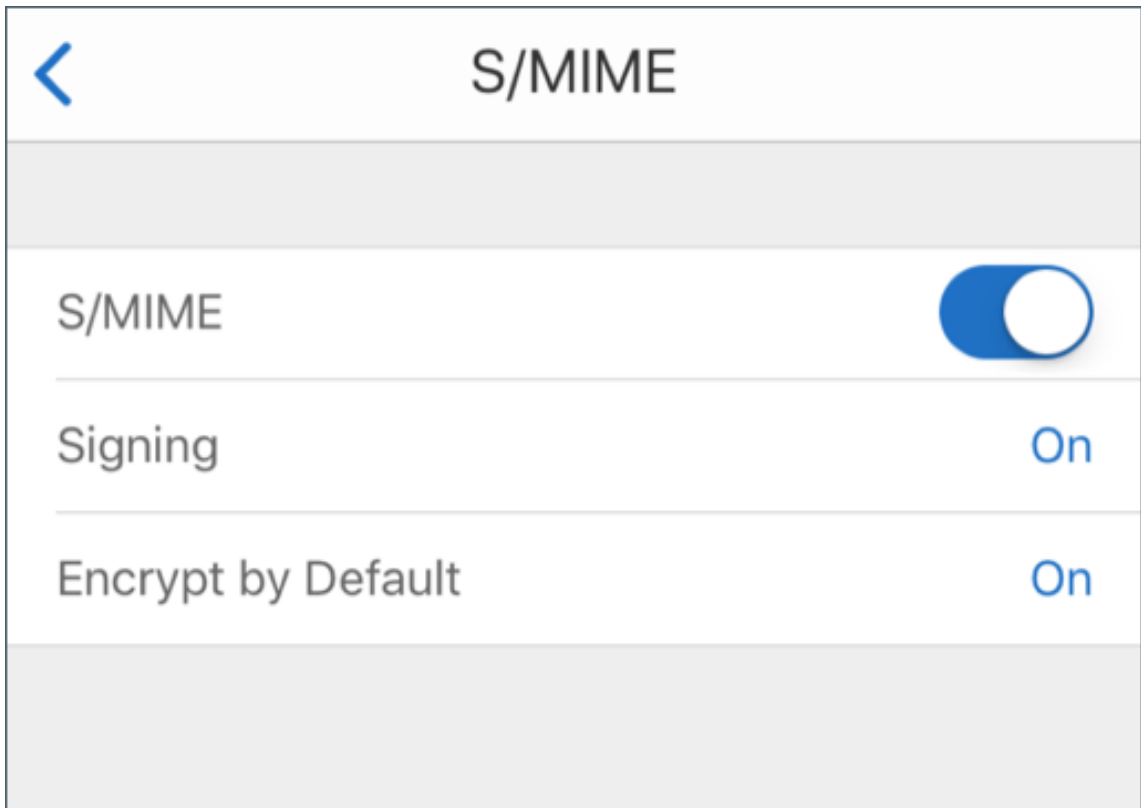


이제 인증서를 가져왔습니다.

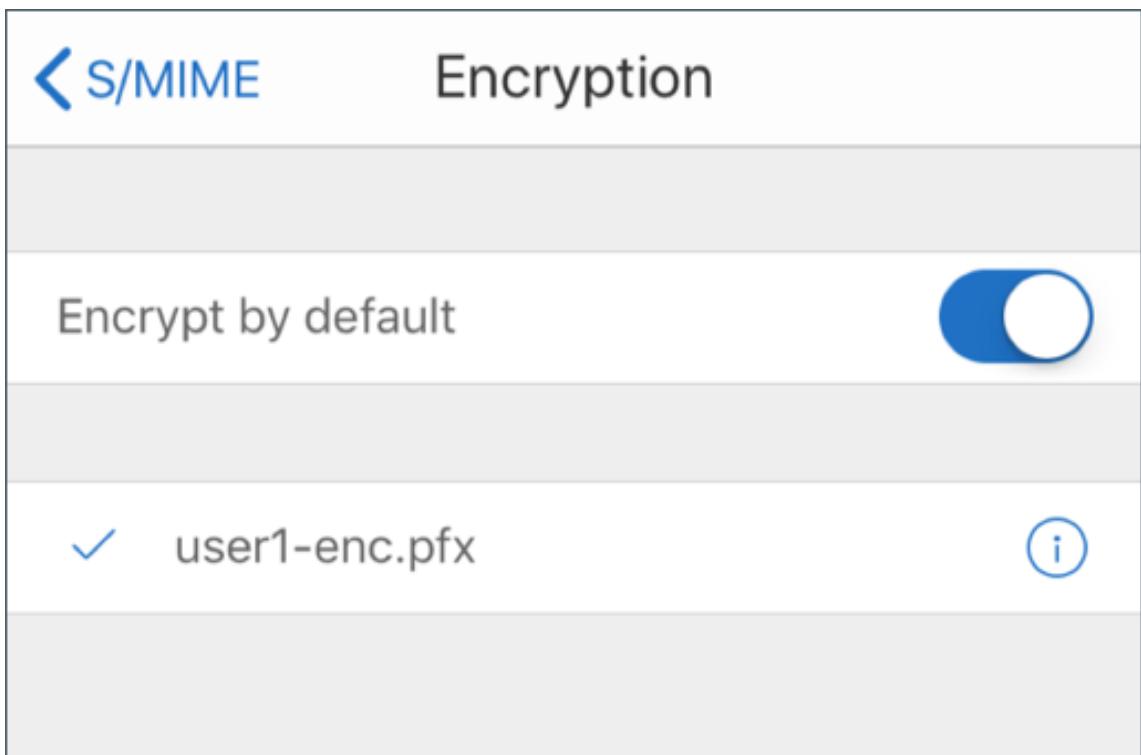
9. 암호화 켜기를 누릅니다.



10. 또는 설정 > **S/MIME** 로 이동하여 기본적으로 암호화를 사용할 S/MIME 를 누릅니다.



11. 암호화 화면에서 올바른 암호화 인증서를 가져왔는지 확인합니다.



참고:


- 1 1. S/MIME으로 디지털 서명된 전자 메일에 첨부 파일이 있고 받는 사람 측에서 S/MIME을 사용하도록 설정하지 않은 경우, 첨부 파일을 받지 못합니다. 이 동작은 Active Sync의 제한 사항입니다. S/MIME 메시지를 효과적으로 받으려면 Secure Mail 설정에서 S/MIME을 활성화합니다.
- 2
- 3 1. ****기본적으로 암호화**** 옵션을 사용하면 전자 메일을 암호화하는 데 필요한 단계를 최소화할 수 있습니다. 이 기능이 켜져 있으면 전자 메일을 작성하는 동안 메일이 암호화 상태에 있게 됩니다. 이 기능이 꺼져 있으면 전자 메일을 작성하는 동안 메일이 암호화되지 않은 상태에 있으므로 암호화하려면 ****잠금**** 아이콘을 눌러야 합니다.


Cancel

Testing smime

Send


To: User1







Cc/Bcc:

Subject: Testing smime






Writing a draft as normal message(without encryption).



q w e r t y u i o p

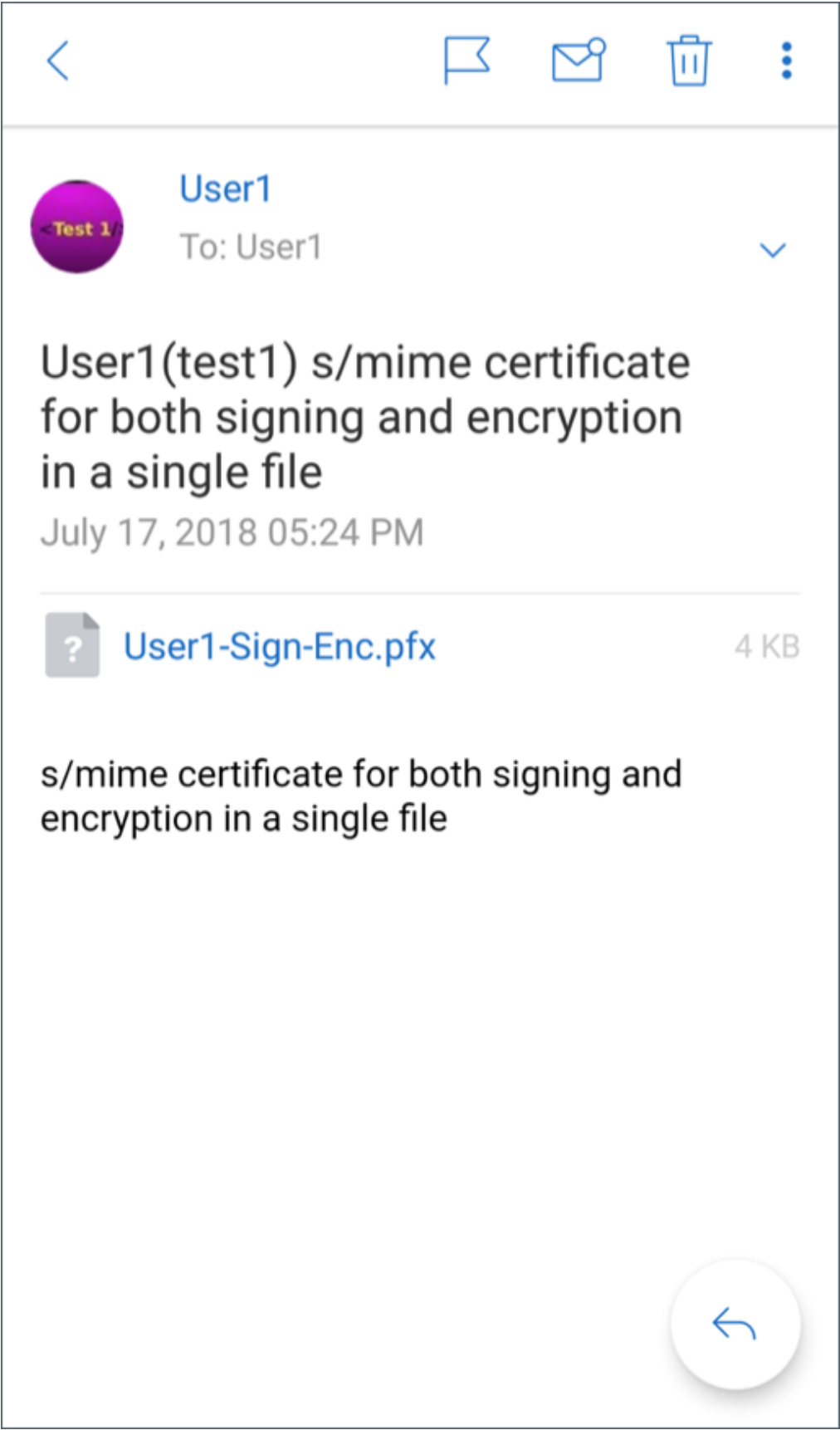
a s d f g h j k l

 z x c v b n m 

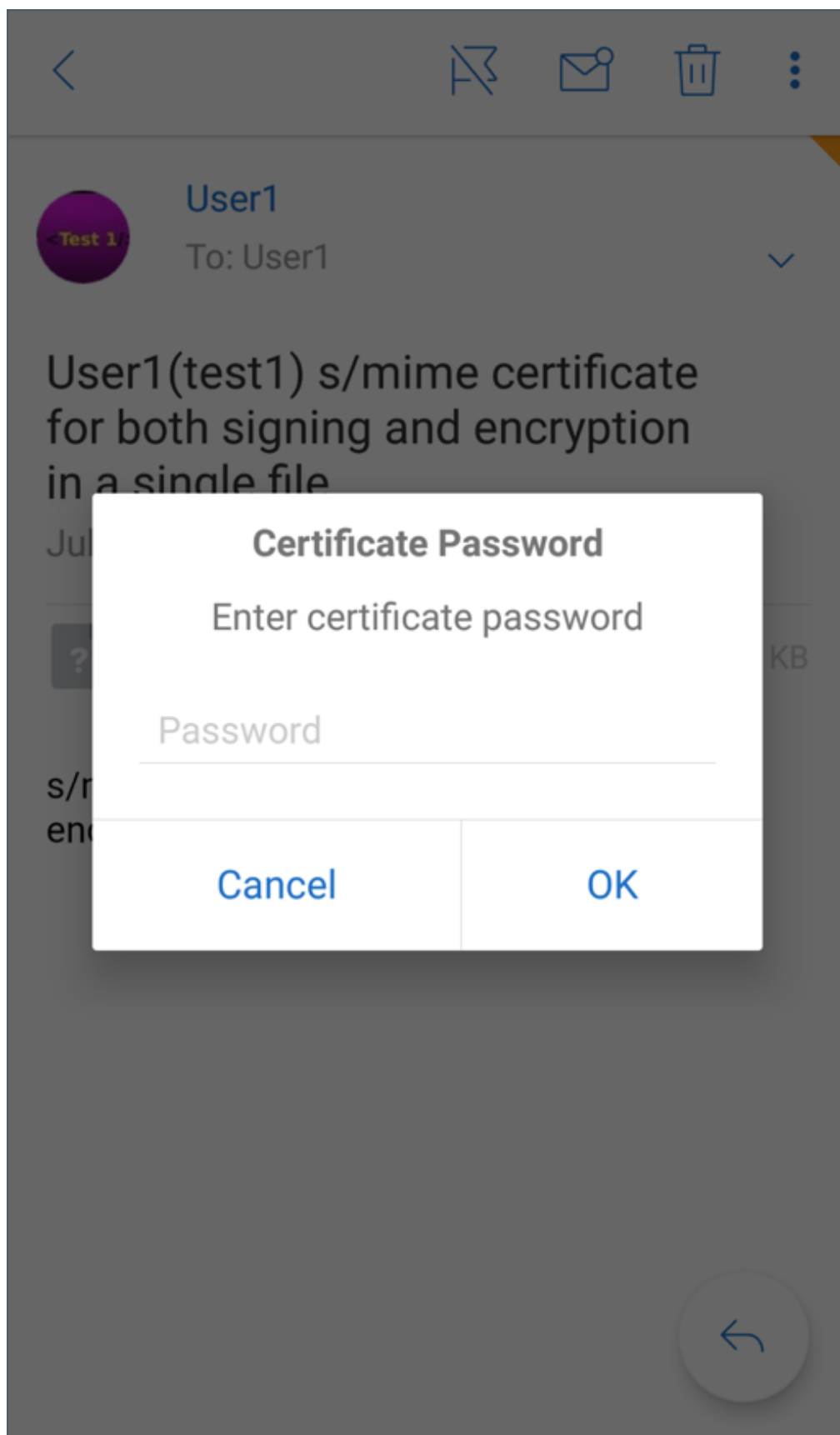
123  space @ . return

단일 서명 및 암호화 인증서와 함께 **S/MIME** 를 사용하도록 설정하려면

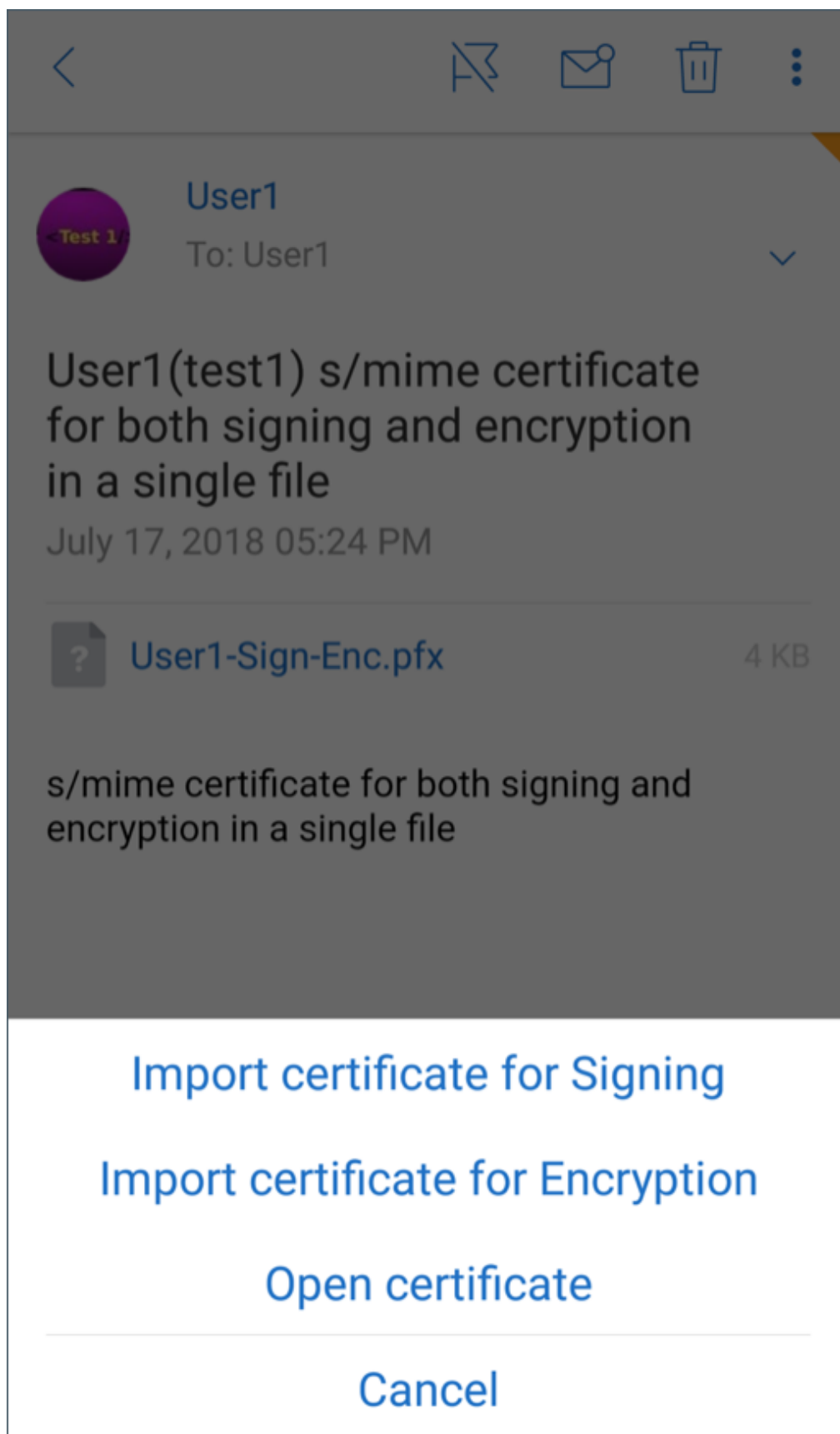
1. Secure Mail 을 열고 S/MIME 인증서가 포함된 전자 메일로 이동합니다.



2. 다운로드하여 가져올 S/SMIME 인증서를 누릅니다.
3. 인증서를 서버에서 내보낼 때 개인 키에 할당된 암호를 입력합니다.



4. 표시되는 인증서 옵션에서 서명 인증서 또는 암호화 인증서를 가져오도록 해당 옵션을 누릅니다.
인증서 열기를 눌러 인증서에 대한 세부 정보를 봅니다.



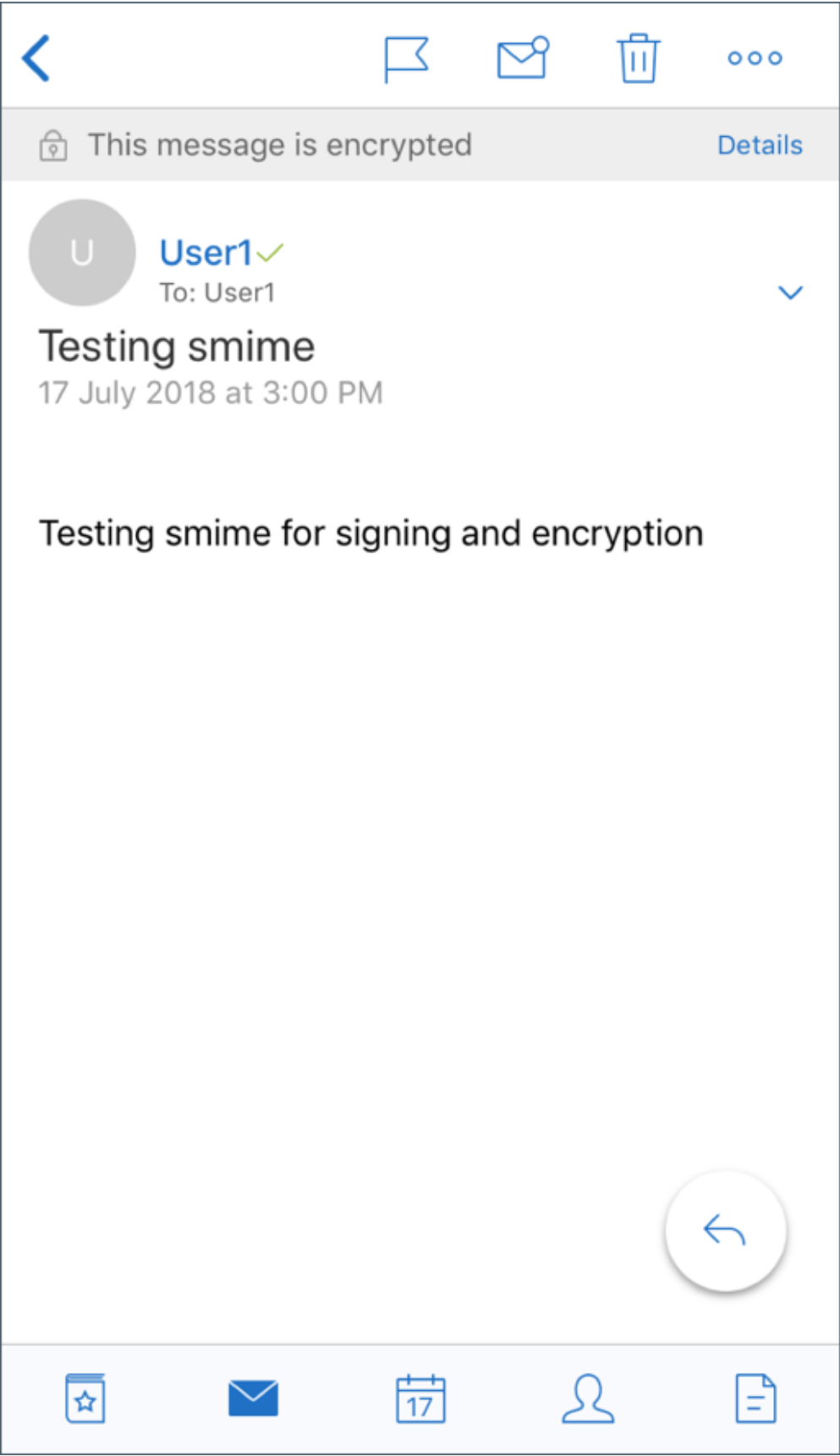
이제 인증서를 가져왔습니다.

설정 > **S/MIME** 로 이동하여 가져온 인증서를 볼 수 있습니다.

iOS 및 **Android** 에서 **S/MIME** 테스트

앞의 섹션에 나열된 단계를 수행한 후에는 받는 사람이 서명 및 암호화된 메일을 읽을 수 있습니다.

다음 이미지는 받는 사람이 읽는 암호화된 메시지의 예를 보여 줍니다.



다음 이미지는 서명된 신뢰할 수 있는 인증서를 확인하는 예를 보여 줍니다.

User1

Save to Contacts

SIGNING

The sender has a trusted certificate

[View Certificate](#)

INTERNET

Work Email

test1@workxen.net

ALIAS

Alias

test1

FACETIME

FaceTime

Secure Mail 은 Active Directory 도메인에서 받는 사람의 공용 암호화 인증서를 검색합니다. 유효한 공개 암호화 키가 없는 받는 사람에게 사용자가 암호화된 메시지를 보내는 경우, 메시지는 암호화되지 않은 상태로 보내집니다. 그룹 메시지의 경우, 단 한 명의 받는 사람이 유효한 키를 갖고 있지 않으면 메시지는 암호화되지 않은 상태로 모든 받는 사람에게 보내집니다.


Cancel


Testing non smime user


Send

Not Encrypted

To: User2










Cc/Bcc:

Subject: Testing non smime user



Hi





q

w

e

r

t

y

u

i

o

p

a

s

d

f


g

h

j

k

l



z

x


c

v


b

n

m



123



space

@

.

return

공용 인증서 출처 구성

S/MIME 공용 인증서를 사용하려면, S/MIME 공용 인증서 원본, LDAP 서버 주소, LDAP 기본 DN 및 익명으로 LDAP 액세스 정책을 구성합니다.

앱 정책과 더불어, 다음을 수행하십시오.

- LDAP 서버가 공용인 경우 트래픽이 LDAP 서버로 직접 이동하는지 확인하십시오. 이렇게 하려면 Secure Mail의 네트워크 정책을 내부 네트워크로 터널링됨으로 구성하고 Citrix ADC에 대해 분할 DNS를 구성해야 합니다.
- LDAP 서버가 내부 네트워크에 있는 경우 다음을 수행하십시오.
 - iOS의 경우 백그라운드 네트워크 서비스 게이트웨이 정책을 구성하지 않았는지 확인하십시오. 이 정책을 구성하는 경우 사용자가 인증 프롬프트가 빈번하게 나타납니다.
 - Android의 경우 백그라운드 네트워크 서비스 게이트웨이 정책의 목록에 **LDAP** 서버 **URL**을 추가했는지 확인하십시오.

Secure Mail에 대한 SSO

December 10, 2021

사용자는 Secure Hub에 등록할 때 Secure Mail에서 사용자가 자동으로 등록되도록 Endpoint Management를 구성할 수 있습니다. 따라서 Secure Mail에서 등록하기 위해 사용자가 더 많은 정보를 입력하거나 더 많은 절차를 거치지 않아도 됩니다. 전자 메일 자격 증명으로 Secure Hub에 등록하는 사용자의 경우, 이 기능을 사용하려면 자동 검색을 사용하도록 설정되어 있어야 합니다. 자동 검색을 사용하도록 설정되어 있지 않으면 다음 등록 방법에 대해 이 기능이 사용되도록 설정할 수 있습니다.

- Endpoint Management 주소가 Secure Hub에서 Secure Mail로 전달됩니다.
- 사용자가 Secure Hub에 등록할 때 Endpoint Management 주소를 입력합니다.

Secure Mail에 자동 등록을 사용하도록 설정하려면

1. Endpoint Management 클라이언트 속성의 설정 페이지에서 다음을 수행합니다.

a. 다음 값을 **true**로 설정합니다.

- ENABLE_PASSCODE_AUTH
- ENABLE_PASSWORD_CACHING
- ENABLE_CREDENTIAL_STORE

b. 다음 구성을 추가합니다.

- 표시 이름: SEND_LDAP_ATTRIBUTES

- 값: `userPrincipalName=${user.userprincipalname},sAMAccountName=${user.samaccountname},displayName=${user.displayName},mail=${user.mail}`
- 설정 페이지에서 서버 속성에 다음 구성을 추가합니다.
MAM_MACRO_SUPPORT 가 **true** 로 설정됨
 - 다음 Secure Mail 속성을 구성합니다.
 - 초기 인증 메커니즘을 사용자 전자 메일 주소로 설정합니다.
 - 초기 인증 자격 증명을 **userPrincipalName** 으로 설정합니다.
 - 사용자의 Exchange Server 사서함에 대한 전자 메일 기반의 자동 검색 서비스를 구성합니다. 지원이 필요한 경우 Microsoft Exchange 관리자에게 문의하십시오. 이 문서에서는 SRV 레코드에 대한 DNS 쿼리를 통해 자동 검색 서비스를 구성하는 것으로 가정합니다.

Secure Mail 앱 정책을 구성하려면

Secure Mail 앱을 Endpoint Management 에 업로드합니다. 올바른 버전의 Secure Mail 앱과 연결된.mdx 파일을 업로드한 후 다음 Secure Mail 앱 설정을 구성합니다.

- 초기 인증 메커니즘에서 사용자 전자 메일 주소를 클릭합니다.
- 초기 인증 자격 증명에서 **userPrincipalName** 또는 **sAMAccountName** 을 클릭합니다. 선택 항목은 사용자의 Exchange Mail Server 에 대해 구성된 인증 유형에 따라 달라집니다.
- Secure Mail Exchange Server 와 Secure Mail 사용자 도메인 필드를 비워 둡니다.
- 필요에 따라 Secure Mail 앱의 다른 정책을 구성하고 필요한 배달 그룹을 할당합니다.

자동 프로비저닝을 통한 완벽한 Secure Mail SSO 사용자 환경 구현

다음 사전 요구 사항을 충족해야 합니다.

- Apple App Store(iOS) 또는 Google Play Store(Android) 에서 Secure Hub 를 설치합니다.
- Secure Hub 를 열고 Endpoint Management 에 등록하는 데 사용할 전자 메일 주소와 암호를 입력합니다.
- Apple App Store(iOS) 또는 Google Play Store(Android) 에서 Secure Mail 을 설치합니다.
- Secure Mail 을 열고 확인을 누릅니다. 이 단계를 통해 Secure Hub 에서 Secure Mail 을 관리할 수 있습니다. Secure Mail 을 열면 Secure Mail 이 자동으로 구성됩니다.

구성한 자동 검색 서비스에서 사용자의 사서함 데이터베이스에 해당하는 Exchange Server 를 가져오게 됩니다. DNS SRV 레코드 쿼리는 Secure Hub 에서 가져온 사용자의 전자 메일 주소를 사용합니다.

전자 메일 주소, userPrincipalName/sAMAccountName, 암호를 비롯하여 계정 구성에 필요한 모든 세부 정보가 Secure Hub 에서 가져와집니다.

계정이 구성되면 **Secure Mail** > 설정 > 계정에서 장치에 대한 세부 정보를 볼 수 있습니다.

문제 해결

SSO 구성에 문제가 발생할 경우 다음 단계를 시도해 볼 수 있습니다.

1. XenMobile Server 버전이 10.5 이상인지 확인합니다.
2. Endpoint Management 에 자동 검색 서비스가 구성되어 있고 전자 메일 주소를 사용하여 사용자 등록이 구성되어 있는지 확인합니다.
3. 자동 검색에 Exchange Server 도메인이 구성되어 있는지 확인합니다. SRV 레코드 쿼리 시 ActiveSync 메일 클라이언트에 대해 필요한 메일 서버 세부 정보가 반환되는지 확인합니다.
4. 이 기능에 문제가 있을 경우 다음 정보를 수집하고 Citrix 기술 지원 팀에 문의합니다.
 - Endpoint Management 진단 로그를 다운로드합니다.
 - 가장 높은 로그 수준으로 Secure Mail 진단 로그를 수집합니다.
 - 자동 검색 서비스를 호스트하는 Exchange Server 의 C:\inetpub\logs\LogFiles\W3SVC1 디렉터리에 서 IIS 로그를 수집합니다. Microsoft 자동 검색 서비스에 대한 자세한 내용은 [Autodiscover service in Exchange Server](#)(Exchange Server 의 자동 검색 서비스)를 참조하십시오.

보안 고려 사항

February 27, 2024

이 문서에서는 Secure Mail 보안 고려 사항과 데이터 보안 개선을 위해 사용할 수 있는 특정 설정에 대해 설명합니다.

Microsoft IRM 및 AIP 전자 메일 권한 보호 지원

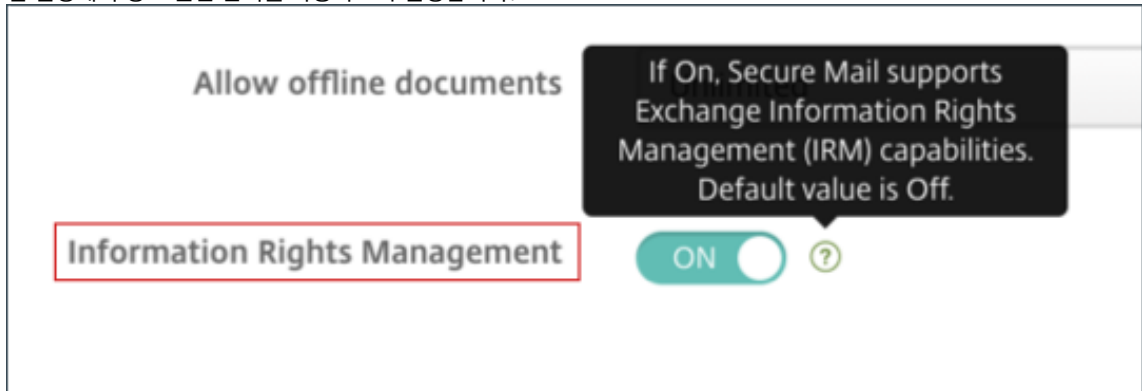
Android 및 iOS 용 Secure Mail 은 Microsoft IRM(정보 권한 관리) 및 AIP(Azure Information Protection) 솔루션으로 보호되는 메시지를 지원합니다. 이 지원은 Citrix Endpoint Management 에 구성된 IRM 정책에 따라 제공됩니다.

IRM 을 사용하는 조직에서는 이 기능을 사용하여 메시징 콘텐츠에 보호를 적용할 수 있습니다. 또한 모바일 장치 사용자는 기능을 사용하여 권한으로 보호되는 콘텐츠를 만들고 사용할 수 있습니다. 기본적으로 IRM 지원은 꺼짐으로 설정되어 있습니다. IRM 지원을 사용하도록 설정하려면 IRM(정보 권한 관리) 정책을 켜짐으로 설정합니다.

Secure Mail 에서 정보 권한 관리를 사용하려면

1. Endpoint Management 에 로그인하고 구성 > 앱으로 이동한 다음 추가를 클릭합니다.
2. 앱 추가 화면에서 **MDX** 를 클릭합니다.
3. 앱 정보 화면에서 앱 세부 정보를 입력하고 다음을 클릭합니다.
4. 장치 OS 에 따라.mdx 파일을 선택하고 업로드합니다.

5. 앱 설정에서 정보 권한 관리를 사용하도록 설정합니다.

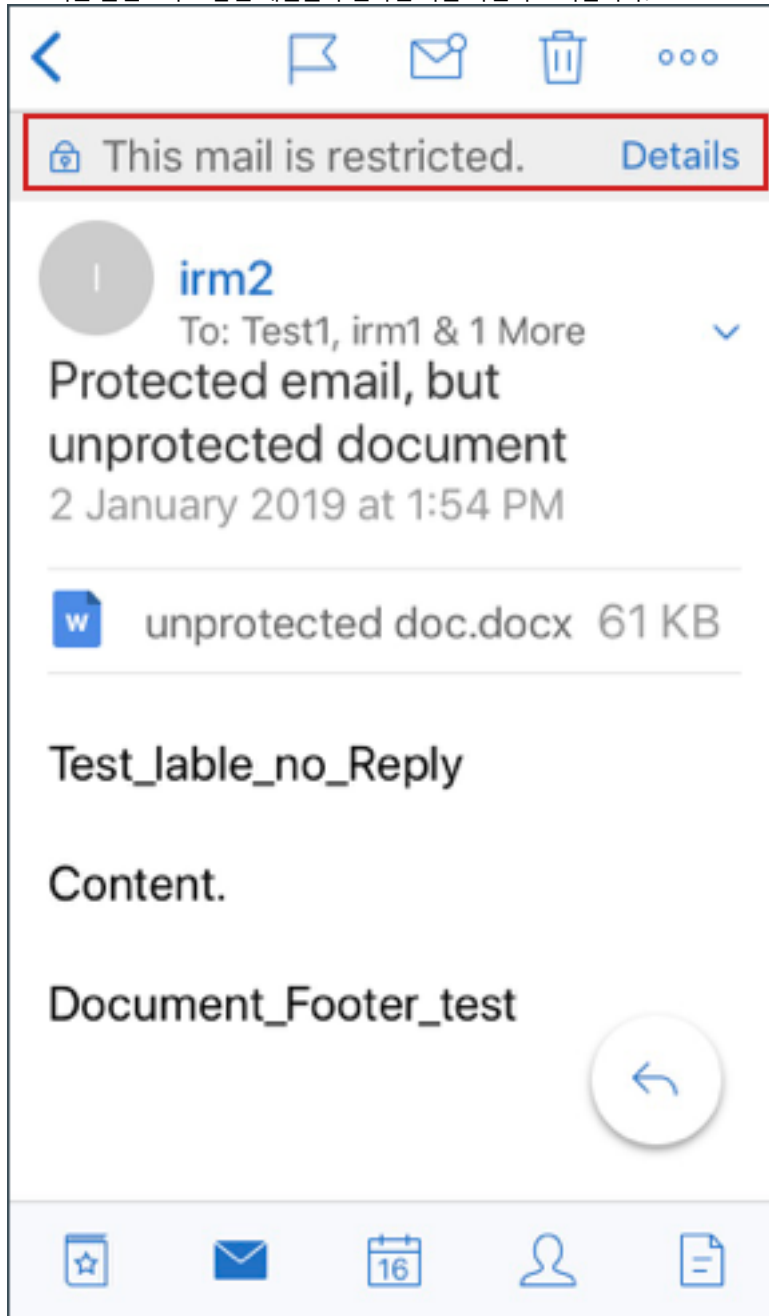


참고:

iOS 와 Android 둘 모두에서 정보 권한 관리를 사용하도록 설정합니다.

권한으로 보호되는 전자 메일을 수신하는 경우

보호되는 콘텐츠가 포함된 메일을 수신하면 다음 화면이 표시됩니다.



사용자에게 부여될 수 있는 권한에 대한 세부 정보를 보려면 세부 정보를 누릅니다.

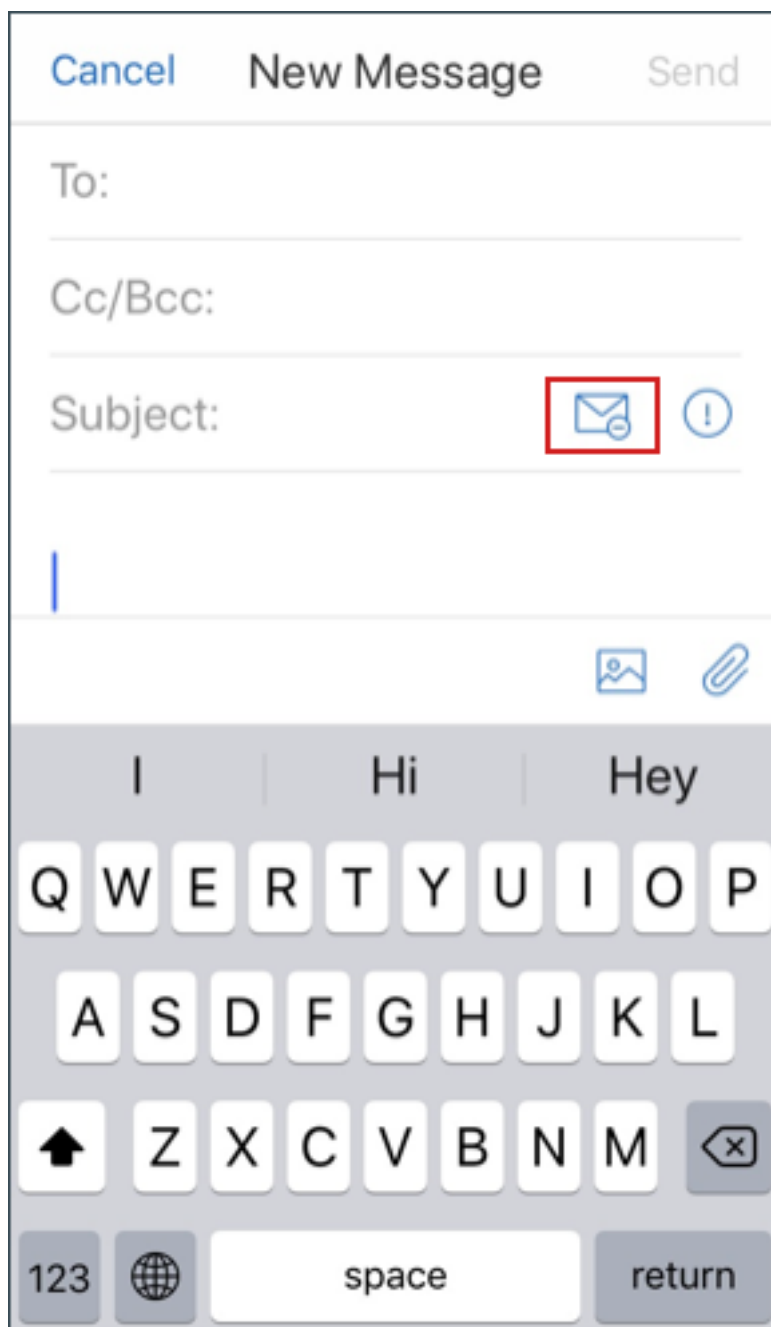
Restrictions	Done
Donot reply, Label to test copy, paste etc..	
OWNER	
irm2@smbler.com	
CONTENT EXPIRATION	
No expiration	
RESTRICTIONS	
✗ Reply	
✗ Reply All	
✓ Forward	
✓ Edit Content	
✓ Modify Recipients	

권한으로 보호된 전자 메일을 작성하는 경우

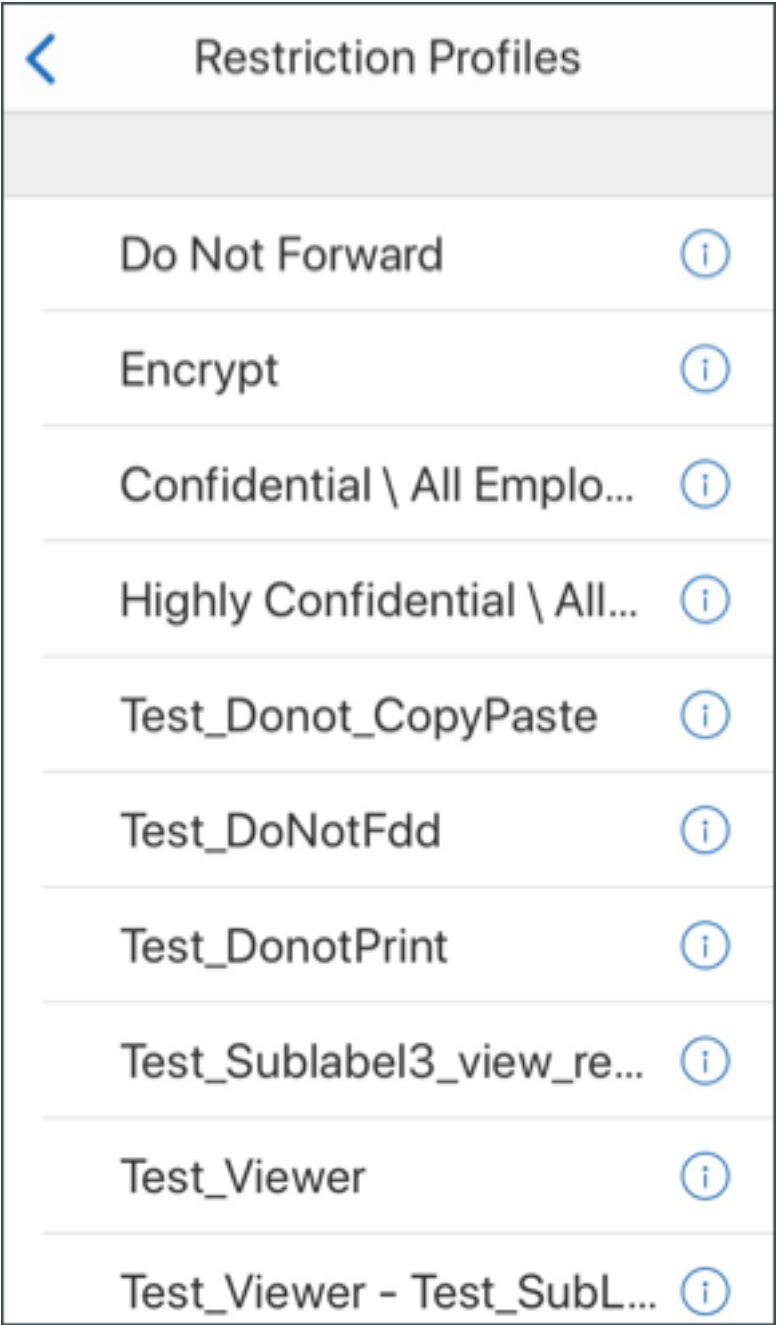
사용자는 메일을 작성할 때 제한 프로필을 설정하여 전자 메일 보호를 사용하도록 설정할 수 있습니다.

전자 메일에 대한 제한을 설정하려면:

1. Secure Mail 에 로그인하고 작성 아이콘을 누릅니다.
2. 작성 화면에서 **Email Restriction**(전자 메일 제한) 아이콘을 누릅니다.

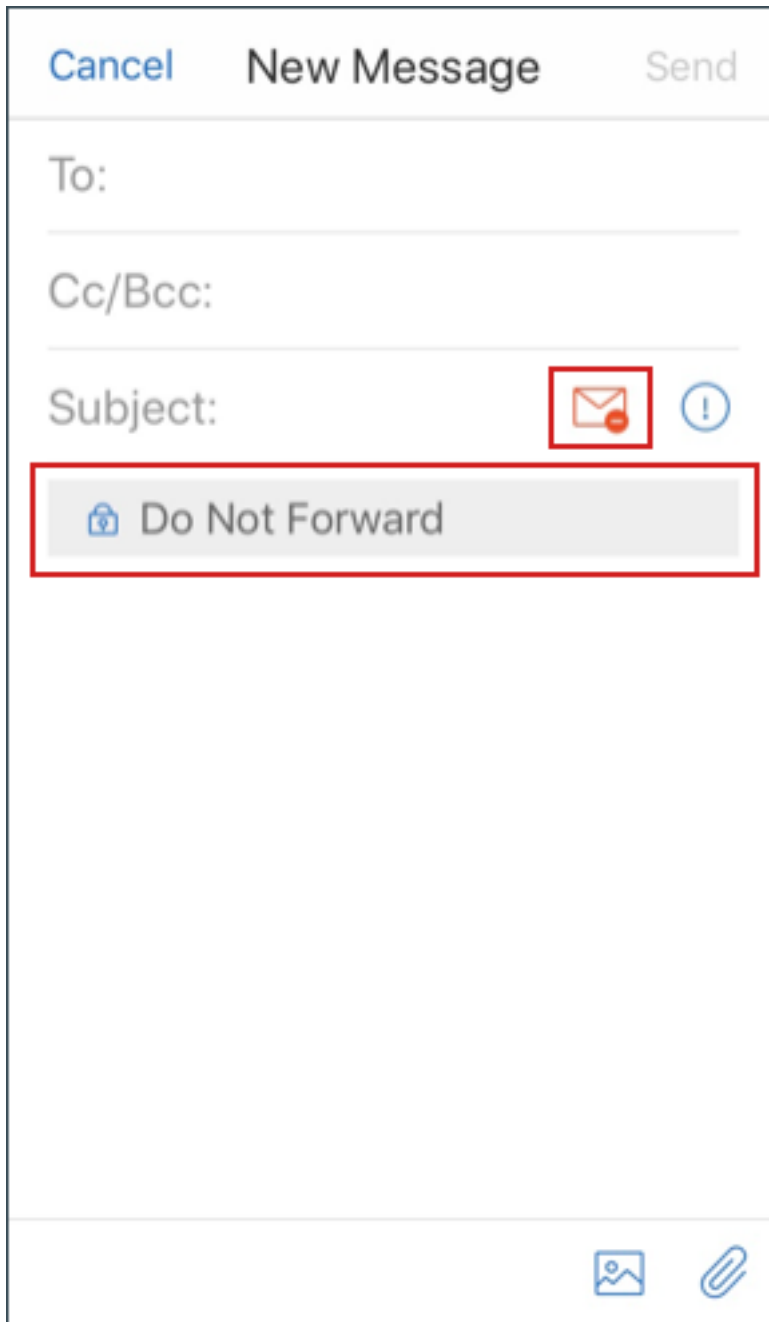


3. 제한 프로필 화면에서 전자 메일에 적용할 제한을 누르고 뒤로를 클릭합니다.



Restriction Profiles	
Do Not Forward	(i)
Encrypt	(i)
Confidential \ All Emplo...	(i)
Highly Confidential \ All...	(i)
Test_Donot_CopyPaste	(i)
Test_DoNotFdd	(i)
Test_DonotPrint	(i)
Test_Sublabel3_view_re...	(i)
Test_Viewer	(i)
Test_Viewer - Test_SubL...	(i)

적용된 제한이 제목 필드 아래에 나타납니다.


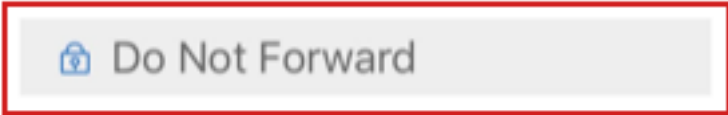



Cancel New Message Send



To:

Cc/Bcc:

Subject:

 Do Not Forward

일부 조직에서는 IRM 정책을 엄격히 준수할 것을 요구할 수 있습니다. Secure Mail 에 액세스하는 사용자가 Secure Mail, 운영 체제 또는 하드웨어 플랫폼을 변조하여 IRM 정책을 우회하려고 시도할 수 있습니다.

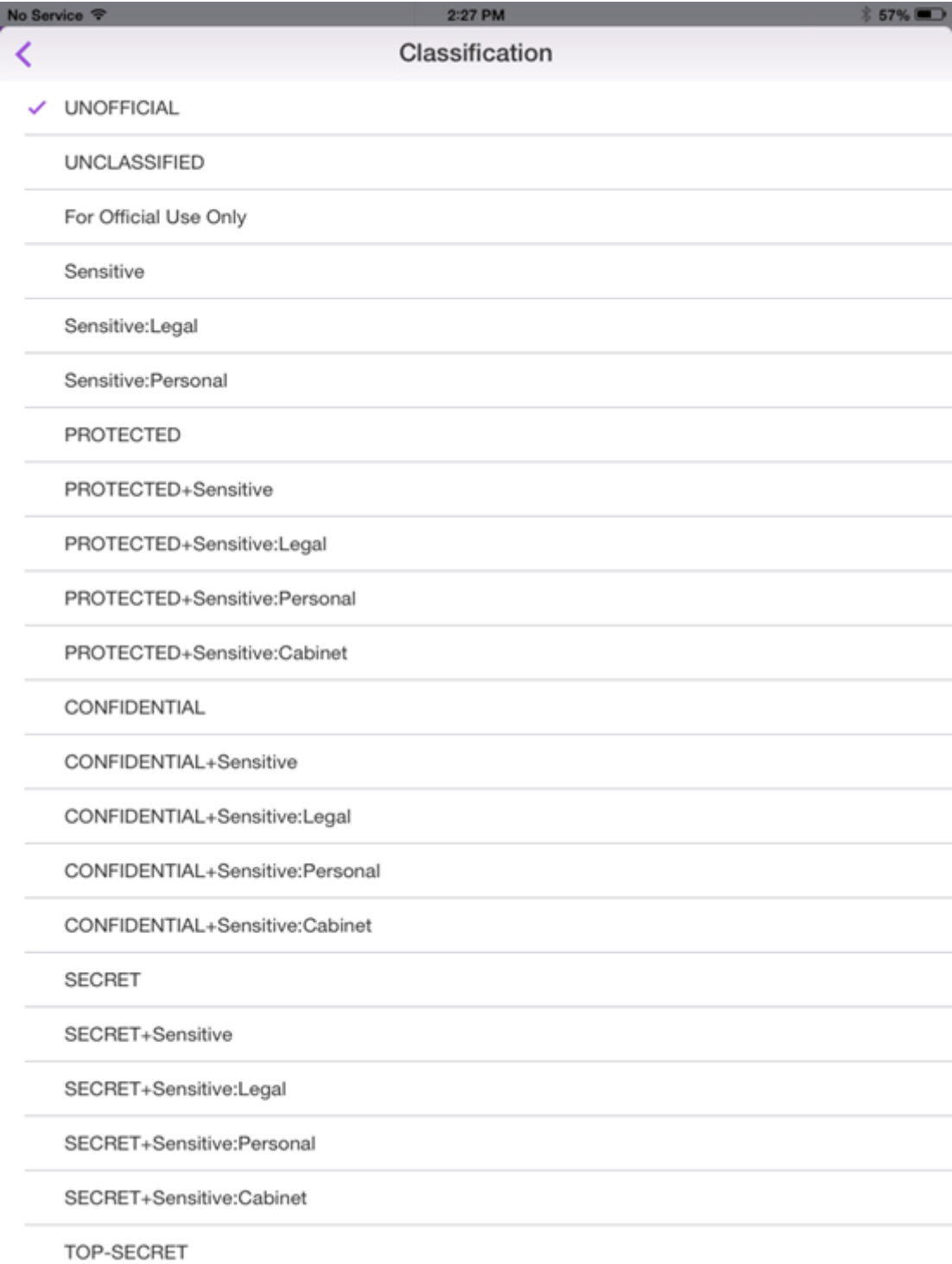
Endpoint Management 가 특정 공격을 탐지할 수는 있지만, 보안 향상을 위해 다음과 같은 예방 조치를 고려하십시오.

- 장치 공급업체가 제공하는 보안 지침을 검토합니다.
- Endpoint Management 기능 또는 다른 기능을 사용하여 지침에 따라 장치를 구성합니다.
- Secure Mail 등에 대해 IRM 기능을 적절히 사용할 수 있도록 사용자에게 지침을 제공합니다.
- 이러한 유형의 공격에 대항하기 위해 추가적인 타사 보안 소프트웨어를 배포합니다.

전자 메일 보안 분류

iOS 및 Android 용 Secure Mail 은 전자 메일 분류 표시를 지원하여 사용자가 전자 메일을 보낼 때 SEC(보안) 및 DLM(Dissemination Limiting Marker) 을 지정할 수 있게 합니다. SEC 표시에는 Protected, Confidential 및 Secret 이 포함됩니다. DLM 에는 Sensitive, Legal 또는 Personal 이 포함됩니다. 전자 메일을 작성할 때 Secure Mail 사용자는 다음 이미지와 같이 표시를 선택하여 전자 메일의 분류 수준을 나타낼 수 있습니다.





받는 사람은 전자 메일 제목에서 분류 표시를 볼 수 있습니다. 예:

- 제목: Planning [SEC = PROTECTED, DLM = Sensitive]
- 제목: Planning [DLM = Sensitive]
- 제목: Planning [SEC = UNCLASSIFIED]

전자 메일 헤더에는 Internet Message Header Extension 으로서 분류 표시가 포함되며, 이 예에서는 분류 표시가 굵은 텍스트 표시되어 있습니다.

Date: Fri, 01 May 2015 12:34:50 +530

제목: Planning [SEC = PROTECTED, DLM = Sensitive]

Priority: normal

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

From: **operations@example.com**

받는 사람: 팀 <mylist@example.com>

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

Secure Mail 은 분류 표시를 표시하기만 합니다. 이 앱은 이러한 표시에 기반하여 조치를 취하지는 않습니다.

분류 표시가 있는 전자 메일에 대해 사용자가 회신하거나 해당 전자 메일을 사용자가 전달하는 경우, SEC 및 DLM 값은 원본 전자 메일의 표시로 기본 설정됩니다. 사용자는 다른 표시를 선택할 수 있습니다. Secure Mail 은 이러한 변경 사항이 원본 전자 메일과 비교하여 유효한지 여부를 검사하지 않습니다.

전자 메일 분류 표시는 다음 MDX 정책을 통해 구성합니다.

- 전자 메일 분류: 커짐인 경우, Secure Mail 은 SEC 및 DLM 을 사용할 수 있도록 전자 메일 분류 표시를 지원합니다. 분류 표시는 전자 메일 헤더에서 “X-Protective-Marking” 값으로 나타납니다. 관련 전자 메일 분류 정책을 구성해야 합니다. 기본값은 꺼짐입니다.
- 전자 메일 분류 네임스페이스: 사용되는 분류 표준에 따라 전자 메일 헤더에 필요한 분류 네임스페이스를 지정합니다. 예를 들어 네임스페이스 “gov.au” 는 헤더에서 “NS=gov.au” 로 표시됩니다. 기본값은 비어 있습니다.
- 전자 메일 분류 버전: 사용되는 분류 표준에 따라 전자 메일 헤더에 필요한 분류 버전을 지정합니다. 예를 들어 버전 “2012.3” 은 헤더에서 “VER=2012.3” 으로 나타납니다. 기본값은 비어 있습니다.
- 기본 전자 메일 분류: 사용자가 표시를 선택하지 않을 경우 Secure Mail 이 전자 메일에 적용할 보호 표시를 지정합니다. 전자 메일 분류 표시 정책 목록에 이 값이 있어야 합니다. 기본값은 **UNOFFICIAL** 입니다.
- 전자 메일 분류 표시: 사용자에게 제공할 분류 표시를 지정합니다. 이 목록이 비어 있으면 Secure Mail 이 보호 표시 목록을 포함하지 않습니다. 표시 목록에는 세미콜론으로 구분된 값 쌍이 들어 있습니다. 각 쌍에는 Secure Mail 에 나타나는 목록 값과 Secure Mail 의 전자 메일 제목 및 헤더에 추가되는 텍스트인 표시 값이 포함되어 있습니다. 예를 들어, 표시 쌍이 “UNOFFICIAL,SEC=UNOFFICIAL;” 인 경우 목록 값은 “UNOFFICIAL” 이고 표시 값은 “SEC=UNOFFICIAL” 입니다.

기본값은 분류 표시 목록이며 수정할 수 있습니다. 다음 표시가 Secure Mail 과 함께 제공됩니다.

- 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

ios 데이터 보호

ASD(Australian Signals Directorate) 데이터 보호 요구 사항을 충족해야 하는 기업은 Secure Mail 및 Secure Web 에 **ios** 데이터 보호 사용 정책을 사용할 수 있습니다. 기본적으로 이 정책은 꺼짐으로 설정되어 있습니다.

Secure Web 에서 **ios** 데이터 보호 사용이 꺼짐으로 설정되어 있으면 Secure Web 은 샌드박스의 모든 파일에 대해 클래스 A 보호 수준을 사용하게 됩니다. Secure Mail 데이터 보호에 대한 자세한 내용은 [Australian Signals Directorate 데이터 보호](#)를 참조하십시오. 이 정책이 사용되도록 설정한 경우 최고 수준의 데이터 보호 클래스가 사용되므로 최소 데이터 보호 클래스 정책을 함께 지정할 필요는 없습니다.

ios 데이터 보호 사용 정책을 변경하려면

1. Endpoint Management 콘솔을 사용하여 Secure Web 및 Secure Mail MDX 파일을 Endpoint Management 로 로드합니다. 새 앱의 경우 구성 > 앱 > 추가로 이동한 후 **MDX** 를 클릭합니다. 업그레이드는 [MDX 또는 엔터프라이즈 앱 업그레이드](#)를 참조하십시오.

2. Secure Mail 의 경우, 앱 설정으로 이동하고 **iOS** 데이터 보호 사용 정책을 찾은 후 켜짐으로 설정합니다. 이전 운영 체제 버전을 실행하는 장치는 이 정책을 사용하도록 설정하여도 영향을 받지 않습니다.
3. Secure Web 의 경우, 앱 설정으로 이동하고 **iOS** 데이터 보호 사용 정책을 찾은 후 켜짐으로 설정합니다. 이전 운영 체제 버전을 실행하는 장치는 이 정책을 사용하도록 설정하여도 영향을 받지 않습니다.
4. 앱 정책을 평소대로 구성하고 설정을 저장하여 앱을 Endpoint Management 앱 스토어에 배포합니다.

Australian Signals Directorate 데이터 보호

Secure Mail 은 ASD 컴퓨터 보안 요구 사항을 충족해야 하는 기업을 위해 Australian Signals Directorate 데이터 보호를 지원합니다. 기본적으로 iOS 데이터 보호 사용 정책은 꺼짐으로 설정되고 Secure Mail 은 Class C 데이터 보호를 제공하거나 프로비전 프로필에 설정된 데이터 보호를 사용합니다.

이 정책이 켜짐인 경우, Secure Mail 은 앱 샌드박스에서 파일을 생성하거나 열 때 보호 수준을 지정합니다. Secure Mail 은 다음에 대해 Class A 데이터 보호를 설정합니다.

- 보낼 편지함 항목
- 카메라 또는 카메라 롤의 사진
- 다른 앱에서 붙여 넣은 이미지
- 다운로드한 첨부 파일

Secure Mail 은 다음에 대해 Class B 데이터 보호를 설정합니다.

- 저장된 메일
- 일정 항목
- 연락처
- ActiveSync 정책 파일

Class B 보호는 잠긴 장치가 동기화될 수 있게 하고 다운로드 시작 후에 장치가 잠긴 경우에도 다운로드가 완료될 수 있게 합니다.

데이터 보호를 사용하도록 설정된 상태에서는 파일을 열 수 없으므로 장치가 잠겨 있으면 대기열에 있는 보낼 편지함 항목이 보내지지 않습니다. 또한 장치가 잠겨 있을 때 장치에서 Secure Mail 을 종료했다가 재시작하면 장치가 잠금 해제되고 Secure Mail 이 시작될 때까지는 Secure Mail 이 동기화될 수 없습니다.

이 정책을 사용 설정하는 경우, Citrix 에서는 Class C 데이터 보호가 적용되는 로그 파일이 생성되지 않아야 할 때에만 Secure Mail 을 사용하도록 설정하기를 권장합니다.

화면 콘텐츠 가리기

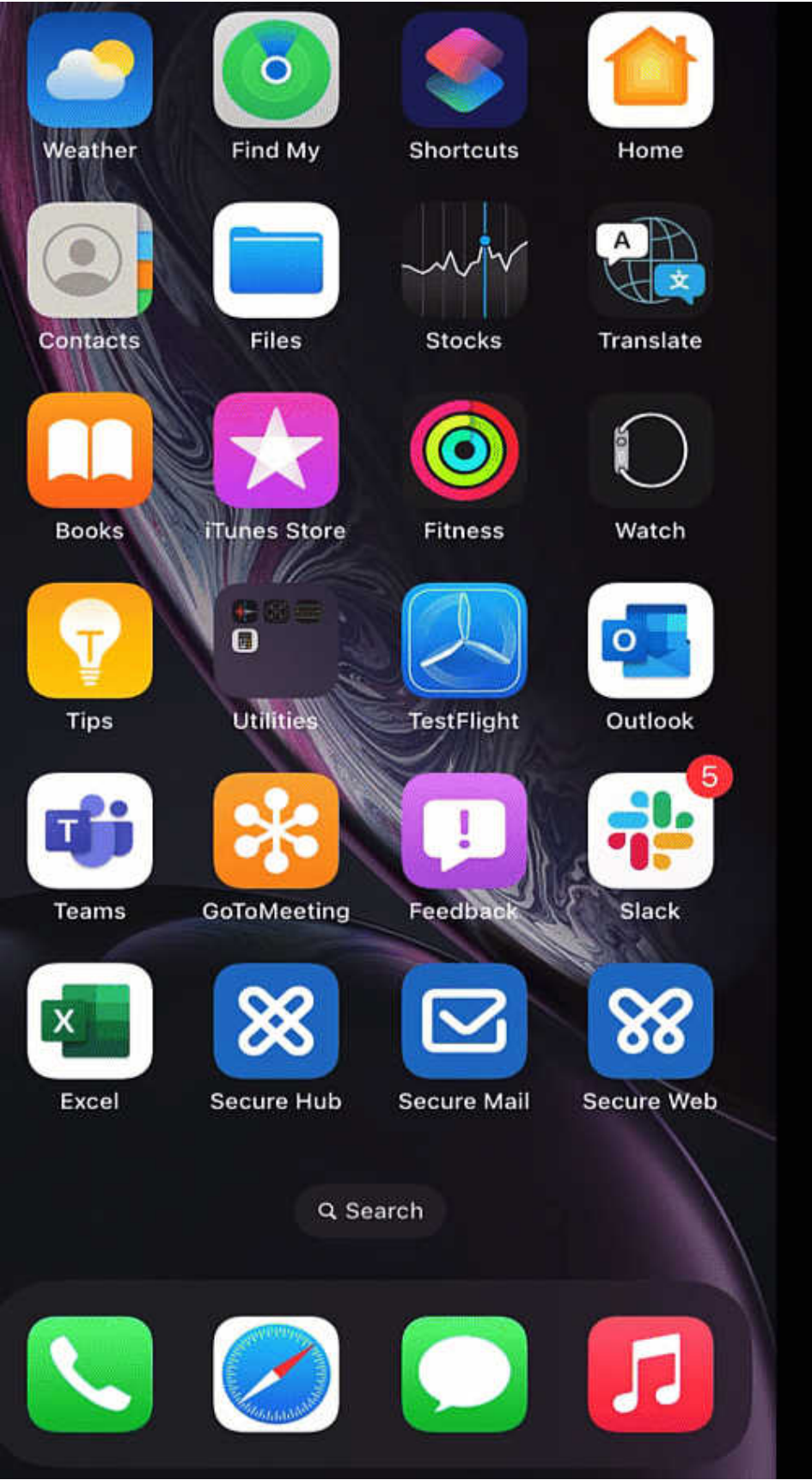
Android 및 iOS 용 Secure Mail 은 앱이 백그라운드로 전환될 때 화면을 가리는 기능을 지원합니다. 이 기능은 사용자 개인 정보를 강화하고 민감한 데이터를 보호하며 권한 없는 액세스를 방지합니다. iOS 또는 Android 장치에서 Secure Mail 에서 이 기능을 사용하도록 설정하려면 다음 섹션을 참조하십시오.

iOS 장치의 경우:

1. 관리자 자격 증명을 사용하여 Citrix Endpoint Management 콘솔에 로그인합니다.
2. 구성 > 앱 > **MDX** 로 이동합니다.
3. 플랫폼 섹션에서 **iOS** 옵션을 선택합니다.
4. 앱 제한 섹션에서 화면 콘텐츠 가리기 옵션을 활성화합니다.

The screenshot shows the Citrix Endpoint Management console interface. The top navigation bar includes 'Endpoint Management', 'Analyze', 'Manage', and 'Configure'. Below this, a sub-navigation bar lists 'Device Policies', 'Apps', 'Media', 'Actions', 'Content Collaboration', 'Enrollment Profiles', and 'Delivery Groups'. The 'Apps' section is active, showing 'MDX' with a list of platform options: '1 App Information', '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. Under '2 Platform', 'iOS' is selected with a checkmark. To the right, the 'App Restrictions' section lists various settings with toggle switches. The 'Obscure screen contents' toggle is turned on (blue) and is highlighted with a red rectangular box. Other toggles include 'Block camera', 'Block Photo Library', 'Block mic record', 'Block dictation', 'Block location services', 'Block SMS compose', 'Block iCloud', 'Block look up', 'Block file backup', 'Block AirPrint', 'Block AirDrop', 'Block file attachments', 'Block Facebook and Twitter APIs', and 'Block third-party keyboards (iOS 11+ only)'. Each toggle has a help icon (question mark) next to it.

화면 콘텐츠 가리기 옵션을 활성화하면 앱이 백그라운드로 전환될 때 Secure Mail 에 회색 화면이 표시됩니다.



Android 장치의 경우:

Secure Mail 앱 콘텐츠를 가리려면 화면 캡처를 제한하는 데 사용하는 정책 (화면 캡처 허용 정책이라고 함) 을 사용할 수 있습니다. 또한 이 정책을 사용하지 않도록 설정하면 앱이 백그라운드로 전환될 때 앱 콘텐츠가 가려집니다. 화면 캡처 허용 정책을 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 Citrix Endpoint Management 설명서의 [Android 설정](#)을 참조하십시오.

iOS 기능

November 19, 2021

이 문서에서는 Secure Mail 에서 지원되는 iOS 기능에 대해 설명합니다.

Secure Mail 일정 이벤트에서 Microsoft Teams 회의 만들기

iOS 용 Secure Mail 에서 일정 이벤트를 만드는 중에 Microsoft Teams 회의 초대를 만들 수 있습니다. Microsoft Teams 회의를 만들려면 **Microsoft Teams** 회의를 전환합니다. 이벤트 세부 정보가 포함된 회의 초대 링크와 세부 정보가 자동으로 전송됩니다. 자세한 내용은 [Secure Mail 일정 이벤트에서 Microsoft Teams 회의 만들기](#)를 참조하십시오.

사전 요구 사항:

Azure Active Directory 의 전역 관리자가 다음을 수행하는지 확인합니다.

- 최신 인증 (OAuth) 을 사용하도록 설정하고 유효한 Microsoft Teams 라이선스가 있는 Exchange Online 사서함 사용자인지 확인합니다.
- Secure Mail 앱에 대한 테넌트 전체의 관리자 동의를 제공합니다.
- Secure Mail 앱에서 Exchange 계정을 구성하고 모든 사용자가 로그인할 수 있도록 앱 권한을 허용합니다. 다음 화면을 참조하십시오.

Dashboard > Enterprise applications > Secure Mail

Secure Mail | Permissions

Enterprise Application

« Refresh Review permissions Got feedback?

Overview
Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups
- Single sign-on
- Provisioning

Security

- Permissions
- Token encryption

Permissions

Applications can be granted permissions to your tenant by an admin consenting to the application for all users (Admin consent), a user consenting to the application for him or herself (User consent), or an admin integrating an application and enabling self-service access or assigning users directly to the application. As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

[Grant admin consent for Citrix](#)

Admin consent User consent

Search permissions

API Name	↑↓	Permission	↑↓	Type	↑↓	Granted through
----------	----	------------	----	------	----	-----------------

- Microsoft Teams 통합 정책을 사용하도록 설정합니다.

Microsoft Teams integration



제한 사항:

Secure Mail 에서 만든 모임의 경우 현재 Microsoft Outlook 일정에는 다음과 같은 기능 제한 사항이 있습니다.

- 온라인 참가 옵션을 사용할 수 없습니다.
- 회의 시작 알림을 사용할 수 없습니다.

임시 보관함 최소화

iOS 용 Secure Mail 에서는 전자 메일을 작성하는 동안 임시 보관함을 최소화하고 앱 내에서 탐색할 수 있습니다. 이 기능은 iOS 13 이상을 실행하는 장치에서 사용할 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [임시 보관함 전자 메일 최소화](#)를 참조하십시오.

MIME 헤더를 사용하여 피싱 전자 메일 보고

iOS 용 Secure Mail 에서 사용자가 피싱 메일을 보고하면 EML 파일이 해당 메일의 첨부 파일로 생성됩니다. 관리자는 이 메일을 수신하고 보고된 메일에 연결된 MIME 헤더를 볼 수 있습니다. 이 기능을 사용하려면 관리자가 Citrix Endpoint

Management 콘솔에서 피싱 보고 전자 메일 주소 정책을 구성하고 피싱 보고 메커니즘을 첨부 파일을 통해 보고로 설정해야 합니다. 자세한 내용은 [첨부 파일로 피싱 전자 메일 보고](#)를 참조하십시오.

WkWebView 지원

iOS 용 Secure Mail 은 WkWebView 를 지원합니다. 이 기능은 Secure Mail 의 전자 메일 및 일정 이벤트가 장치에서 렌더링되는 방식을 개선합니다.

Slack EMM 지원

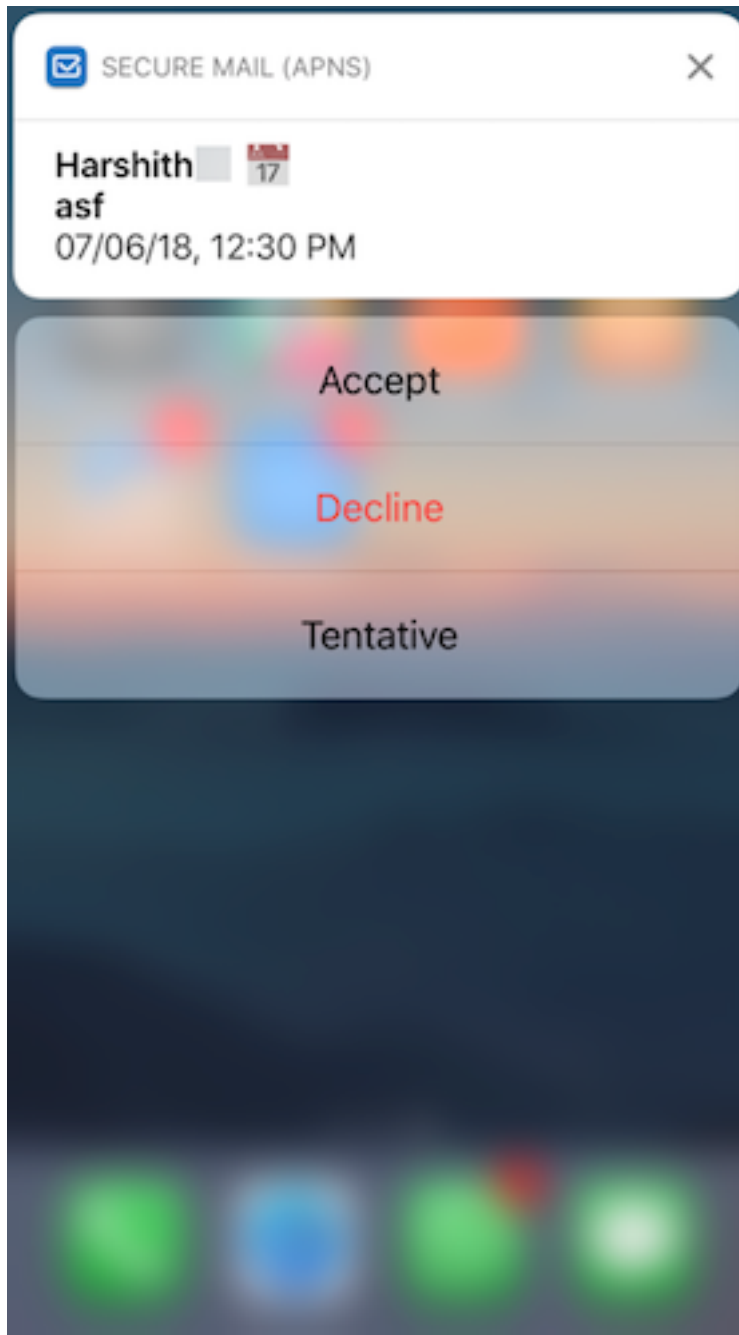
Slack EMM 은 EMM(엔터프라이즈 모빌리티 관리) 을 사용하는 Slack 고객을 위해 제공됩니다. iOS 용 Secure Mail 은 응용 프로그램 **Slack EMM** 을 지원하며, 이를 통해 관리자가 Secure Mail 을 **Slack** 앱과 통합할지 아니면 **Slack EMM** 앱과 통합할지 선택할 수 있습니다.

그룹 알림

그룹 알림 기능을 사용하면 전자 메일 스레드의 대화가 그룹화됩니다. 장치의 잠금 화면에서 그룹화된 알림을 간단히 확인할 수 있습니다. 그룹 알림 설정은 장치에서 기본적으로 사용되도록 설정되어 있습니다. 이 기능을 사용하려면 iOS 12 가 필요합니다.

알림 응답 옵션

iOS 용 Secure Mail 사용자는 수락, 거부 및 미정을 사용하여 회의 알림에 응답할 수 있습니다. 또한 회신 및 삭제를 사용하여 메시지 알림에 응답할 수 있습니다.



풍부한 푸시 알림 실패 메시지에 대한 향상된 기능

iOS 용 Secure Mail에서는 장치의 알림 센터에 알림 실패 유형에 따라 해당하는 푸시 알림 실패 메시지가 나타납니다. 자세한 내용은 [Secure Mail 알림](#)을 참조하십시오.

Microsoft 설정에서 다양한 방식의 푸시 알림 지원

iOS 용 Secure Mail 은 Microsoft EMS(Enterprise Mobility + Security)/Intune 및 최신 인증 (O365) 을 실행하는 설정에서 서식 있는 푸시 알림을 지원합니다. 서식 있는 푸시 알림 기능을 사용하려면 다음 사전 요구 사항을 충족해야 합니다.

- Endpoint Management 콘솔에서 푸시 알림을 켜짐으로 설정합니다.
- 네트워크 액세스 정책이 제한 없음으로 설정되어 있습니다.
- 잠긴 화면 알림 제어 정책이 허용 또는 전자 메일 보낸 사람 또는 이벤트 제목으로 설정되어 있습니다.
- Secure Mail** > 설정 > 알림으로 이동하여 메일 알림을 사용하도록 설정합니다.

파생된 자격 증명에 대한 S/MIME 지원

iOS 용 Secure Mail 은 파생된 자격 증명에 대해 S/MIME 를 지원합니다. 이 기능이 작동하려면 다음을 수행해야 합니다.

- 파생된 자격 증명을 S/MIME 인증서 원본으로 선택합니다. 자세한 내용은 [iOS 용 파생된 자격 증명](#)을 참조하십시오.
- Citrix Endpoint Management 에서 LDAP Attributes 클라이언트 속성을 추가합니다. 다음 정보를 사용합니다.
 - 키: SEND_LDAP_ATTRIBUTES
 - 값: `userPrincipalName=${ user.userprincipalname } ,sAMAccountName=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`

클라이언트 속성 추가 방법에 대한 단계는 XenMobile Server 의 경우 [클라이언트 속성](#)을 참조하고 Endpoint Management 의 경우 [클라이언트 속성](#)을 참조하십시오.

파생된 자격 증명을 통한 장치 등록 방법에 대한 자세한 내용은 [파생된 자격 증명을 사용하여 장치 등록](#)을 참조하십시오.

- Endpoint Management 콘솔에서 구성 > 앱으로 이동합니다.
- Secure Mail** 을 선택한 다음 편집을 클릭합니다.
- iOS 플랫폼에서 S/MIME 인증서 원본에 대해 파생된 자격 증명을 선택합니다.

Push notifications region: Americas

S/MIME certificate source: Derived Credential

Enable S/MIME during first Secure Mail startup: OFF

Calendar Web and Audio Options: GoToMeeting and User Entered

S/MIME public certificate source: Exchange

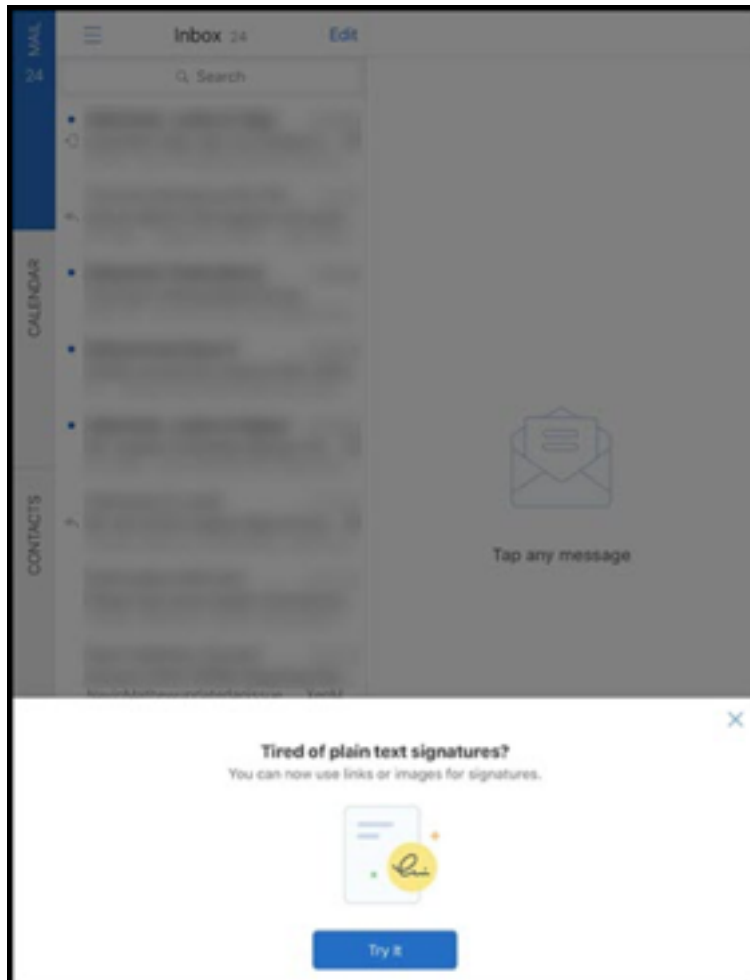
Ldap server address:

Ldap Base DN:

Back Next >

서식 있는 텍스트 서명

전자 메일 서명에 이미지 또는 링크를 사용할 수 있습니다. 서명을 업데이트하려면 이미지 또는 링크를 복사하여 서명 필드에 붙여 넣으면 됩니다.



서식 있는 텍스트 서명을 추가하려면

1. 사용할 이미지 또는 URL 을 복사합니다.
2. **Secure Mail** > 설정 > 서명으로 이동합니다.
3. 이미지 또는 URL 을 붙여 넣습니다.

또는 서명 필드를 길게 누르고 사진 삽입을 눌러 갤러리에서 이미지를 선택합니다.

Secure Mail 발신자 ID

iOS 용 Secure Mail 의 장치 설정에서 Secure Mail 발신자 ID 를 사용하도록 설정하여 Secure Mail 연락처에서 걸려오는 전화를 식별할 수 있습니다. 다음과 같은 관리 필수 구성 요소를 사용하도록 설정해야 합니다. Citrix Endpoint Management 에서 CallerIDSupportEnabled MDX 정책이 사용되도록 설정되었는지 확인합니다.

이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [발신자 ID 설정](#)을 참조하십시오.

일정에서 색상 설정

이 일정 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [동기화된 Secure Mail 일정에 색상 설정](#)을 참조하십시오.

Files 앱을 사용한 파일 첨부

Secure Mail for iOS 에서 iOS 의 기본 앱인 파일 앱을 사용하여 파일을 첨부할 수 있습니다. iOS 파일 앱에 대한 자세한 내용은 Apple 문서 [iPhone, iPad 및 iPod touch 에서 파일 앱 사용하기](#)를 참조하십시오. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [파일 보기 및 첨부](#)를 참조하십시오.

맞춤법 검사 기능

Secure Mail 맞춤법 검사는 다음과 같이 일반 > 키보드 아래에 있는 자동 대문자 표시 및 맞춤법 검사 설정과 상호 작용합니다.

		Secure Mail 에서의 맞춤법	
장치에서의 자동 수정	장치에서의 맞춤법 검사	검사	동작
켜짐	켜짐	켜짐	빨간색 밑줄이 표시됩니다. 누르면 단어가 분홍색으로 강조 표시되고 제안 내용이 나타납니다.
꺼짐	꺼짐	켜짐	빨간색 줄이 표시됩니다. 누르면 제안 내용이 나타나지 않습니다.
켜짐	켜짐	꺼짐	빨간색 밑줄이 표시되지 않습니다. 누르면 단어가 분홍색으로 강조 표시되고 제안 내용이 나타납니다.
꺼짐	꺼짐	꺼짐	빨간색 밑줄, 강조 표시 또는 제한 내용이 나타나지 않습니다.

Secure Mail 에서의 맞춤법			
장치에서의 자동 수정	장치에서의 맞춤법 검사	검사	동작
켜짐	꺼짐	켜짐	빨간색 밑줄이 표시됩니다. 누르면 단어가 분홍색으로 강조 표시되고 제안 내용이 나타납니다.
꺼짐	켜짐	켜짐	빨간색 밑줄이 표시됩니다. 누르면 단어가 분홍색으로 강조 표시되고 제안 내용이 나타납니다.
켜짐	꺼짐	꺼짐	빨간색 밑줄이 표시되지 않습니다. 누르면 단어가 분홍색으로 강조 표시되고 제안 내용이 나타납니다.
꺼짐	켜짐	꺼짐	빨간색 밑줄이 표시되지 않습니다. 누르면 단어가 분홍색으로 강조 표시되고 제안 내용이 나타납니다.

사서함 화면

사서함 화면에는 구성된 모든 계정이 표시되며 다음과 같은 보기가 포함됩니다.

- 모든 계정: 구성된 모든 Exchange 계정의 전자 메일이 포함됩니다.
- 개별 계정: 개별 계정의 전자 메일 및 폴더가 포함됩니다. 이러한 계정은 확장 시 하위 폴더가 표시되는 목록으로 표시됩니다.

모든 계정 사서함은 기본적으로 글로벌 보기입니다. 이 보기에는 장치에서 구성된 모든 Exchange 계정의 첨부 파일과 전자 메일이 포함됩니다.

모든 계정 사서함의 메뉴 항목은 다음과 같습니다.

- 모든 첨부 파일
- 받은 편지함
 - 읽지 않음
 - 플래그 지정됨
- 임시 보관함
- 보낸 편지함
- 보낼 편지함
- 지운 편지함

모든 계정 보기에는 여러 계정의 전자 메일이 종합적으로 표시되지만 다음 동작에는 기본 계정 또는 주 계정의 전자 메일 주소가 사용됩니다.

- 새 메시지
- 새 이벤트

새 메일을 작성하는 동안 모든 계정 보기에서 보낸 사람의 전자 메일 주소를 변경하려면 보낸 사람: 필드의 기본 주소를 누르고 표시되는 메일 계정에서 다른 계정을 선택합니다.

참고:

대화 보기에서 전자 메일을 작성하면 보낸 사람: 필드가 대화 보기에 지정된 전자 메일 주소로 자동 입력됩니다.

개별 계정

구성한 모든 계정은 모든 계정 아래에 목록으로 표시됩니다. 기본 계정 또는 주 계정이 항상 처음에 표시되고 다른 계정이 알파벳 순서로 표시됩니다.

개별 계정에는 생성한 하위 폴더가 표시됩니다. 폴더 옆에 있는 **V** 아이콘을 누르면 하위 폴더를 볼 수 있습니다.

다음 동작은 개별 계정에만 적용됩니다.

- 항목 이동
- 대화 보기에서 전자 메일 작성
- vCard 가져오기
- 연락처 저장

일정

일정에는 장치의 여러 계정과 관련된 모든 이벤트가 표시됩니다. 개별 계정에 색상을 설정하여 개별 계정과 관련된 일정 이벤트를 구분할 수 있습니다.

일정 이벤트에 색상을 설정하려면

1. 바닥글 표시줄에서 일정 아이콘을 누른 다음 왼쪽 위에 있는 햄버거 아이콘을 누릅니다.
일정 화면에 구성된 모든 계정이 표시됩니다.
2. Exchange 계정의 오른쪽에 표시된 기본 색상을 누릅니다.
색상 화면에 해당 계정에 사용할 수 있는 색상이 표시됩니다.
3. 원하는 색상을 선택한 후 저장을 누릅니다.
4. 이전 화면으로 돌아가려면 취소를 누릅니다.
선택한 색상이 해당 Exchange 계정과 관련된 모든 일정 이벤트에 설정됩니다.

일정 초대 또는 이벤트를 생성하는 경우 주최자 필드에 기본 계정의 전자 메일 주소가 자동으로 입력됩니다. 메일 계정을 변경하려면 이 전자 메일 주소를 누르고 다른 계정을 선택합니다.

참고:

종료 후 Secure Mail 을 시작하면 앱이 장치에 마지막으로 구성된 일정 설정을 복원합니다.

검색

사서함 또는 연락처 보기에서 글로벌 검색을 수행할 수 있습니다. 이 동작을 수행하면 앱의 모든 계정이 검색되고 해당하는 결과가 표시됩니다.

개별 계정 내의 모든 검색에서는 해당 계정과 관련된 결과만 표시됩니다.

iOS 의 전자 메일, 일정 이벤트 또는 인라인 이미지 인쇄

이제 iOS 장치의 전자 메일, 일정 이벤트 또는 인라인 이미지를 인쇄할 수 있습니다.

사전 요구 사항

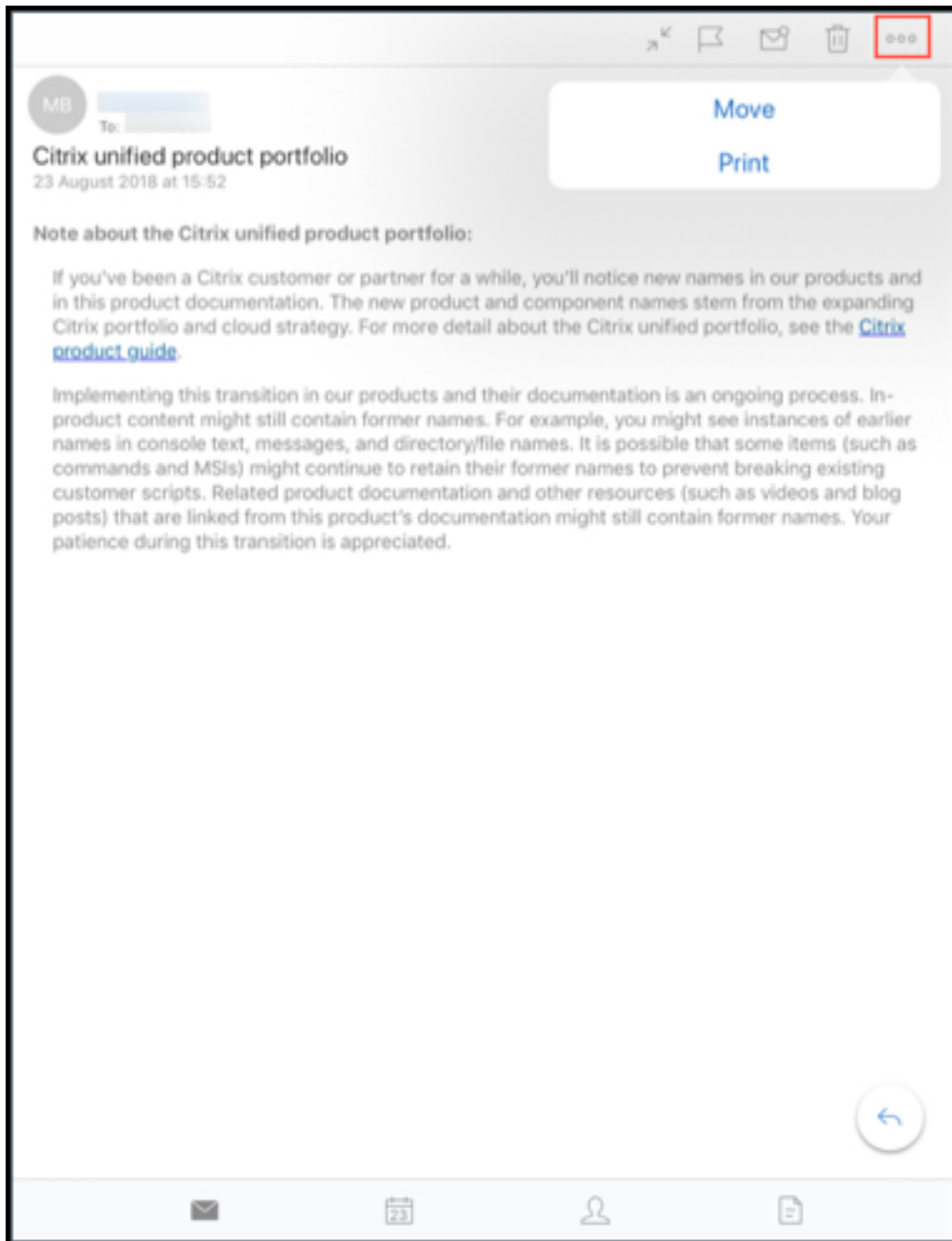
시작하기 전에 다음 요구 사항이 충족되었는지 확인하십시오.

- **AirPrint** 차단 옵션이 꺼짐으로 설정되어 있습니다.
- IRM 에서 보는 사람이 인쇄할 수 있도록 허용 옵션이 사용하지 않도록 설정되어 있습니다.

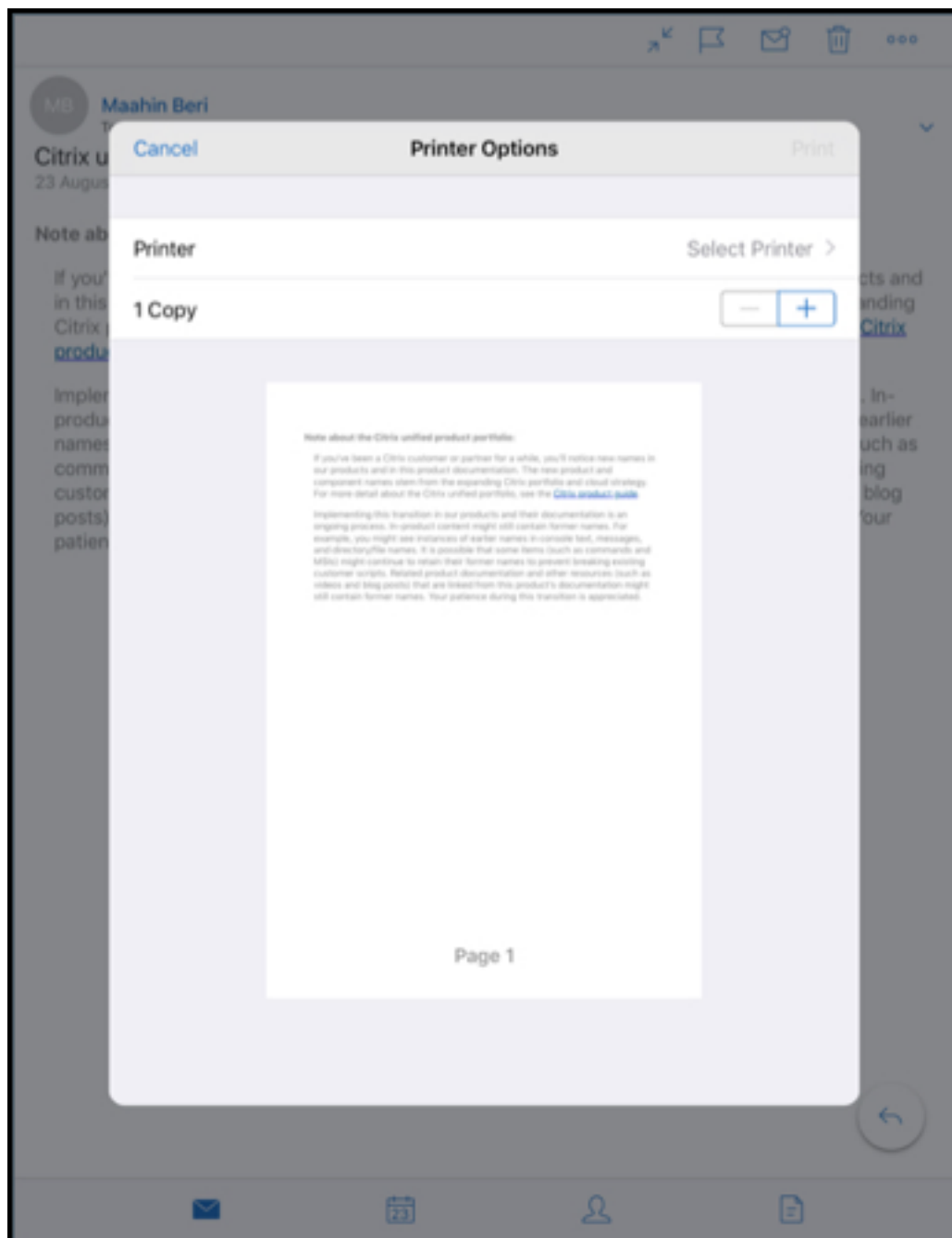
iOS 용 Secure Mail 에서는 인쇄 기능이 기본적으로 사용하도록 설정됩니다. 관리자는 Apple AirPrint 또는 Microsoft IRM(정보 권한 관리) 에서 관리 정책을 통해 인쇄 기능을 제어할 수 있습니다. 이러한 시나리오에서는 전자 메일, 일정 이벤트 또는 인라인 이미지 인쇄가 작동하지 않고 오류 메시지가 표시될 수 있습니다.

전자 메일을 인쇄하려면

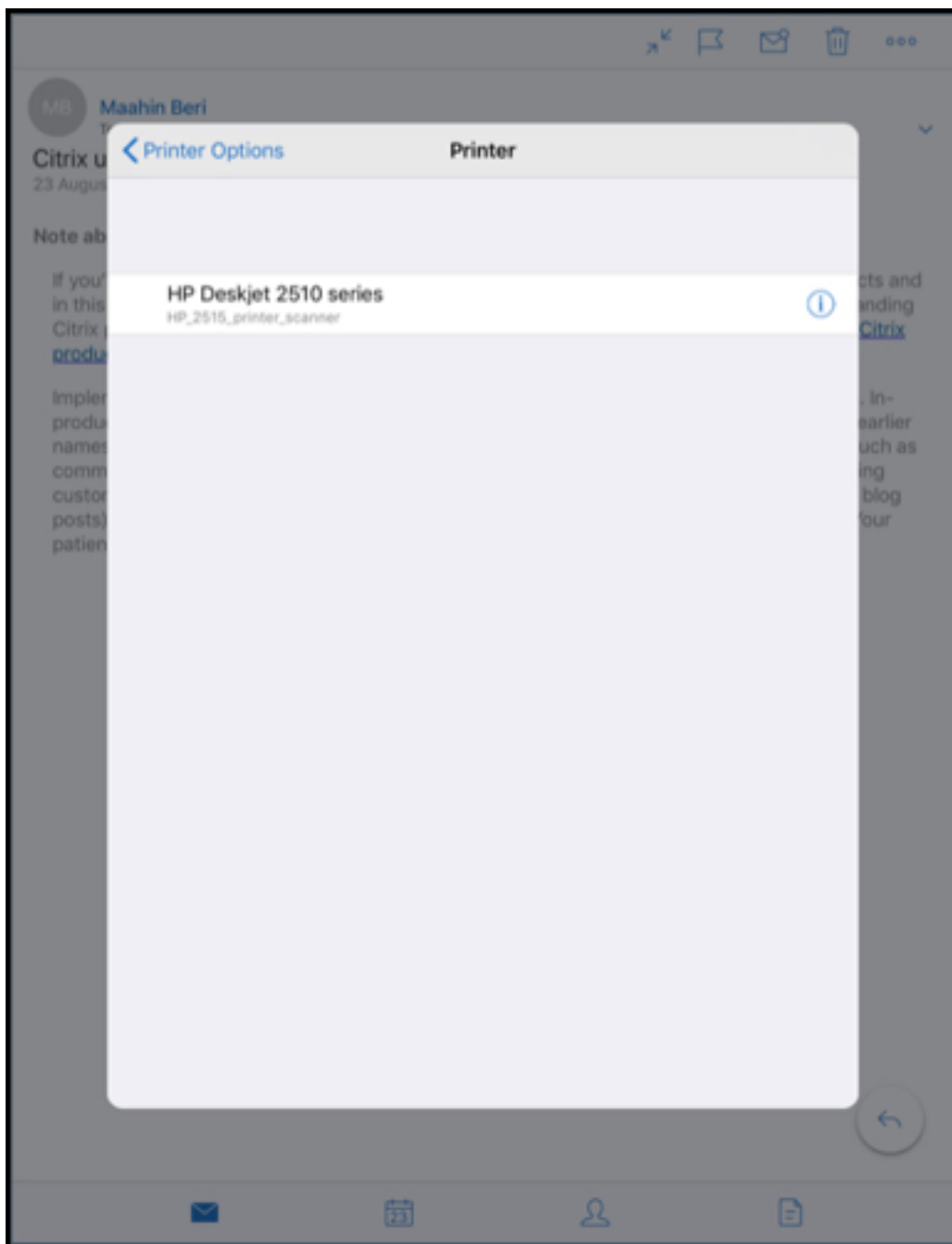
1. 인쇄하려는 전자 메일 항목을 엽니다.
2. 화면 왼쪽 위에 있는 자세히 아이콘을 누릅니다. 다음 옵션이 표시됩니다.
 - 이동
 - 인쇄



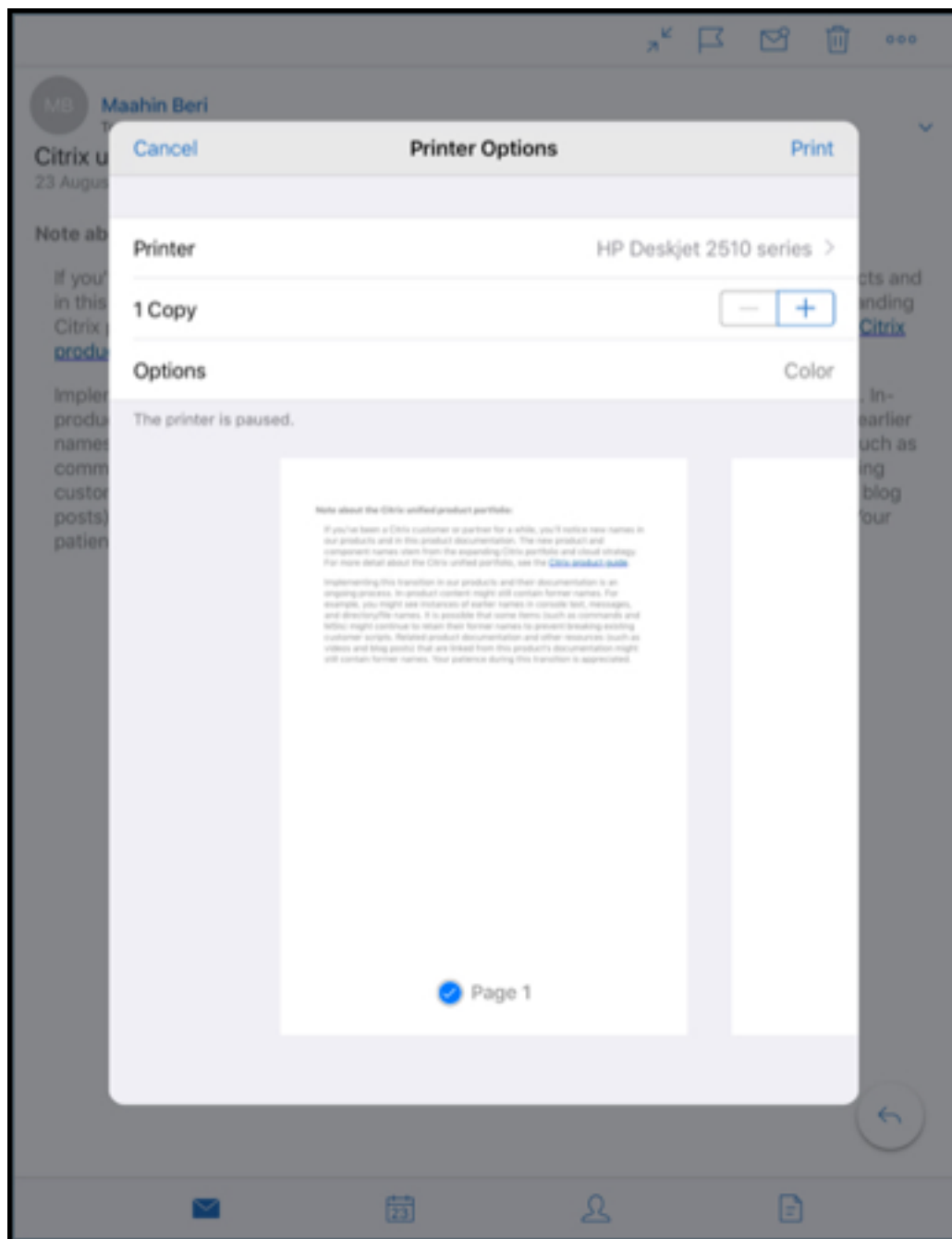
3. 인쇄를 누릅니다.
프린터 옵션 화면이 나타납니다.



4. 프린터를 선택하려면 프린터 선택을 누릅니다.
프린터 화면이 나타납니다.



5. 인쇄할 프린터를 선택합니다.



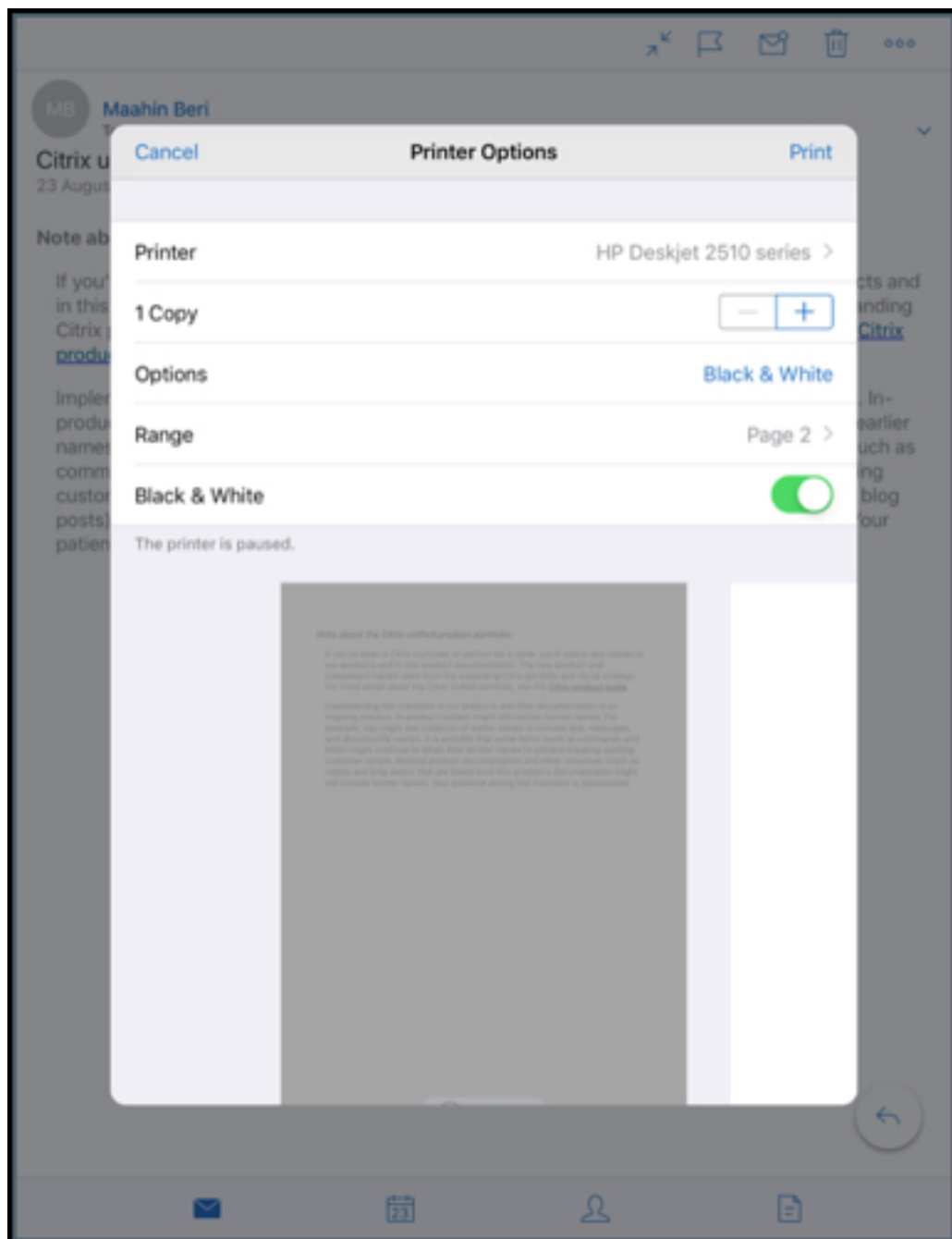
6. - 또는 + 를 눌러 인쇄할 사본의 수를 줄이거나 늘립니다.
7. 특정 페이지 또는 페이지 범위를 인쇄하려면 범위를 누릅니다.
페이지 범위 화면이 나타납니다. 기본적으로 모든 페이지가 선택됩니다.



8. 페이지 선택을 변경하려면 페이지 번호를 위 또는 아래로 살짝 밀니다.



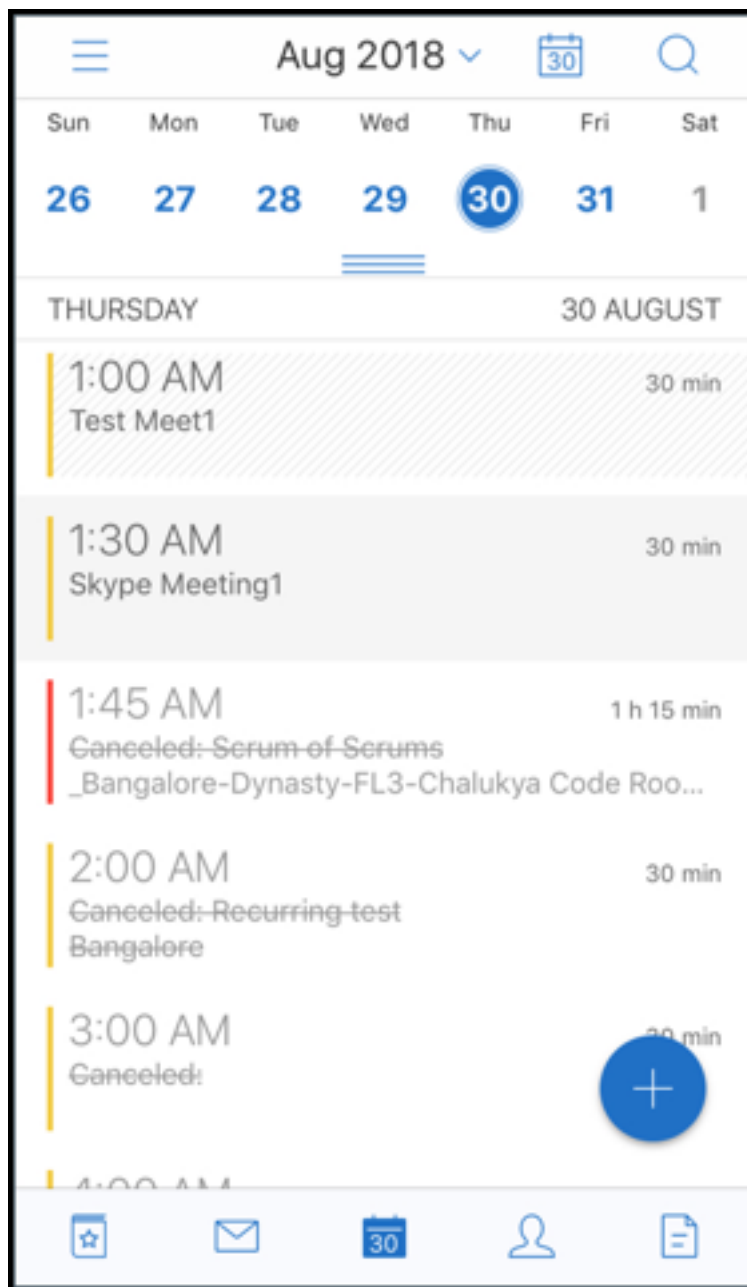
9. 프린터 옵션을 눌러 프린터 옵션 화면으로 돌아갑니다.



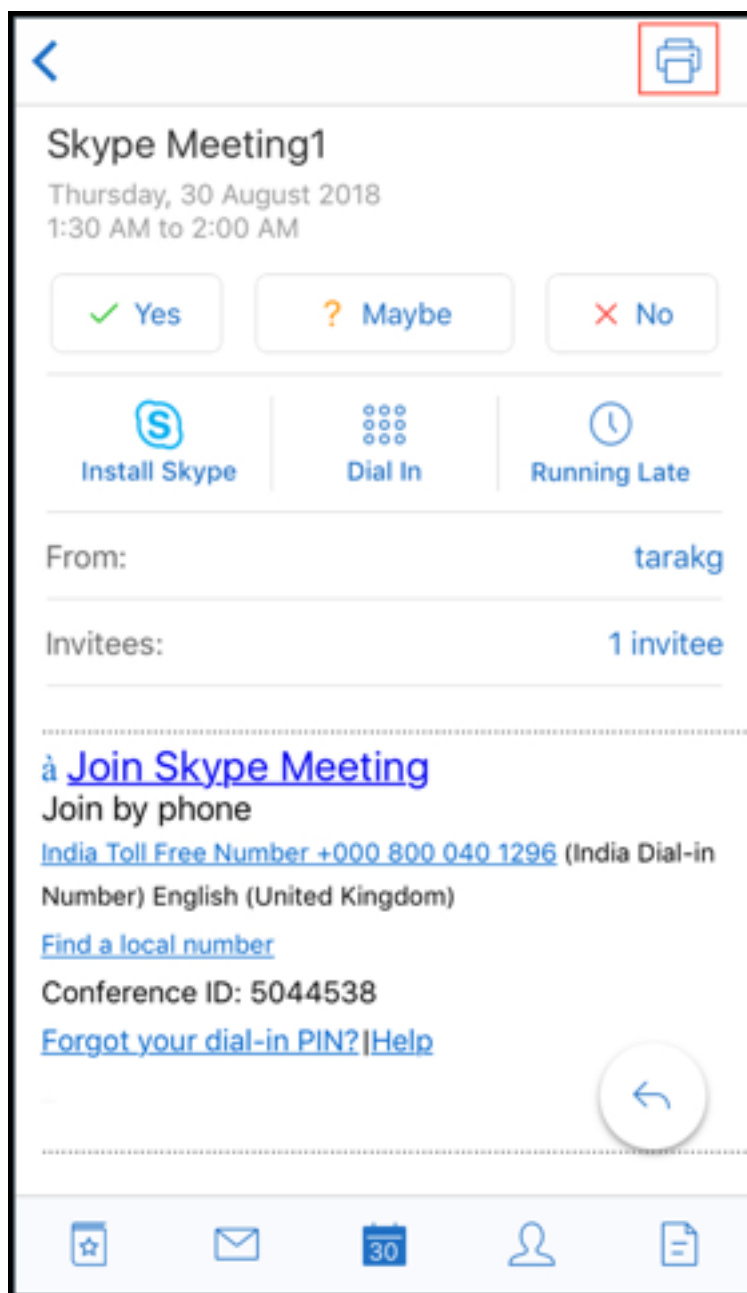
10. 흑백으로 인쇄하려면 흑백 단추를 누릅니다. 기본적으로 Secure Mail 은 컬러로 인쇄합니다.
11. 오른쪽 위의 인쇄를 눌러 전자 메일을 인쇄합니다.
12. 인쇄 작업을 취소하려면 왼쪽 위의 취소를 누릅니다.

일정 이벤트를 인쇄하려면

1. 일정으로 이동하고 이벤트를 선택합니다.

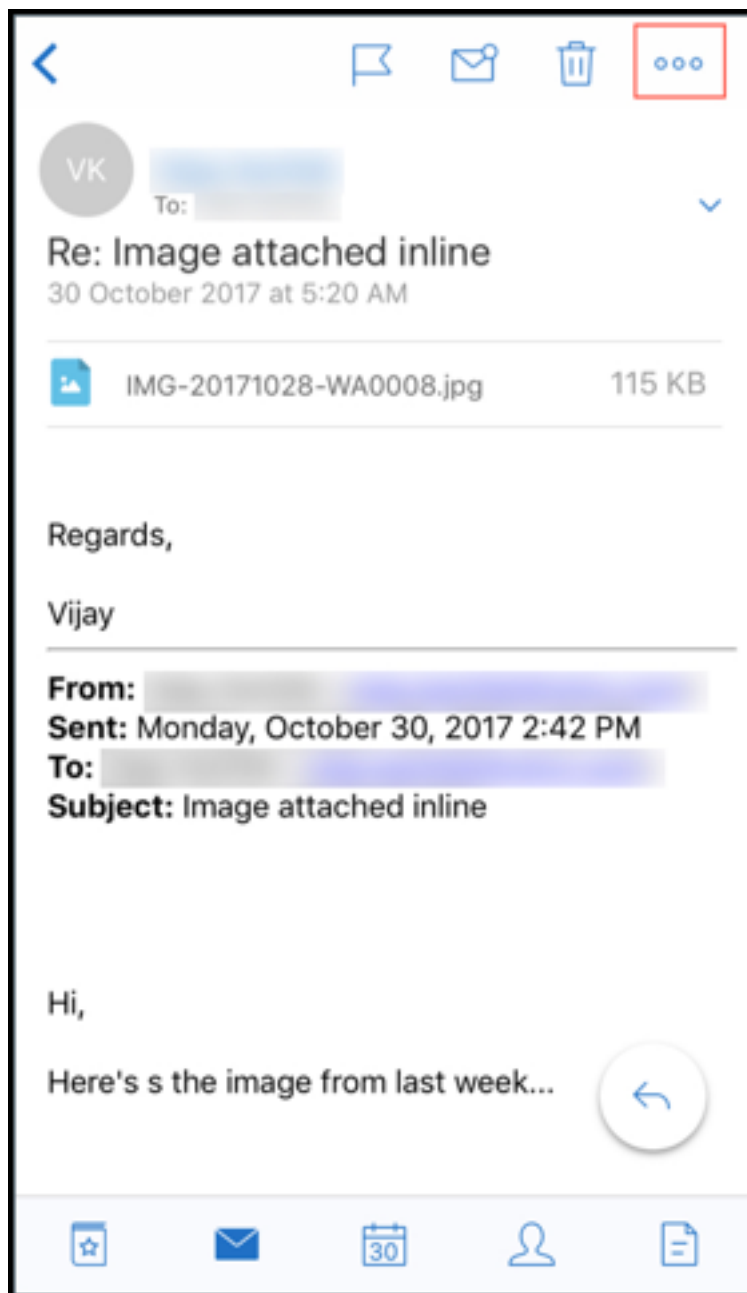


2. 인쇄 아이콘을 누르고 위의 전자 메일을 인쇄하려면 섹션에 설명된 동일한 지침을 따릅니다.



인라인 이미지를 인쇄하려면:

1. 인라인 이미지가 포함된 전자 메일 항목을 엽니다.
2. 자세히 아이콘을 누릅니다. 다음 옵션이 표시됩니다.
 - 이동
 - 인쇄
 - 취소



3. 인쇄를 누르고 위의 전자 메일을 인쇄하려면 섹션에 설명된 동일한 지침을 따릅니다.

다중 회의 코드 (모임에 전화 접속)

iOS 용 Secure Mail 은 다중 회의 코드를 지원합니다. 이제 사용 가능한 회의 코드 목록 중에서 하나를 선택하여 모임에 참가할 수 있습니다.

모임에 전화 접속하려면

1. 모임 초대를 열고 전화 접속을 누릅니다.
2. 전화 번호 목록이 나타나면 하나를 선택하여 전화를 겁니다.
3. 회의 코드 목록이 나타나면 하나를 선택하여 모임에 참가합니다.
4. 전화걸기를 눌러 모임에 참가합니다.

전자 메일 첨부 파일 인쇄 지원

iOS 용 Secure Mail 이 전자 메일 첨부 파일 인쇄를 지원합니다.

Android 기능

August 18, 2022

이 문서에서는 Secure Mail 에서 지원되는 Android 기능에 대해 설명합니다.

Secure Mail 일정 이벤트에서 Microsoft Teams 회의 만들기

Android 용 Secure Mail 에서 일정 이벤트를 만드는 중에 Microsoft Teams 회의 초대를 만들 수 있습니다. Microsoft Teams 회의를 만들려면 **Microsoft Teams** 회의를 전환합니다. 이벤트 세부 정보가 포함된 회의 초대 링크와 세부 정보가 자동으로 전송됩니다.


Cancel

New Event


Save

Weekly sync up meeting

Microsoft Teams

 Microsoft Teams meeting

☒

 Other meeting type

None

Invitees

None

All Day

☐

Time Zone

(GMT+5:30) India Standard Time

Starts

Fri, Mar 5, 2021 12:00 PM

Ends

Fri, Mar 5, 2021 1:00 PM

More Options

▼

Attach from Citrix Files

Notes

사전 요구 사항:

Azure Active Directory의 전역 관리자가 다음을 수행하는지 확인합니다.

- 최신 인증 (OAuth) 을 사용하도록 설정하고 유효한 Microsoft Teams 라이선스가 있는 Exchange Online 사서함 사용자인지 확인합니다.
- Secure Mail 앱에 대한 테넌트 전체의 관리자 동의를 제공합니다.
- Secure Mail 앱에서 Exchange 계정을 구성하고 모든 사용자가 로그인할 수 있도록 앱 권한을 허용합니다. 다음 화면을 참조하십시오.

Dashboard > Enterprise applications > Secure Mail

Secure Mail | Permissions

Enterprise Application

« Refresh Review permissions Got feedback?

Overview
Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups
- Single sign-on
- Provisioning

Security

- Permissions
- Token encryption

Permissions

Applications can be granted permissions to your tenant by an admin consenting to the application for all users (Admin consent), a user consenting to the application for him or herself (User consent), or an admin integrating an application and enabling self-service access or assigning users directly to the application. As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

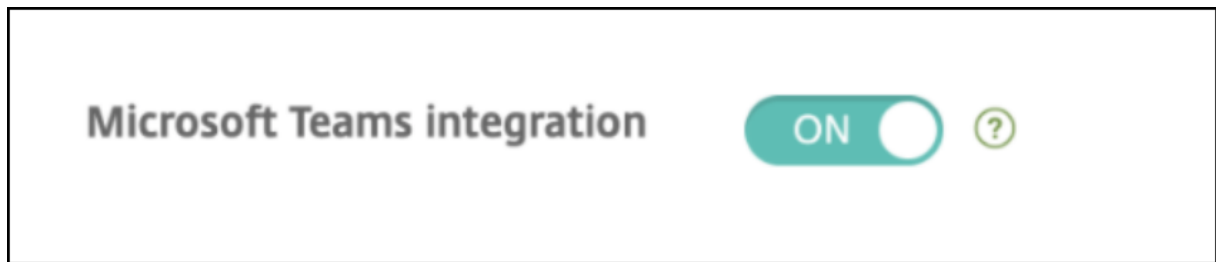
[Grant admin consent for Citrix](#)

Admin consent User consent

Search permissions

API Name	↑↓	Permission	↑↓	Type	↑↓	Granted through
----------	----	------------	----	------	----	-----------------

- Microsoft Teams 통합 정책을 사용하도록 설정합니다.



제한 사항:

Secure Mail 에서 만든 모임의 경우 현재 Microsoft Outlook 일정에는 다음과 같은 기능 제한 사항이 있습니다.

- 온라인 참가 옵션을 사용할 수 없습니다.
- 회의 시작 알림을 사용할 수 없습니다.

양방향 연락처 동기화

Android 용 Secure Mail 에서 로컬 연락처 목록을 사용하여 Secure Mail 연락처를 생성, 편집 및 삭제할 수 있습니다.

보낸 메일 실행 취소

Android 용 Secure Mail 에서 보낸 메일을 실행 취소할 수 있습니다. 보내기 단추를 누르면 보낸 작업을 실행 취소할 수 있는 알림 메시지가 표시됩니다. 실행 취소를 눌러 보낸 작업을 되돌리고 메일 및 메일 받는 사람을 편집하거나 첨부 파일을 첨부 또는 제거하거나 메일을 삭제합니다.

임시 보관함 폴더에서 첨부 파일 동기화

Android 용 Secure Mail 에서 임시 보관함 폴더가 동기화되면 첨부 파일도 동기화되고 모든 장치에서 사용할 수 있게 됩니다. 이 기능은 Exchange ActiveSync 버전 16 이상을 실행하는 장치에서 사용할 수 있습니다.

앱에서 바로 **PDF** 파일 보기

Android 용 Secure Mail 의 경우 PDF 파일을 책갈피 및 주석과 함께 앱 내에서 볼 수 있습니다. 다른 Microsoft Office 첨부 파일의 향상된 보기도 가능합니다.

Microsoft Office 365 로 최신 인증을 실행하는 설정의 터널링 정책에 웹 **SSO** 를 사용할 수 있습니다

Android 용 Secure Mail 에 **Use Web SSO for tunneling**(터널링에 웹 **SSO** 사용)이라는 이름의 새 정책이 추가되었습니다. 이 정책을 사용하면 OAuth 트래픽을 터널링하여 터널링—웹 SSO 를 통과할 수 있습니다. 이 작업을 수행하려면:

- **Use Web SSO for tunneling**(터널링에 웹 **SSO** 사용) 정책을 **On**(켜기) 으로 설정합니다.
- 네트워크 액세스 정책에서 **Tunneled - Web SSO**(터널링됨 - 웹 **SSO**) 옵션을 선택합니다.
- **Background services**(백그라운드 서비스) 정책에서 OAuth 와 관련된 모든 호스트 이름을 제외합니다.

일정 이벤트 끌어서 놓기

Android 용 Secure Mail 에서 이벤트를 끌어서 놓는 방법으로 기존 일정 이벤트의 시간을 변경할 수 있습니다. 이 일정 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [일정 이벤트 시간 변경](#)을 참조하십시오.

Google Play 의 **64** 비트 앱 지원

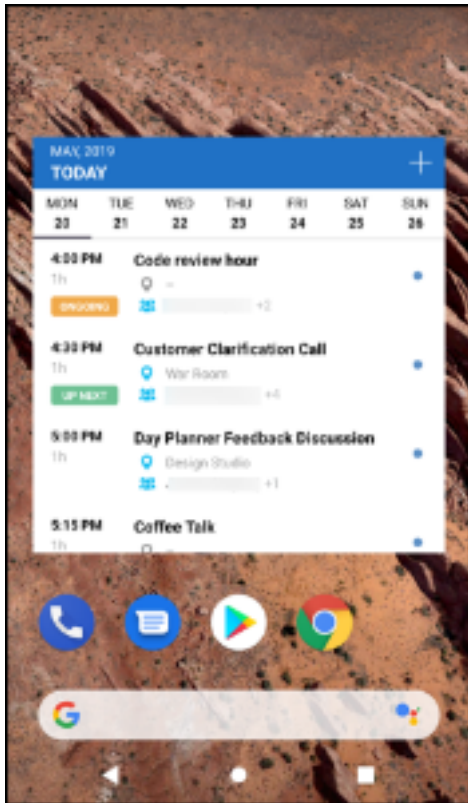
Android 용 Secure Mail 은 64 비트 아키텍처를 지원합니다.

Android 용 **Secure Mail** 에서 당겨서 새로 고침 **UI** 개선

Material Design 지침에 따라 당겨서 새로 고침 기능을 다소 개선했습니다. 햄버거 아이콘을 누르면 화면 하단에서 동기화 타임스탬프를 사용할 수 있습니다.

일정 목록에 대한 위젯

Android 용 Secure Mail 에서 일정 목록을 위젯으로 사용할 수 있습니다. 이 위젯에서 일정의 한 주 동안 예정된 이벤트를 볼 수 있습니다. 이 기능을 사용하면 일정 이벤트를 만들고 기존 이벤트를 보고 세부 정보를 편집할 수 있습니다. 홈 화면에 배치된 위젯에는 화면 캡처 차단 정책이 적용되지 않습니다. 그러나 일정 목록 위젯 허용 정책을 사용하여 위젯을 사용하지 않도록 설정할 수 있습니다.



네트워크 액세스 정책

Android 용 Secure Mail 에서 터널링됨 - 웹 **SSO** 라는 새 옵션이 네트워크 액세스 MDX 정책에 추가되었습니다. 이 정책을 구성하면 터널링됨-웹 SSO 및 STA(Secure Ticket Authority) 를 통해 내부 트래픽을 동시에 유연하게 터널링할 수 있습니다. 또한 NTLM, Okta, Kerberos 등과 같은 인증 서비스에 대해 터널링됨-웹 SSO 연결을 허용할 수 있습니다. STA 를 처음 구성할 때 서비스 주소의 개별 FQDN 및 포트를 백그라운드 네트워크 서비스 정책에 추가해야 합니다. 하지만 터널링됨 - 웹 **SSO** 옵션을 구성하는 경우 이러한 구성이 필요하지 않습니다.

Citrix Endpoint Management 콘솔에서 Android 용 Secure Mail 에 대해 이 정책을 사용하도록 설정하려면:

1. Android 용.mdx 파일을 다운로드하여 사용합니다. 자세한 내용은 [MDX 앱 추가](#)의 단계를 참조하십시오.
2. 네트워크 액세스 정책에서 터널링됨-웹 **SSO** 옵션을 클릭합니다. 자세한 내용은 [앱 네트워크 액세스](#)를 참조하십시오.

피드 카드에 대한 개선 사항

Android 용 Secure Mail 에서는 기존 피드 폴더에 다음과 같은 개선이 이루어졌습니다.

- 자동으로 동기화된 모든 폴더의 모임 초대가 피드 카드에 표시됩니다.
- 피드 카드에 최대 5 개의 예정된 모임이 표시됩니다.
- 이제 예정된 모임이 현재 시간으로부터 24 시간의 기간을 기준으로 표시됩니다. 이러한 모임 초대는 오늘과 내일로 구분됩니다. 이전 릴리스에서는 하루가 끝날 때까지 예정된 모임이 피드에 표시되었습니다.

첨부 파일 보기

Android 용 Secure Mail에서는 메일 및 일정의 첨부 파일을 손쉽게 볼 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [파일 보기 및 첨부](#)를 참조하십시오.

전자 메일 및 일정 이벤트 인쇄

Android 용 Secure Mail에서 Android 장치의 전자 메일 및 일정 이벤트를 인쇄할 수 있습니다. 이 인쇄 기능은 Android 인쇄 프레임워크를 사용합니다.

사전 요구 사항

- Citrix Endpoint Management 콘솔에서 관리자가 인쇄 차단 정책을 꺼짐으로 설정했는지 확인합니다. Android의 이 정책에 대한 자세한 내용은 [Block Printing policy\(인쇄 차단 정책\)](#)를 참조하십시오.
- 전자 메일이 IRM으로 보호되는 경우 전자 메일에서 보는 사람이 인쇄할 수 있도록 허용 옵션을 사용하도록 설정해야 합니다.

이러한 정책이 올바르게 설정되지 않은 경우 전자 메일 또는 일정 이벤트를 인쇄할 수 없습니다.

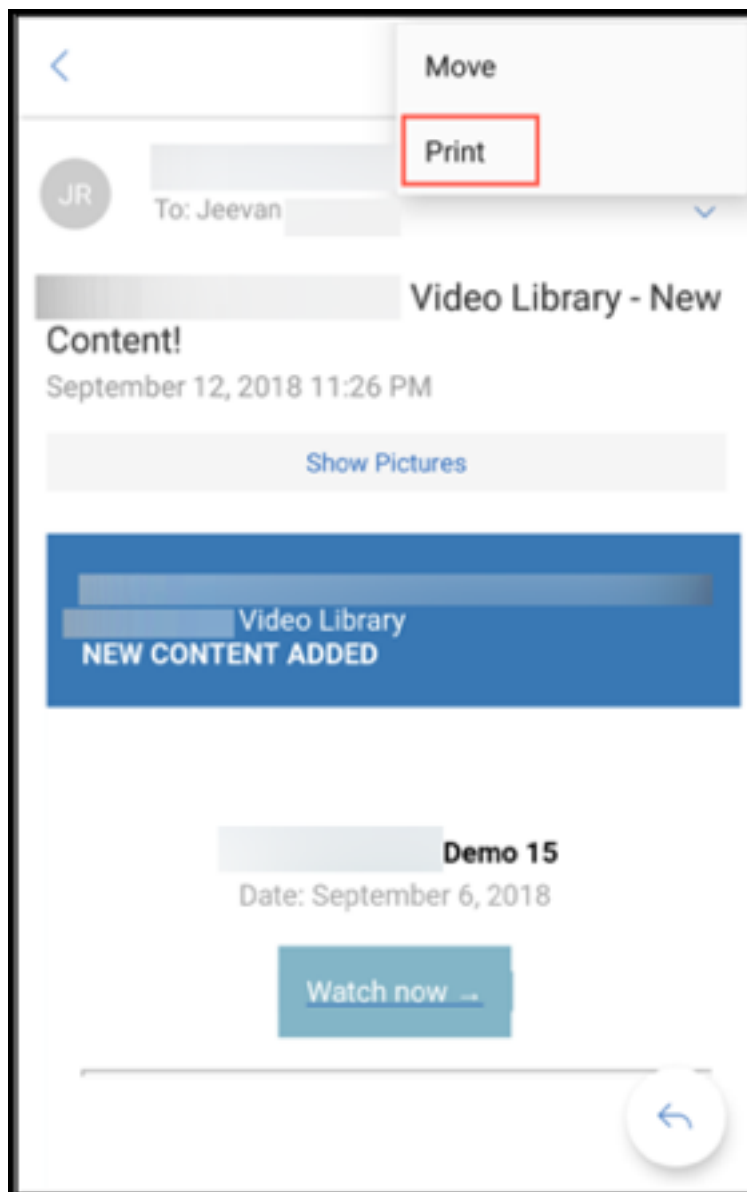
참고:

이 인쇄 기능에는 다음과 같은 알려진 제한 사항이 있습니다.

- 인라인 이미지는 사진 표시를 눌러 이미지를 다운로드한 경우에만 인쇄됩니다. 사진 표시를 누르지 않으면 이미지 자리 표시자만 인쇄됩니다.
- Secure Mail에서 크기가 큰 전자 메일이 잘립니다. 인쇄 전에 전체 메시지 다운로드를 눌러 전체 전자 메일을 인쇄하십시오. 전체 메시지가 다운로드되지 않으면 잘린 전자 메일이 인쇄됩니다.
- 전자 메일 또는 이벤트를 인쇄하는 동안 이러한 항목의 메타데이터는 추가되지 않습니다.

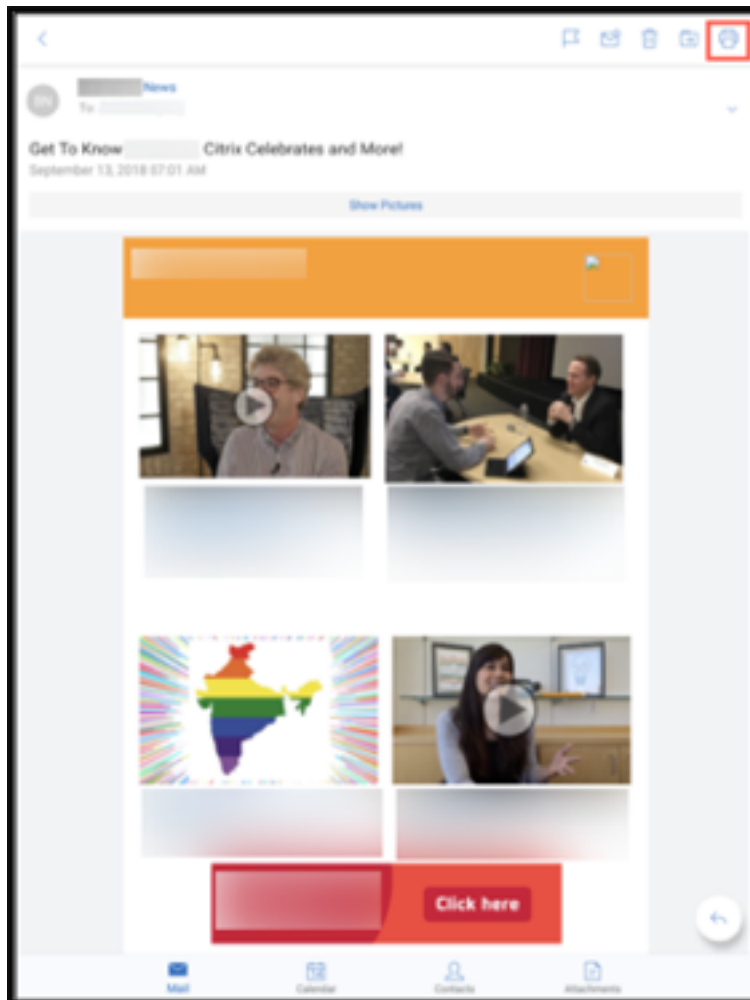
전자 메일을 인쇄하려면

1. 인쇄하려는 전자 메일을 엽니다.
2. 화면 왼쪽 위에 있는 자세히 아이콘을 누릅니다. 다음 옵션이 표시됩니다.
 - 이동
 - 인쇄

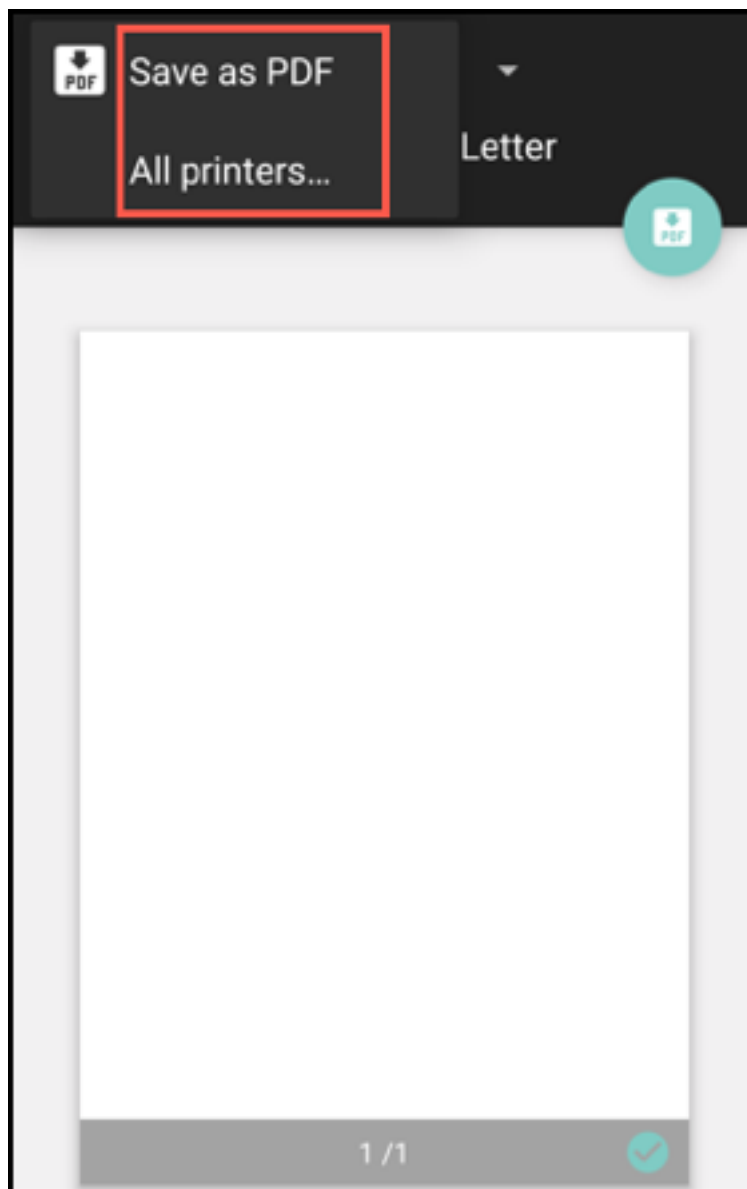


참고:

태블릿에서는 화면 왼쪽 위의 인쇄 아이콘을 직접 사용하여 전자 메일을 인쇄할 수 있습니다.



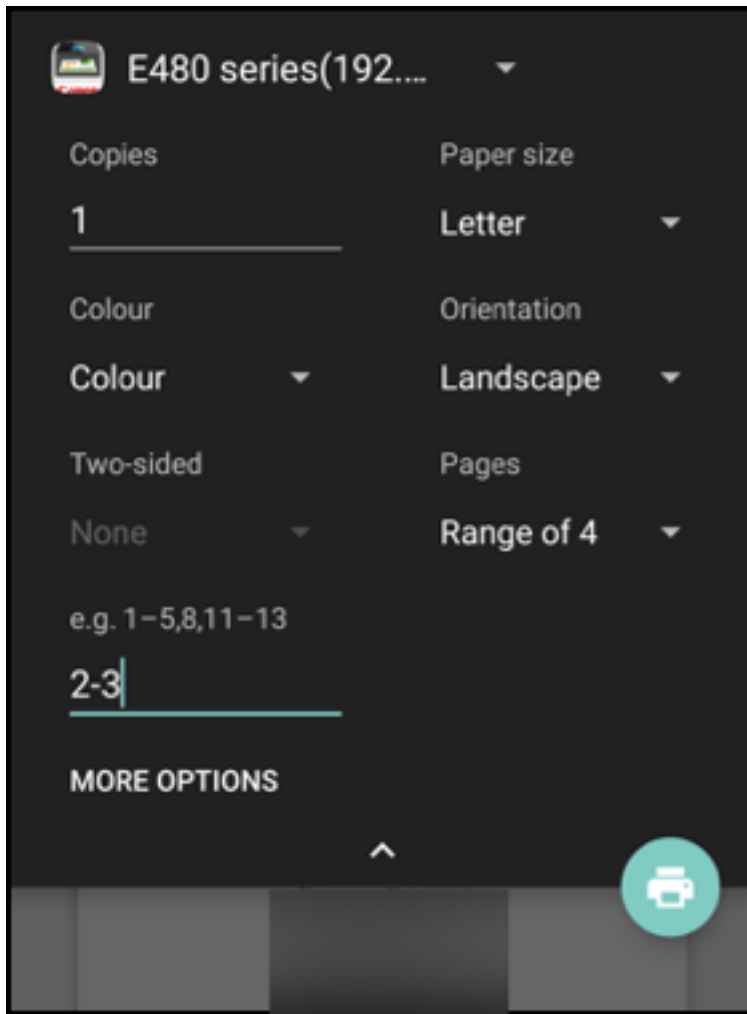
1. 인쇄를 누릅니다. 전자 메일의 미리 보기가 나타납니다.
2. 목록을 누르면 다음 옵션이 나타납니다.
 - PDF 로 저장
 - 모든 프린터



3. **PDF** 로 저장을 눌러 전자 메일을 PDF 형식으로 저장합니다.
4. 모든 프린터를 누릅니다. 요구 사항에 따라 프린터를 설치합니다.
5. 프린터가 설치되면 프린터 선택을 눌러 프린터를 선택합니다. 프린터 화면이 나타납니다.

참고:

인쇄 옵션은 선택한 프린터에 따라 다릅니다. 다음 이미지는 Canon E480 프린터에 대한 것이며 설명을 위해 사용되었습니다.



6. 인쇄할 프린터를 선택합니다. 다음 인쇄 옵션을 사용합니다.

- 인쇄할 사본 수를 수동으로 입력합니다.
- 목록에서 용지 크기를 선택합니다.
- 목록에서 색상을 선택합니다.
- 필요에 따라 페이지 방향을 선택합니다.
- 페이지 또는 페이지 범위를 선택하고 페이지 범위를 수동으로 입력합니다.

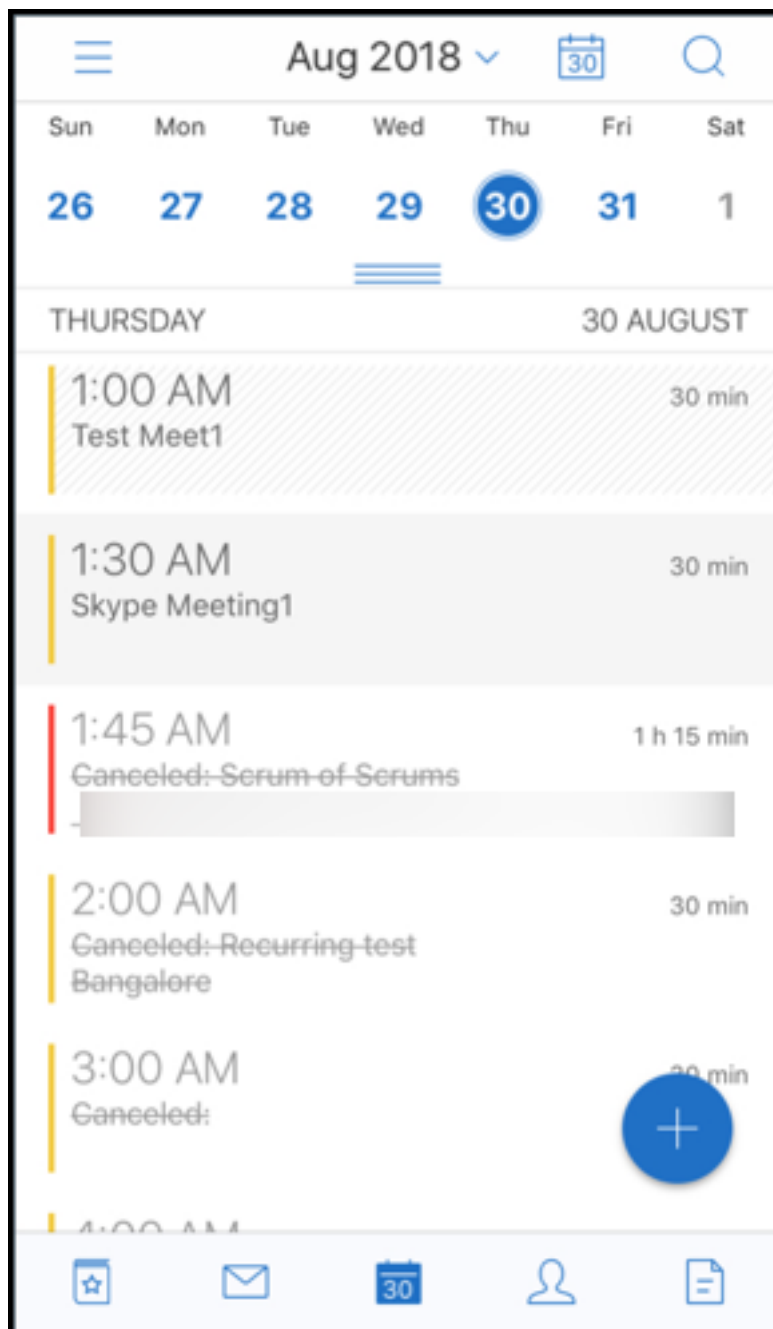
7. 인쇄 옵션을 설정한 후 화면에서 인쇄 아이콘을 누릅니다.

인라인 이미지를 인쇄하려면

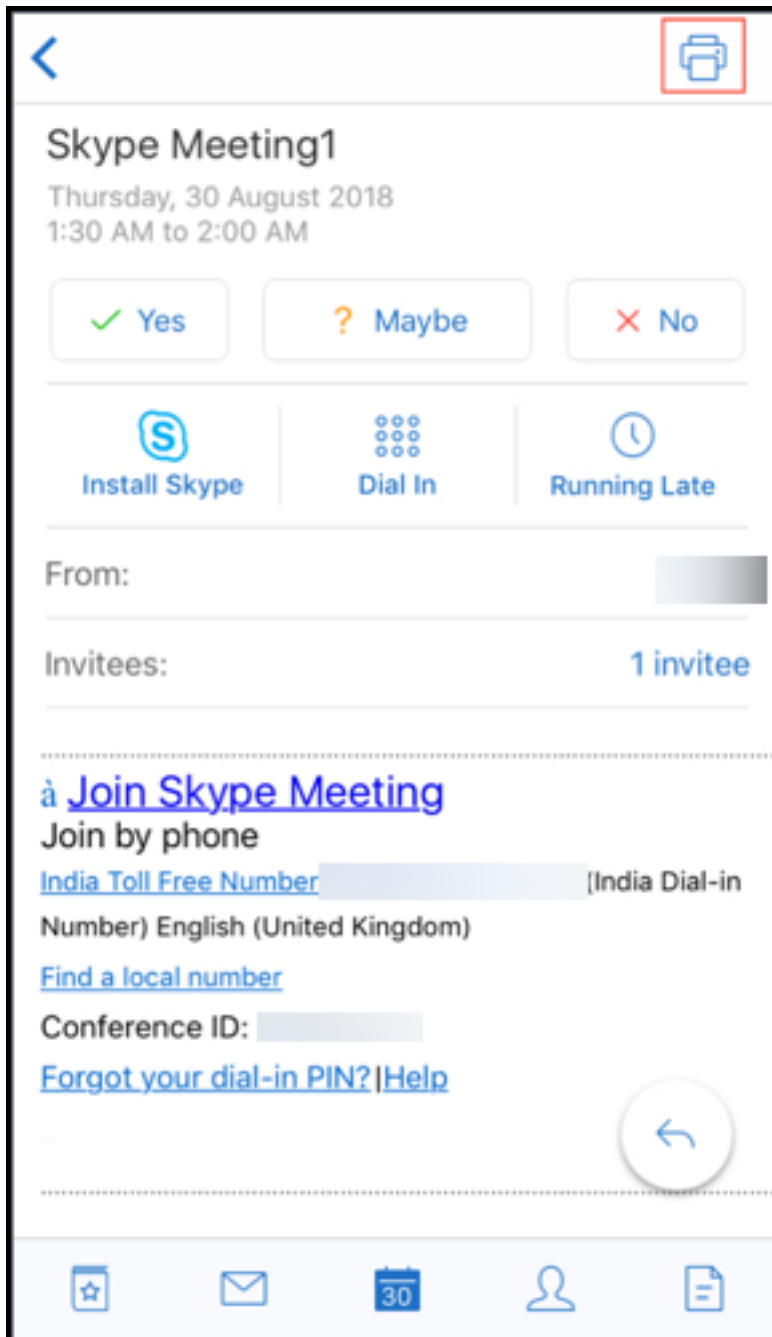
- 전자 메일 안에서 사진 표시를 누르고 위의 [전자 메일을 인쇄하려면](#) 섹션에 설명된 지침을 따릅니다.

일정 이벤트를 인쇄하려면

1. 일정으로 이동하고 이벤트를 누릅니다.



2. 인쇄 아이콘을 누르고 위의 전자 메일을 인쇄하려면 섹션에 설명된 동일한 지침을 따릅니다.



ActiveSync 헤더를 사용하여 피싱 전자 메일 보고

Android 용 Secure Mail 에서 사용자가 피싱 메일을 보고하면 EML 파일이 해당 메일의 첨부 파일로 생성됩니다. 관리자는 이 메일을 수신하고 보고된 메일에 연결된 ActiveSync 헤더를 볼 수 있습니다.

이 기능을 사용하려면 관리자가 Citrix Endpoint Management 콘솔에서 피싱 보고 전자 메일 주소 정책을 구성하고 피싱 보고 메커니즘을 첨부 파일을 통해 보고로 설정해야 합니다. Secure Mail 의 MDX 정책 구성에 대한 자세한 내용은 [모바일 생산성 앱에 대한 MDX 정책](#)을 참조하십시오.

하위 폴더 알림

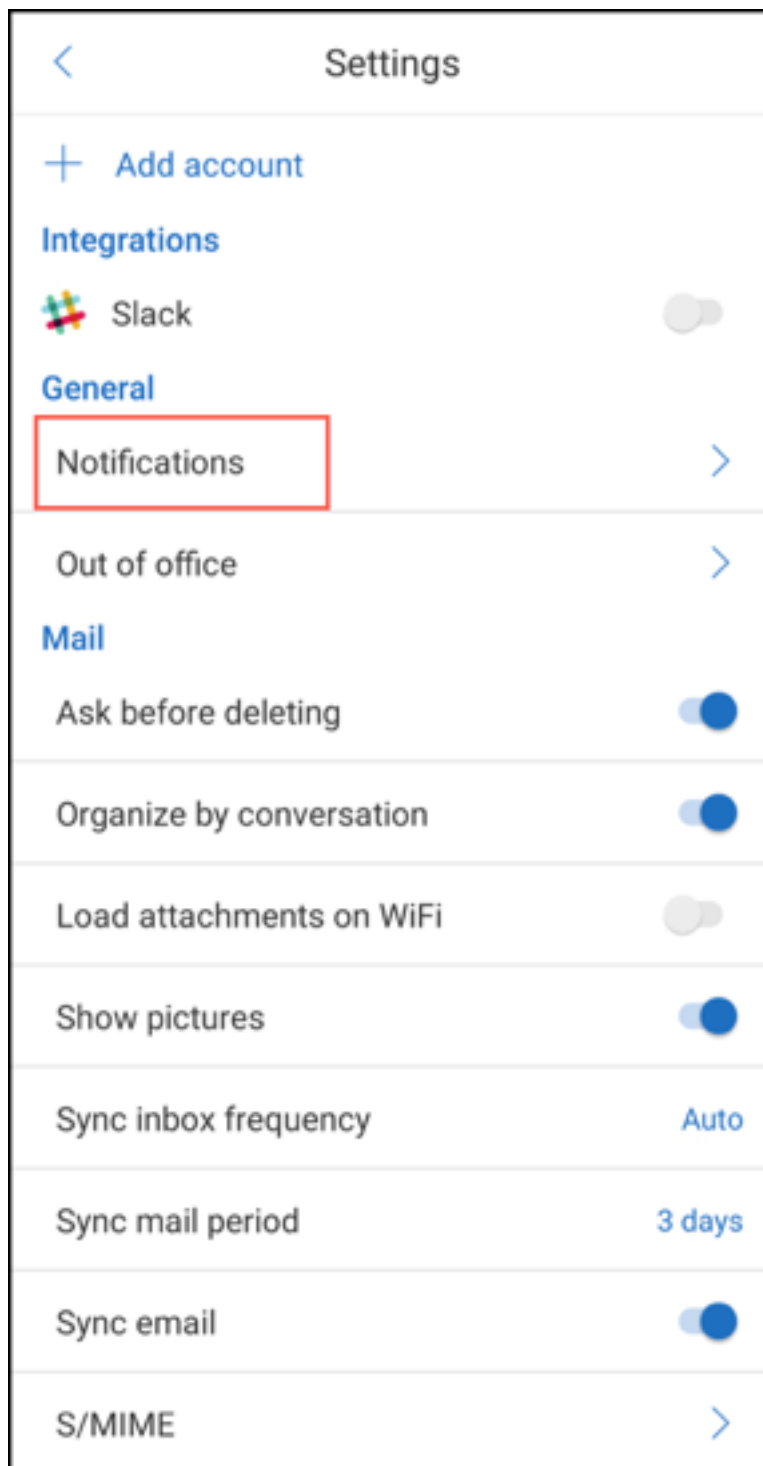
Android 용 Secure Mail 에서 메일 계정의 하위 폴더에서 메일 알림을 받을 수 있습니다.

참고:

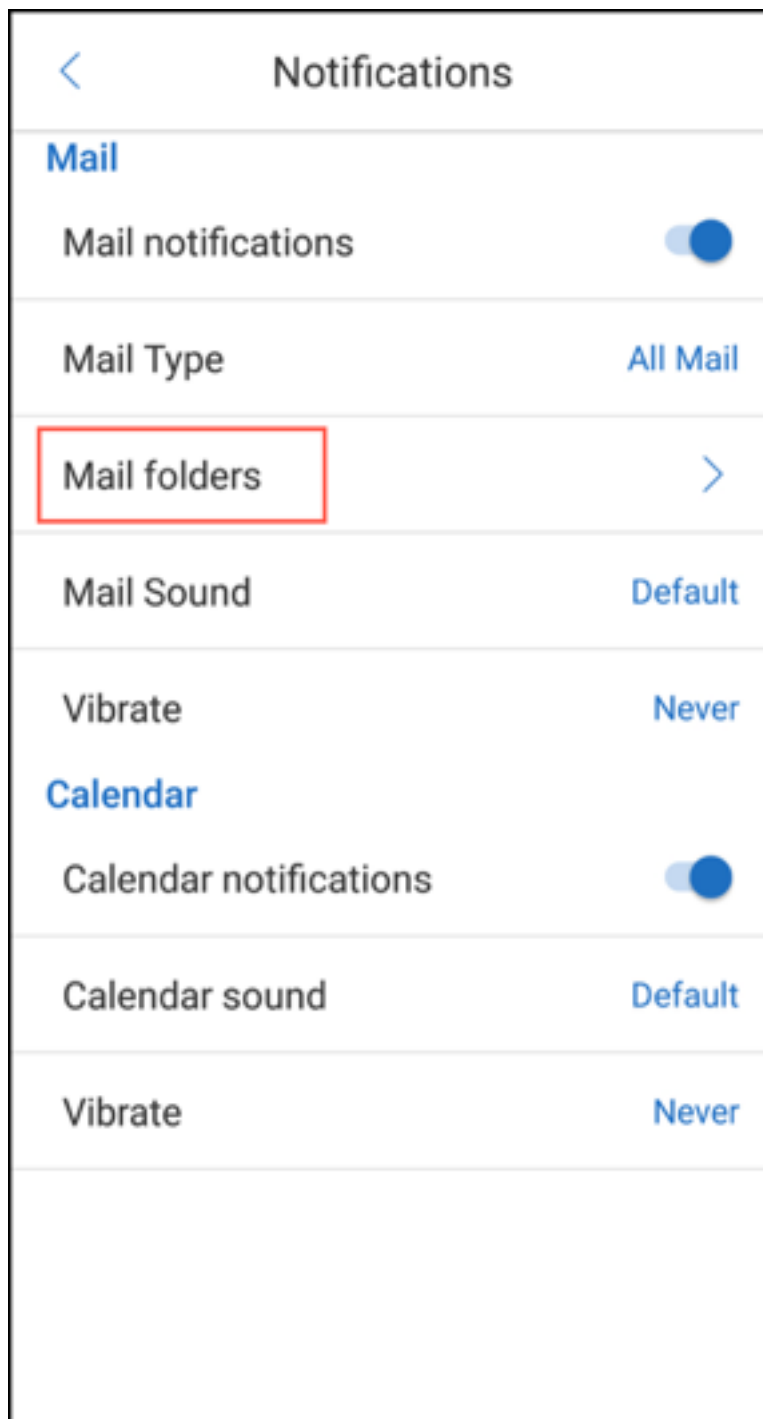
- 하위 폴더에 대한 알림을 받으려면 Endpoint Management 콘솔에서 FCM 기반 푸시 알림이 사용되도록 설정되었는지 확인합니다. FCM 기반 푸시 알림 구성에 대한 내용은 [Secure Mail 을 위한 푸시 알림](#)을 참조하십시오.
- Lotus Notes Server 의 경우 하위 폴더 알림 기능을 사용할 수 없습니다.

하위 폴더에 대한 알림을 사용하도록 설정하려면

1. 설정으로 이동한 다음 일반에서 알림을 누릅니다.



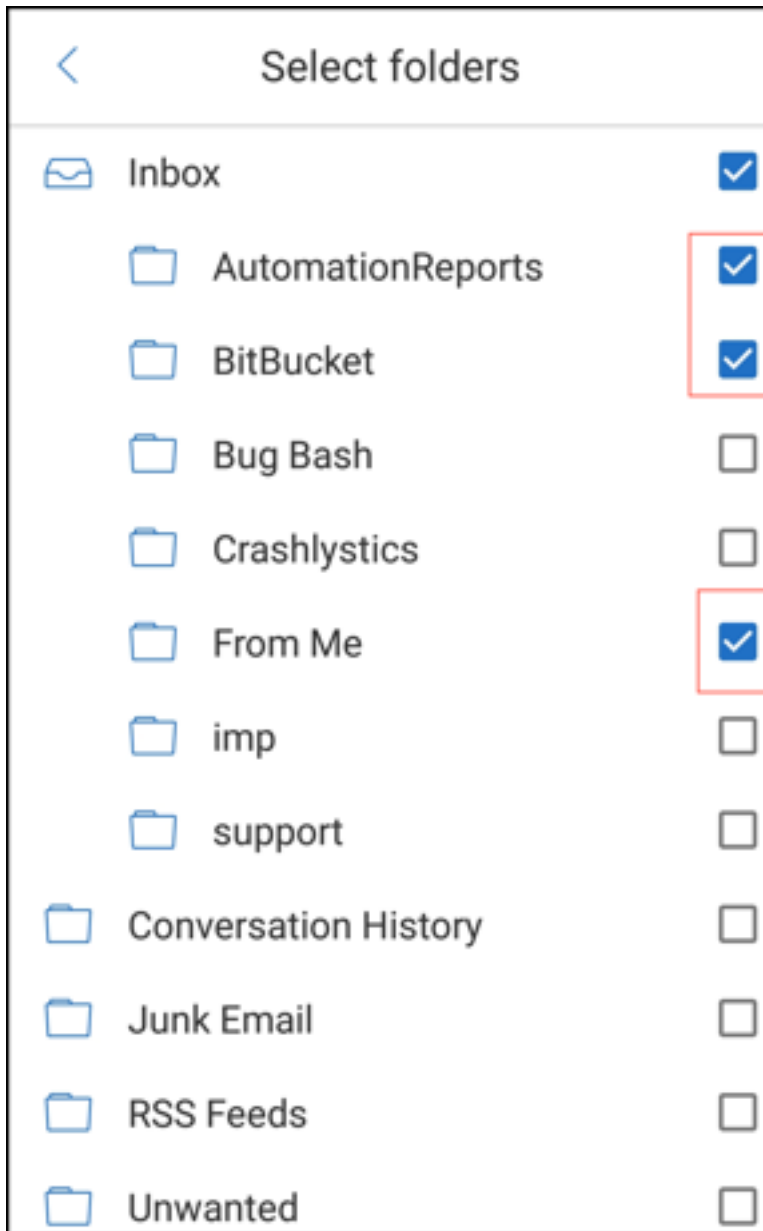
2. 알림 화면에서 메일 폴더를 누릅니다. 받은 편지함 내의 하위 폴더 목록이 나타납니다.



3. 알림을 받을 하위 폴더를 눌러 선택합니다. 받은 편지함이 기본적으로 선택되어 있습니다.

참고:

하위 폴더에 대한 알림을 사용하도록 설정하면 자동 동기화가 사용됩니다.

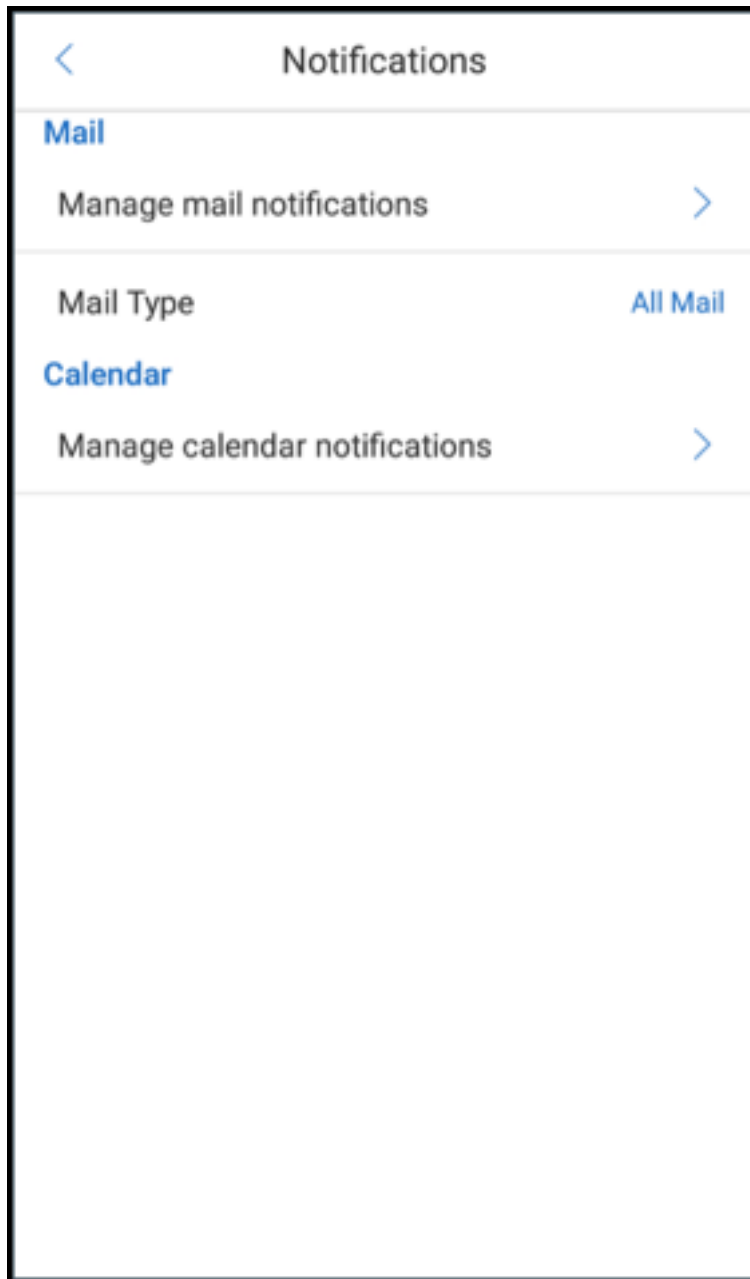


하위 폴더 알림을 사용하지 않으려면 알림을 받지 않을 하위 폴더의 확인란을 선택 취소합니다.

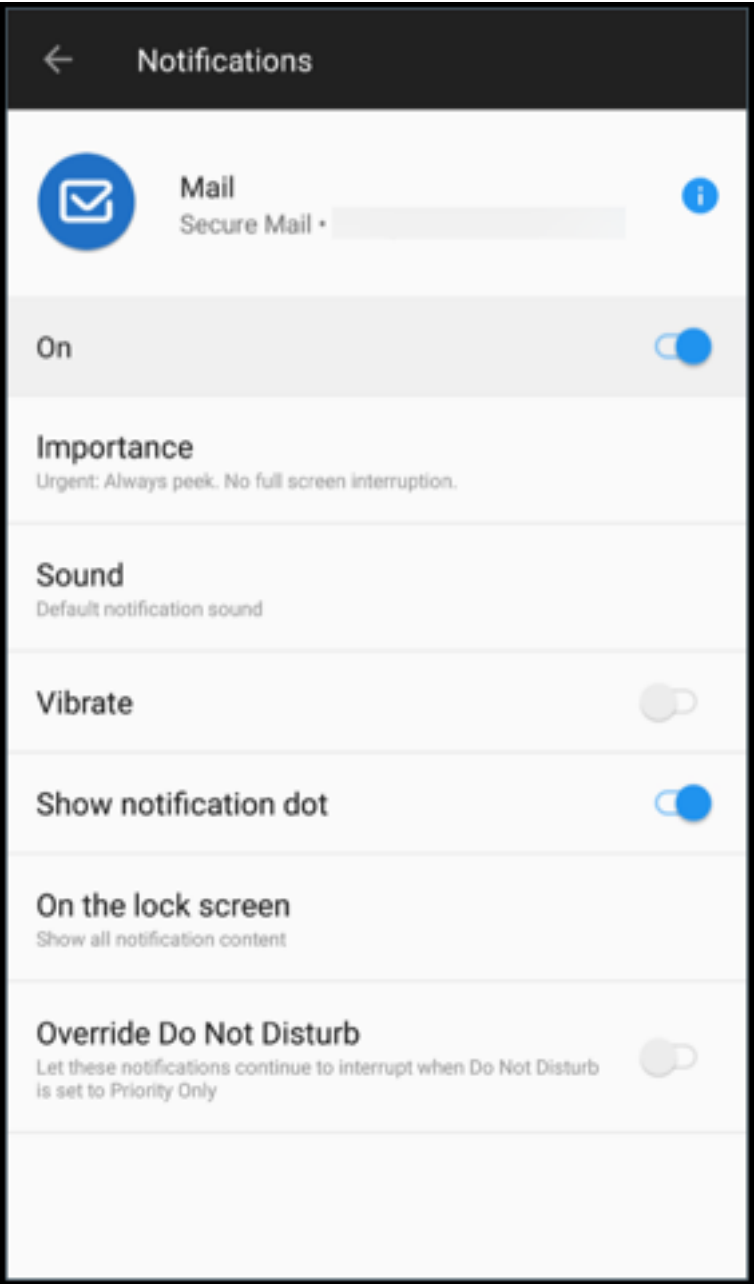
알림 채널

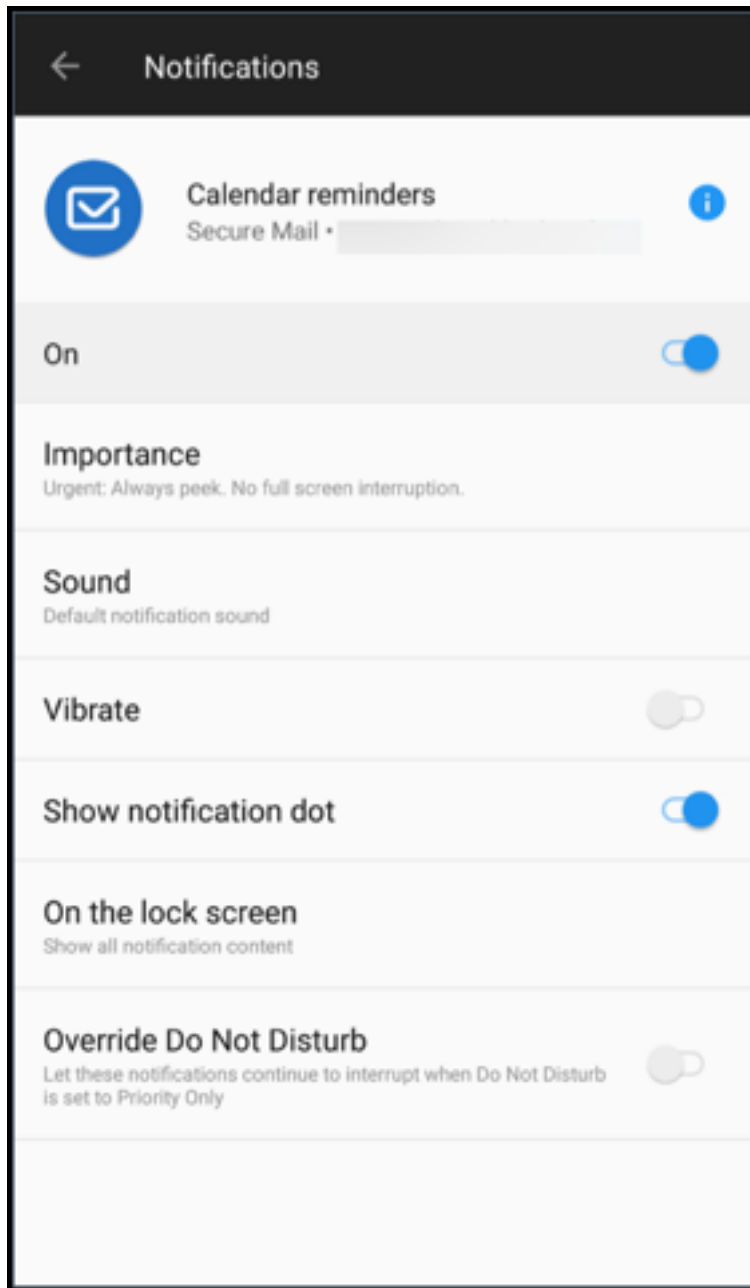
Android O 이상을 실행하는 장치에서 알림 채널 설정을 사용하여 전자 메일 및 일정 알림이 처리되는 방식을 관리할 수 있습니다. 이 기능을 통해 알림을 사용자 지정하고 관리할 수 있습니다.

메일 알림 또는 일정 미리 알림을 구성하려면 Secure Mail 을 열고 설정 > 알림으로 이동하여 원하는 알림 옵션을 선택합니다.



그런 다음 메일 알림 관리 또는 일정 알림 관리로 이동하여 각각 전자 메일 또는 일정 알림을 관리할 수 있습니다.





또는 장치의 Secure Mail 앱 아이콘을 길게 누르고 앱 정보를 선택한 다음 알림을 누릅니다.

이전에 진동 설정이 무음 시에만으로 설정된 경우, 이 기능에 대해 기본 진동 설정 (꺼짐) 으로 바뀝니다.

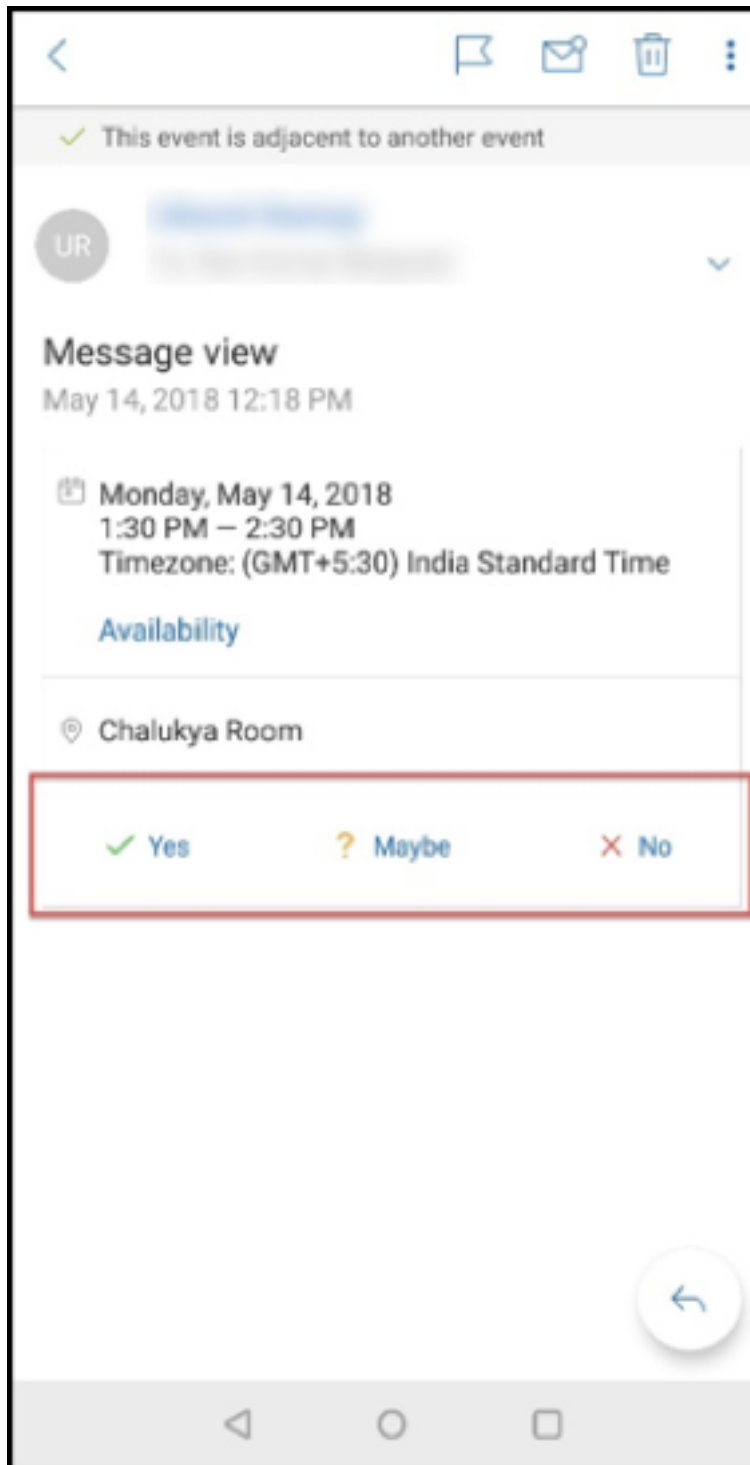
참고:

잠금 화면에서 알림을 사용할 수 있는지 여부는 관리자가 잠긴 화면 알림 제어 MDX 정책을 어떻게 구성했는지에 따라 달라 집니다.

전자 메일 내의 모임 응답 단추

Android 용 Secure Mail 에서 회의 응답 단추가 전자 메일 안에 표시됩니다. 회의 초대에 대한 전자 메일 알림을 받은 경우 다음 옵션 중 하나를 눌러 초대에 응답할 수 있습니다.

- 예
- 나중에 결정
- 아니요



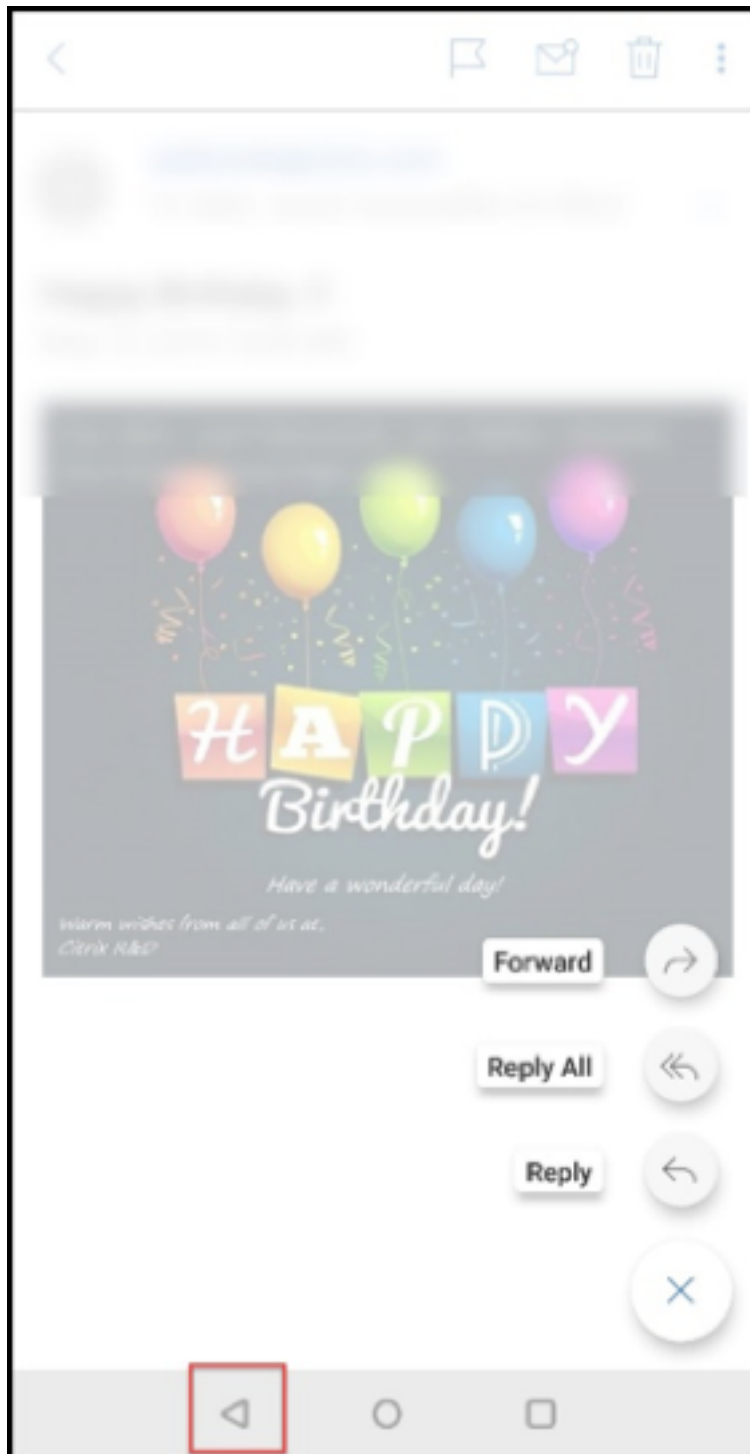
첨부 파일 기능 개선

Android 용 Secure Mail 에서는 첨부 파일을 간편하게 볼 수 있습니다. 사용자 경험을 개선하기 위해 불필요한 단계를 제거했지만 이전 릴리스의 첨부 파일 옵션은 유지했습니다.

Secure Mail 앱 내에서 첨부 파일을 볼 수 있습니다. Secure Mail 을 사용하여 볼 수 있는 첨부 파일은 직접 열립니다. Secure Mail 을 사용하여 첨부 파일을 볼 수 없는 경우 앱 목록이 나타납니다. 필요한 앱을 선택하여 첨부 파일을 볼 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [파일 보기 및 첨부](#)를 참조하십시오.

뒤로 단추 기능 개선

Android 용 Secure Mail 사용자는 장치에서 뒤로 단추를 눌러 부동 작업 단추의 확장된 옵션을 축소할 수 있습니다. 이 작업을 수행하면 메시지 또는 이벤트 세부 정보 보기로 돌아갑니다.



Android 의 갤러리에서 파일 첨부 파일을 사용하도록 설정하는 관리 단계

Secure Mail 버전 10.3.5 이상에서는 인바운드 문서 교환 (열기) 정책이 제한됨으로 설정된 경우 사용자가 갤러리 앱으로부터 바로 이미지를 첨부할 수 없습니다. 이 정책을 제한됨으로 설정해 둔 채로 사용자가 갤러리로부터 사진을 추가할 수 있게 하려면

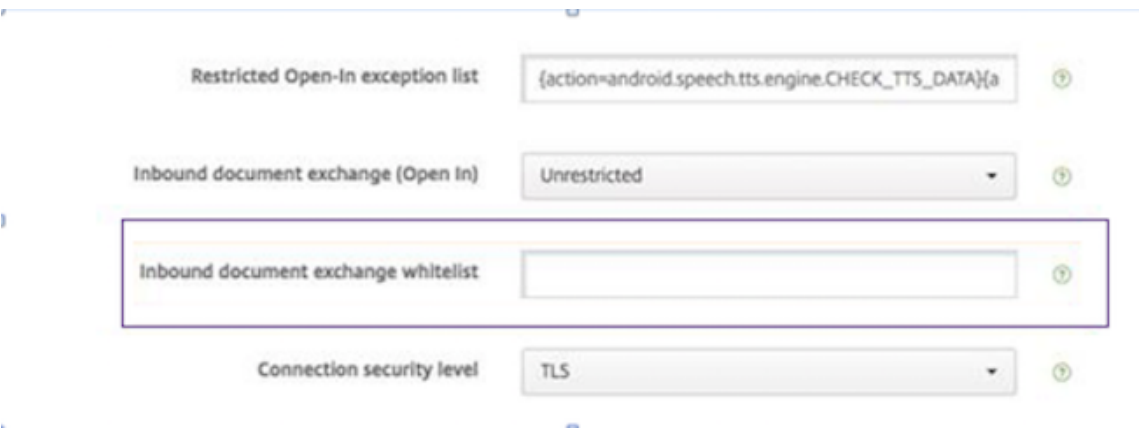
Endpoint Management 콘솔에서 다음과 같은 단계를 따르십시오.

1. 갤러리 차단을 꺼짐으로 설정합니다.
2. 장치의 Gallery 패키지 ID 를 얻습니다. 일부 예:
 - **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.photos
 - **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. 숨겨진 정책 InboundDocumentExchangeWhitelist 가 표시되도록 합니다.
 - WorxMail APK 파일을 다운로드하고 이 파일을 MDX Toolkit 으로 래핑합니다.
 - 컴퓨터에서.mdx 파일을 찾아 파일 접미사를.zip 으로 변경합니다.
 - .zip 파일을 열고 policy_metadata.xml 파일을 찾습니다.
 - InboundDocumentExchangeWhitelist 를 검색하여 `<PolicyHidden>true</PolicyHidden>`에서 `<PolicyHidden>false</PolicyHidden>`로 변경합니다.
 - policy_metadata.xml 파일을 저장합니다.
 - 해당 폴더에 있는 모든 파일을 선택하고 압축하여.zip 파일을 생성합니다.

참고:

바깥쪽 폴더를 zip 파일로 압축하지 마십시오. 폴더 내의 모든 파일을 선택하고 선택된 파일을 압축하십시오.

 - 생성된 압축 파일을 클릭합니다.
 - **Get Info**(정보 얻기) 를 선택하고 파일 접미사를 다시.mdx 로 변경합니다.
4. 수정된.mdx 파일을 Endpoint Management 콘솔로 업로드하고 이제는 표시되는 인바운드 문서 교환 화이트리스트 정책에 Gallery 패키지 ID 목록을 추가합니다.



패키지 ID 는 다음과 같이 쉼표로 구분되어야 합니다.

com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photo

5. Secure Mail 을 저장하고 배포합니다.

이제 Android 사용자는 갤러리 앱에서 이미지를 첨부할 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [파일 보기 및 첨부](#)에서 참조하십시오.

지원되는 파일 형식

X 는 Secure Mail 에서 첨부, 보기 및 열기가 가능한 파일 형식을 나타냅니다.

형식	iOS	Android
비디오: H.263 AMR NB codec_Mp4		X
비디오: H.263 AMR NB codec_3gp		X
비디오: H.264 AAC codec_3gp	X	X
비디오: H.264 AAC codec_mp4	X	X
비디오: H.264 Acclc codec_mp4	X	X
GTM recorded_wmv		X
AVI		X
WAV	X	X
MP4	X	X
3GP	X	X
Flac		X

Secure Mail

형식	iOS	Android
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(단일 페이지만)	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
DOCX	X	X
XLS	X	X
XLSM	X	X
XLSX	X	X
TXT	X	X
POT	X	X
POTX		X
HTM	X	X

Secure Mail

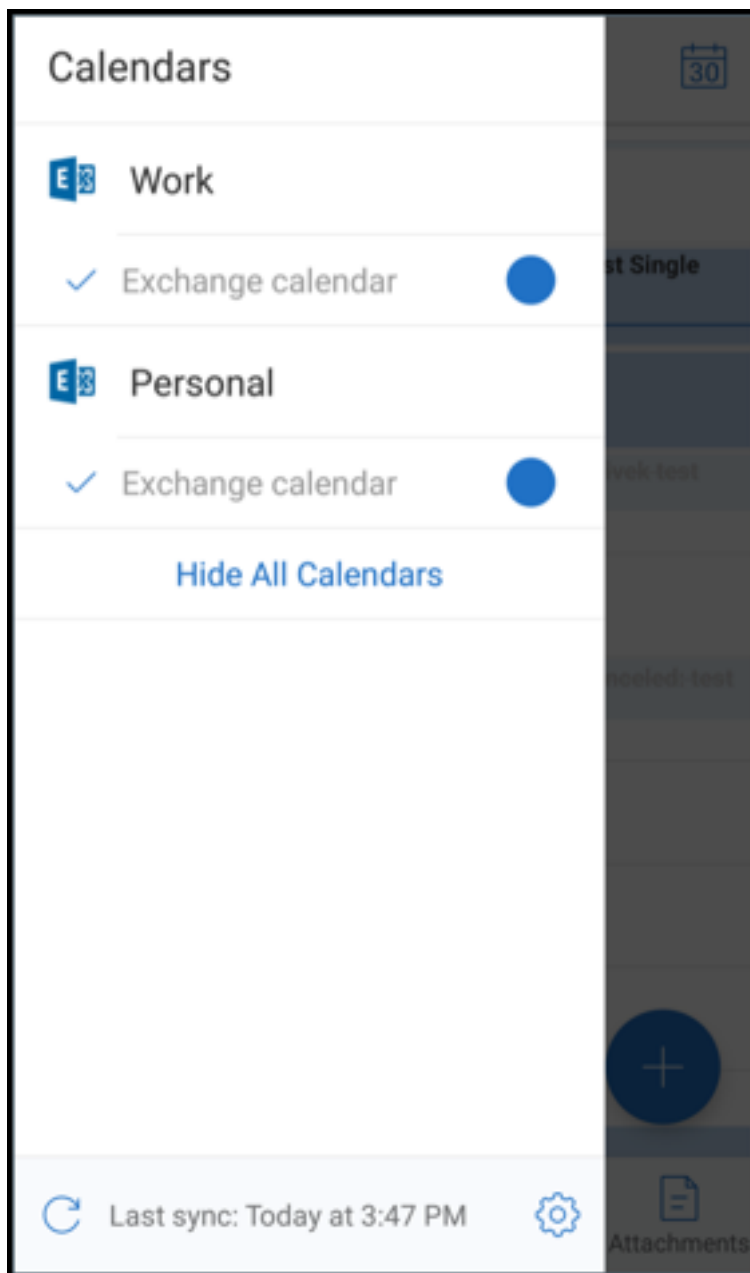
형식	iOS	Android
HTML	X	X
ZIP	X	X
EML	X	X

일정

일정에는 장치의 여러 계정과 관련된 모든 이벤트가 표시됩니다. 개별 계정에 색상을 설정하여 개별 계정과 관련된 일정 이벤트를 구분할 수 있습니다.

참고:

개인 일정 기능은 항상 주 계정 또는 기본 계정과 연결됩니다 (사용하도록 설정한 경우).



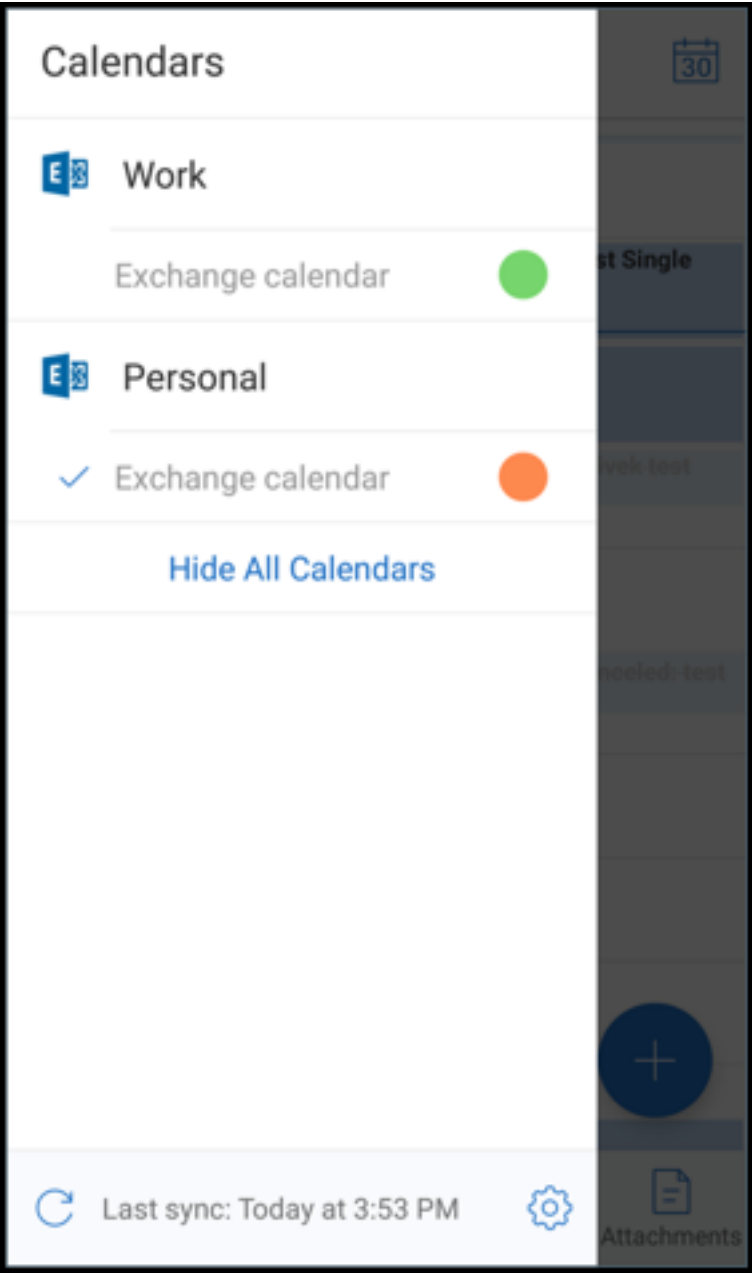
일정 이벤트에 색상을 설정하려면

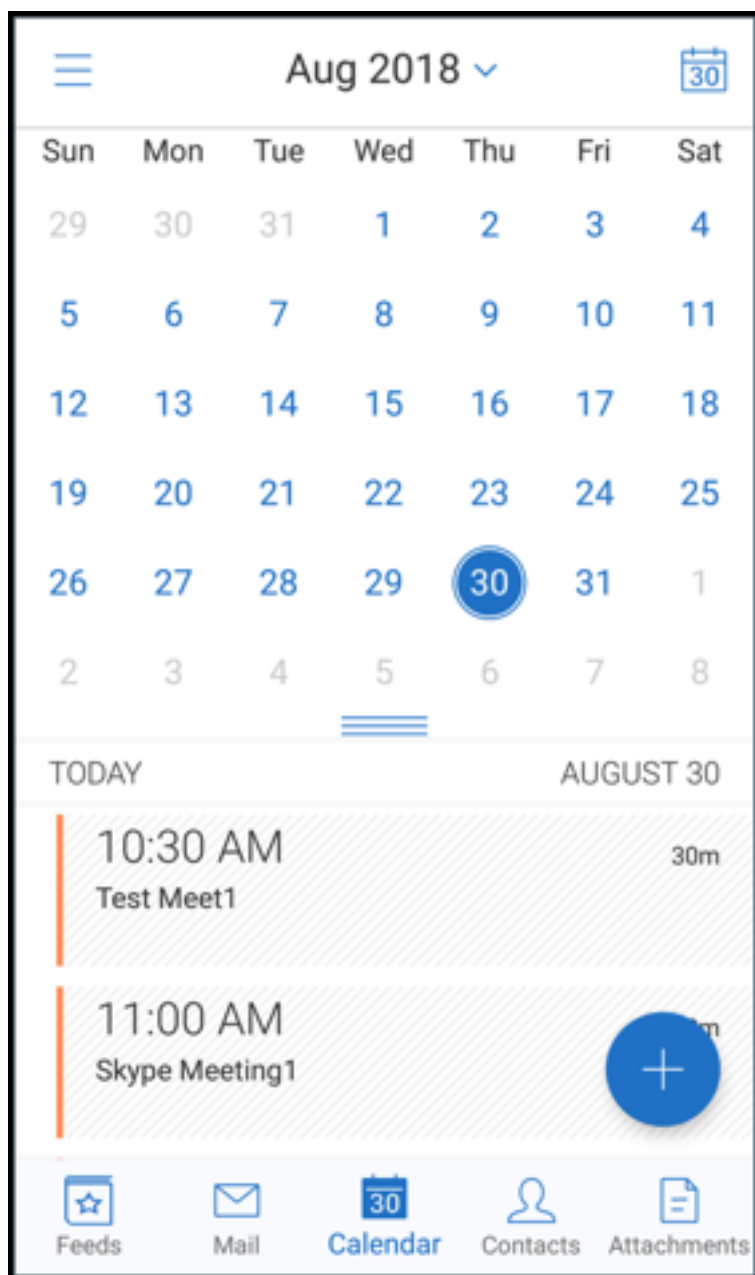
1. 바닥글 표시줄에서 일정 아이콘을 누른 다음 왼쪽 위에 있는 햄버거 아이콘을 누릅니다.
일정 화면에 구성된 모든 계정이 표시됩니다.
2. Exchange 계정의 오른쪽에 표시된 기본 색상을 누릅니다.
색상 화면에 해당 계정에 사용할 수 있는 색상이 표시됩니다.
3. 원하는 색상을 선택한 후 저장을 누릅니다.

4. 이전 화면으로 돌아가려면 취소를 누릅니다.

선택한 색상이 해당 Exchange 계정과 관련된 모든 일정 이벤트에 설정됩니다.







일정 초대 또는 이벤트를 생성하는 경우 주최자 필드에 기본 계정의 전자 메일 주소가 자동으로 입력됩니다. 메일 계정을 변경하려면 이 전자 메일 주소를 누르고 다른 계정을 선택합니다.

Cancel

New Event

Save

Organizer

Work

Title

Location

Web & Audio

None

Invitees

None

All Day

☐

Time Zone

(GMT+5:30) India Standard Time

Starts

Thu, Aug 30, 2018 4:30 PM

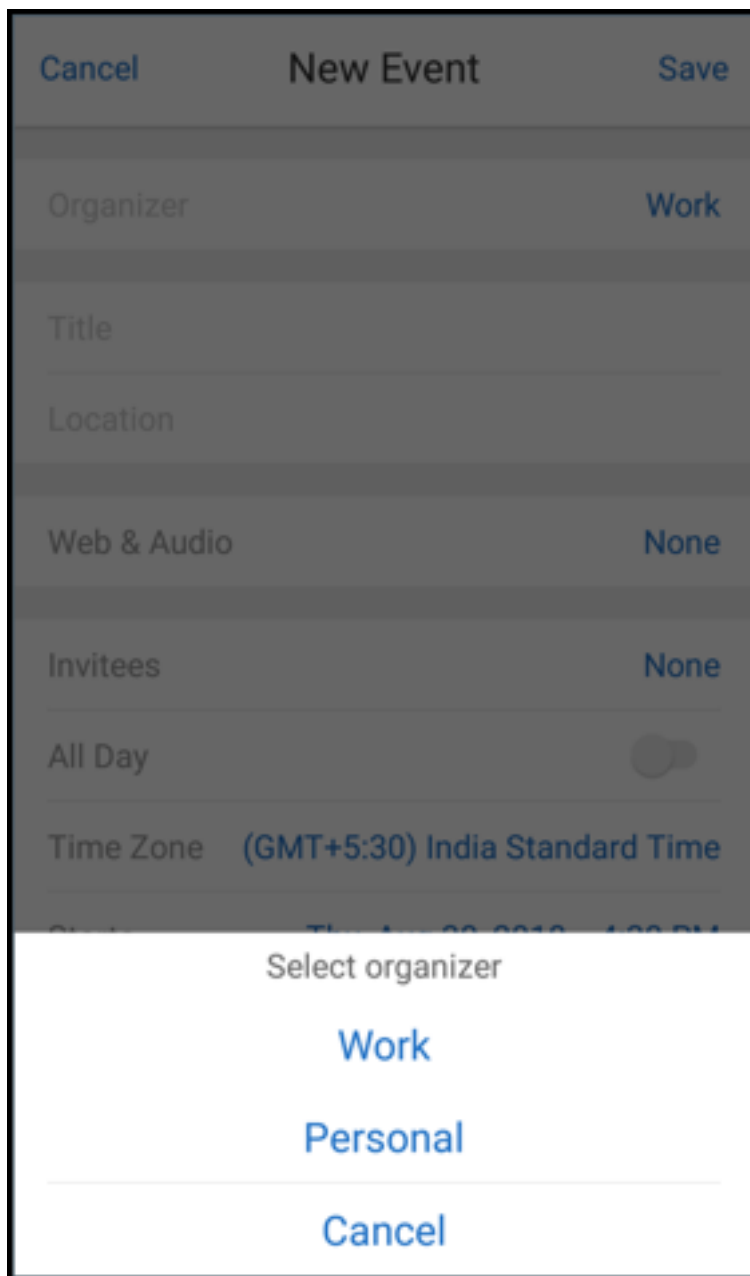
Ends

Thu, Aug 30, 2018 5:30 PM

More Options

▼

Attach from ShareFile



검색

사서함 또는 모든 연락처 보기에서 글로벌 검색을 수행할 수 있습니다. 이 동작을 수행하면 앱의 모든 계정이 검색되고 해당하는 결과가 표시됩니다.

개별 계정 내의 모든 검색에서는 해당 계정과 관련된 결과만 표시됩니다.

백그라운드 서비스에 대한 업데이트

Android 8.0(API 수준 26) 이상을 실행하는 장치에서 Google Play 백그라운드 실행 제한 요구 사항을 충족하기 위해 Secure Mail 백그라운드 서비스가 업그레이드되었습니다. 장치의 메일 동기화 및 알림을 중단 없이 사용하려면 FCM(Firebase Cloud Messaging) 서비스 푸시 알림을 사용하도록 설정합니다. FCM 기반 푸시 알림 사용에 대한 자세한 내용은 [Secure Mail 을 위한 푸시 알림](#)을 참조하십시오.

장치의 Secure Mail 설정에서 메일 알림을 켜야 합니다. 이 업데이트에 대한 자세한 내용은 이 [Support Knowledge Center 문서](#)를 참조하십시오.

제한 사항:

- FCM 기반 푸시 알림을 사용하도록 설정하지 않은 경우 백그라운드 동기화는 15 분마다 한 번씩 발생합니다. 이 간격은 앱이 백그라운드에서 실행되는지, 아니면 전경에서 실행되는지에 따라 달라집니다.
- 사용자가 장치 설정에서 시간을 수동으로 업데이트하면 일정 위젯의 날짜가 자동으로 업데이트되지 않습니다.

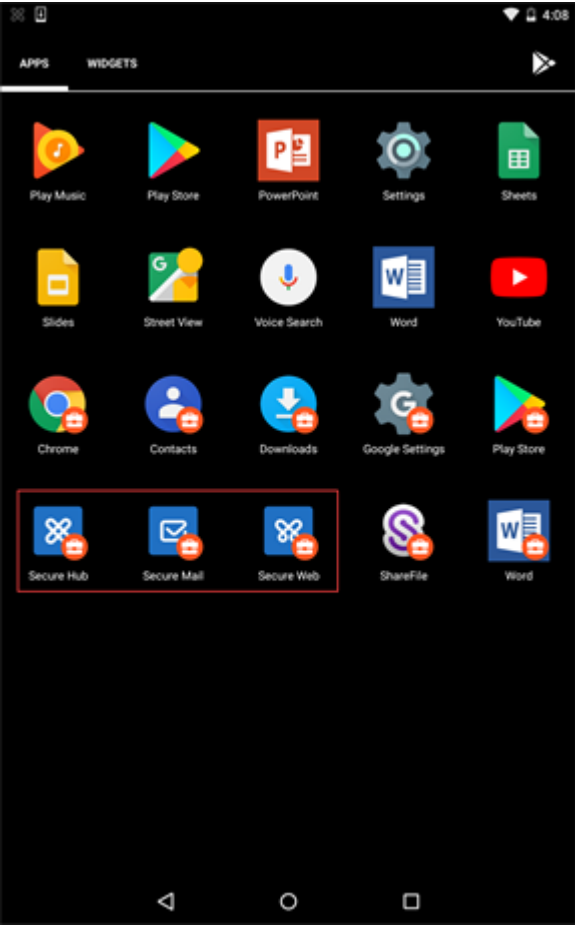
Secure Mail 의 Android Enterprise

Android 용 Secure Mail 및 Secure Web 은 Android Enterprise(이전 명칭: Android for Work) 와 호환됩니다.

사전 요구 사항

- 이 기능을 사용할 수 있으려면 장치가 Android 5.0 이상을 실행해야 합니다.
- 온-프레미스 배포인 경우 **afw.accounts** Endpoint Management 속성이 **TRUE** 로 설정되어 있어야 합니다.

Endpoint Management 에서 Android Enterprise 를 설정하면 장치에서 모바일 생산성 앱을 사용할 수 있습니다. 이러한 앱은 아래 이미지에 강조 표시된 것처럼 Android Enterprise 아이콘으로 식별됩니다.



Android Enterprise 와 호환되는 기능

다음 표에는 Android Enterprise 와 호환되는 Secure Mail 기능이 나와 있습니다.

기능	지원
Exchange Server 자동 검색	X
STA(Secure Ticket Authority)	X
연락처 내보내기	X
Microsoft 정보 권한 관리	X
잠금 화면 알림	X
메일 동기화	X
전자 메일 분류	X
S/MIME 서명 및 암호화	X

Secure Mail

기능	지원
FCM(Firebase Cloud Messaging) 서비스	X
최신 인증 (OAuth)	
여러 Exchange 계정	X
개인 일정	
메일 설정 내보내기	X
공유 장치	
Endpoint Management integration with Microsoft Intune/EMS	
Office 365	X
LDAP Exchange Server 2010, 2013 및 2016	X
CBA(인증서 기반 인증)	
GoToMeeting	X
Skype for Business	
개인 배포 목록	X
Citrix Files 호환성	X
Single Sign-on 과 함께 전자 메일 등록	X

아래 표에는 Android Enterprise 와 호환되는 Secure Web 기능이 나와 있습니다.

기능	지원
터널링됨—웹 SSO 모드	X
전체 VPN 모드	X
모든 앱 기능	X
Secure Mail 와의 호환성	X

제한 사항

- 작업 프로필 모드에서 Android Enterprise 에 대해 **Allow use of the status bar**(상태 표시줄 사용 허용) 장치 제한 정책이 커짐으로 설정되어 있으며 Android 용 Secure Mail 의 일정 내보내기 진행률 및 푸시 알림이 상태 표시줄에 나타나지 않습니다. 하지만 이러한 알림이 허용된 경우 잠금 화면에 표시됩니다. 자세한 내용은 [Android Enterprise 설정](#)을 참조하십시오.

Secure Mail 의 iOS 및 Android 기능

June 14, 2022

이 문서에서는 Secure Mail 에서 지원되는 iOS 및 Android 기능에 대해 설명합니다.

Azure 정부 클라우드 컴퓨팅 지원

Secure Mail 은 Azure Active Directory 테넌트에서 최신 인증 (OAuth) 을 위한 Government Cloud Computing(GCC) High 를 지원합니다. Secure Mail 은 모든 GCC High 서비스에 대한 Microsoft 의 필수 요구 사항을 충족하기 위해 GCC High 에 엔드포인트로 등록됩니다. 자세한 내용은 [Microsoft 365 Government 의 Azure Active Directory 에 대한 새로운 소식](#)을 참조하십시오.

이번 변경을 통해 인증용 Azure Active Directory 테넌트에서 GCC High 로 라우팅됩니다. 또한 관리자는 Azure Active Directory 테넌트에서 Secure Mail 에 대한 권한을 허용해야 합니다.

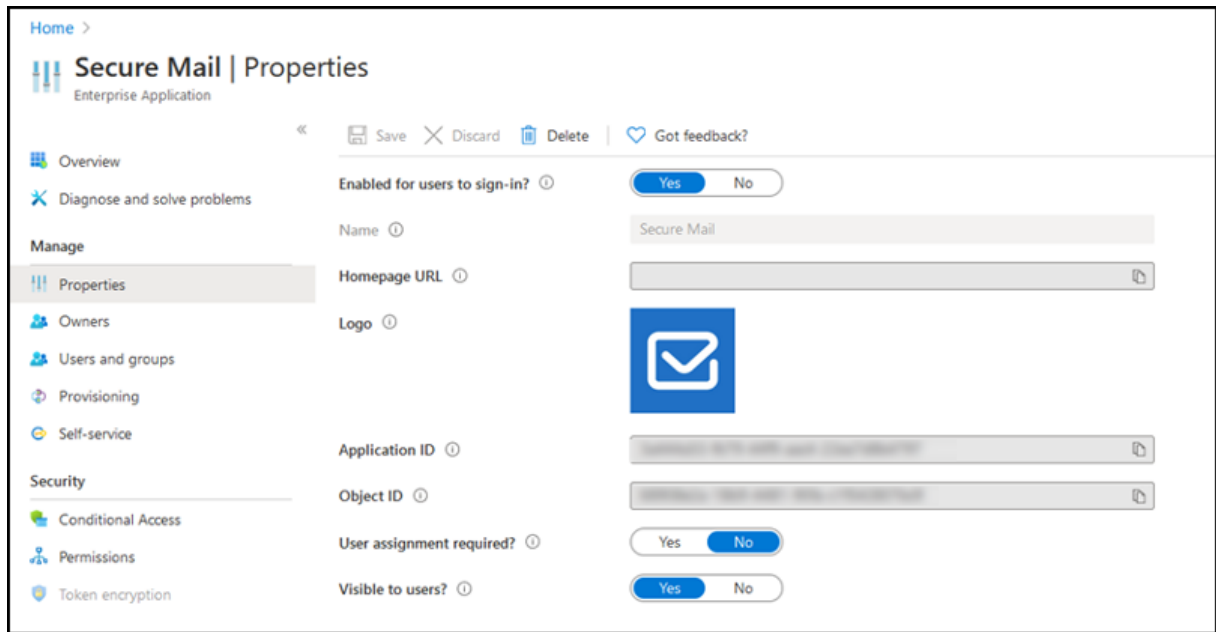
사전 요구 사항

Azure Active Directory 의 전역 관리자가 다음을 수행하는지 확인합니다.

- 장치에 최신 버전의 Secure Mail 을 다운로드합니다.
- Secure Mail 앱에서 Exchange 계정을 구성하고 모든 사용자가 로그인할 수 있도록 Azure Active Directory 의 앱 권한을 허용합니다. 다음 화면을 참조하십시오.

참고:

이러한 단계는 일회성 요구 사항으로 전역 관리자에게만 해당됩니다. 앱에 액세스 권한이 부여되면 App Store 에서 간단하게 업그레이드할 수 있습니다.



업그레이드 후

업그레이드하고 나면 새로 고침 토큰이 만료된 후 다시 인증할 것인지를 묻는 메시지가 나타나며, Azure AD의 GCC High로 리디렉션됩니다. 권한 부여 요청이 Azure AD의 GCC High로 전송되도록 하려면 이전 워크플로의 유효성을 검사합니다.

다음 방법 중 하나를 사용하여 워크플로를 검증할 수 있습니다.

- 앱 이름 **Secure Mail-GCC High**가 포함된 Secure Mail이 Azure Active Directory 테넌트의 로그인 페이지에 나타납니다.
- Secure Mail 로그를 확인하여 재인증 후 <https://login.microsoftonline.us>를 통해 리디렉션이 수행되는지 확인합니다.

ICS 파일 지원

Secure Mail에서 첨부 파일로 받은 ICS 파일을 미리 보고 이벤트로 일정에 가져올 수 있습니다.

Secure Mail의 연락처 사진

Secure Mail에서 전자 메일 또는 모임 초대에 받는 사람을 추가할 때 연락처 사진을 볼 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [연락처의 사진 표시](#)를 참조하십시오.

피드 관리

이제 Secure Mail 에서 필요에 따라 피드 카드를 구성할 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [전자 메일 구성](#)을 참조하십시오.

Office 365 Exchange Server 정책을 사용하여 Office 365 서버 주소 정의

Secure Mail 에서 OAuth 의 Office 365 지원 섹션 아래에 **Office 365 Exchange Server** 라는 이름의 새 정책이 추가되었습니다. 이 정책을 사용하면 클라우드에 있는 Office 365 사서함의 호스트 이름을 정의할 수 있습니다. 이 정책을 사용하면 정부 기관에 대한 Office 365 도 지원할 수 있습니다. 호스트 이름은 *outlook.office365.com* 과 같은 단일 값입니다. 기본값은 *outlook.office365.com* 입니다.

암호화 관리 지원

암호화 관리를 사용하면 최신 장치 플랫폼 보안을 사용하는 동시에 플랫폼 보안을 효과적으로 사용하기에 충분한 상태를 유지할 수 있습니다. 암호화 관리를 사용하면 iOS 또는 Android 플랫폼에서 파일 시스템 암호화가 제공되므로 로컬 데이터 암호화 중복을 제거할 수 있습니다. 이 기능을 사용하려면 관리자가 Citrix Endpoint Management 콘솔에서 암호화 유형 MDX 정책을 규정 준수를 적용하여 플랫폼 암호화로 구성해야 합니다.

암호화 관리 기능을 사용하려면 Citrix Endpoint Management 콘솔에서 암호화 유형 정책을 규정 준수를 적용하여 플랫폼 암호화로 설정합니다. 이렇게 하면 암호화 관리와 사용자 장치에 있는 기존의 모든 암호화된 응용 프로그램 데이터가 MDX 가 아닌 장치로 암호화된 상태로 원활하게 전환됩니다. 이 전환 중에 일회성 데이터 마이그레이션을 위해 앱이 일시 중지됩니다. 마이그레이션이 성공하면 로컬로 저장된 데이터의 암호화에 대한 책임이 MDX 에서 장치 플랫폼으로 이전됩니다. MDX 는 앱을 시작할 때마다 장치의 규정 준수를 계속 확인합니다. 이 기능은 MDM + MAM 및 MAM 전용 환경 모두에서 작동합니다.

암호화 유형 정책을 규정 준수를 적용하여 플랫폼 암호화로 설정하면 새 정책이 기존 MDX 암호화를 대체합니다.

Secure Mail 에 대한 암호화 관리 MDX 정책에 대한 자세한 내용은 다음 위치에서 암호화 섹션을 참조하십시오.

- [Android 용 모바일 생산성 앱의 MDX 정책](#)
- [iOS 용 모바일 생산성 앱의 MDX 정책](#)

장치가 최소 규정 준수 요구 사항을 충족하지 못하는 경우 규정을 준수하지 않는 장치 동작 정책을 사용하여 수행할 작업을 선택할 수 있습니다.

- 앱 허용 - 앱의 정상적인 실행을 허용합니다.
- 경고 후 앱 허용 - 앱이 최소 규정 준수 요구 사항을 충족하지 않는다는 내용의 경고를 사용자에게 표시하고 앱의 실행을 허용합니다. 기본값입니다.
- 앱 차단 - 앱 실행을 차단합니다.

iOS 를 실행하는 장치

장치가 iOS 를 실행하는 장치에 대한 최소 규정 준수 요구 사항을 충족하는지 여부는 다음 기준에 따라 결정됩니다.

- iOS 10 - 앱이 지정된 버전 이상의 운영 체제 버전을 실행하고 있습니다.
- 디버거 액세스 - 앱에 디버깅이 활성화되어 있지 않습니다.
- 탈옥된 장치 - 앱이 탈옥 장치에서 실행되고 있지 않습니다.
- 장치 암호 - 장치 암호가 켜져 있습니다.
- 데이터 공유 - 앱에 대해 데이터 공유가 활성화되지 않았습니다.

Android 를 실행하는 장치

장치가 Android 를 실행하는 장치에 대한 최소 규정 준수 요구 사항을 충족하는지 여부는 다음 기준에 따라 결정됩니다.

- Android SDK 24(Android 7 Nougat) - 앱이 지정된 버전 이상의 운영 체제 버전을 실행하고 있습니다.
- 디버거 액세스 - 앱에 디버깅이 활성화되어 있지 않습니다.
- 루팅 장치 - 앱이 루팅된 장치에서 실행되고 있지 않습니다.
- 장치 잠금 - 장치 암호가 켜져 있습니다.
- 장치 암호화 - 앱이 암호화된 장치에서 실행 중입니다.

반응형 전자 메일 지원

Secure Mail 이 반응형 전자 메일을 제공하도록 최적화되었습니다. 이전에는 큰 테이블이나 이미지가 포함된 전자 메일 내용이 잘못 렌더링되었습니다. 이 기능은 전자 메일의 형식과 크기에 관계없이 지원되는 모든 장치에서 전자 메일 내용을 더 쉽게 읽을 수 있도록 합니다.

일정 이벤트 끌어서 놓기

Secure Mail 에서 이벤트를 끌어서 놓는 방법으로 기존 일정 이벤트의 시간을 변경할 수 있습니다. 이 일정 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [일정 이벤트 시간 변경](#)을 참조하십시오.

피드 관리

이제 Secure Mail 에서 필요에 따라 피드 카드를 구성할 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [전자 메일 구성](#)을 참조하십시오.

자동 진행

Secure Mail 에서 **Conversations(대화)**의 메시지를 삭제할 때 돌아갈 메시지를 선택할 수 있습니다. 이 기능을 사용하려면 **Settings(설정) > Auto Advance(자동 진행)**로 이동합니다. 그런 다음 사용 가능한 선택 항목에서 기본 설정을 선택합니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [대화에서 전자 메일 삭제 및 자동 진행](#)을 참조하십시오.

임시 보관함 폴더 자동 동기화

임시 보관함 폴더가 자동으로 동기화되고 모든 장치에서 임시 보관함을 사용할 수 있습니다. 이 기능은 Office 365 또는 Exchange Server 2016 이상을 실행하는 장치에서 사용할 수 있습니다.

메모:

Secure Mail 임시 보관함에 첨부 파일이 포함된 경우 첨부 파일은 서버로 동기화되지 않습니다.

비디오를 포함하여 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [임시 보관함 폴더 자동 동기화](#)를 참조하십시오.

MDM + MAM 모드에서 Microsoft Intune 을 사용할 때 Single Sign-on 지원

iOS 를 실행하는 장치:

이 기능을 사용하려면 장치에 Microsoft Authenticator 앱이 설치되어 있어야 합니다. Microsoft Authenticator 앱 설치에 대한 자세한 내용은 Docs.microsoft.com 에서 **Microsoft Authenticator** 앱 다운로드 및 설치를 참조하십시오.

Android 를 실행하는 장치:

이 기능을 사용하려면 장치에 Intune Company Portal 앱이 설치되어 있어야 합니다. Intune Company Portal 앱에 로그인한 후에는 Secure Mail 에서 자격 증명을 사용하여 재인증하지 않고도 MDM + MAM 모드에서 SSO 를 사용할 수 있습니다.

연락처 기능 개선

Secure Mail 에서 연락처를 누르고 연락처를 선택하면 해당 연락처의 세부 정보가 연락처 탭에 나타납니다. 조직 탭을 누르면 관리자, 직속 부하 및 동료 같은 조직 계층 세부 정보가 나타납니다. 화면 오른쪽의 자세히 아이콘을 누르면 다음 옵션이 나타납니다.

- 편집
- VIP 에 추가
- 취소

조직 탭에서 관리자, 직속 부하 또는 동료 오른쪽의 자세히 아이콘을 누를 수 있습니다. 이 작업을 수행하여 전자 메일 또는 일정 이벤트를 만들 수 있습니다. 전자 메일 또는

일정 이벤트의 받는 사람: 필드에는 관리자, 직속 부하 또는 동료의 세부 정보가 자동으로 입력됩니다. 전자 메일을 작성하고 보낼 수 있습니다.

사전 요구 사항

Exchange Server 에서 EWS(Exchange 웹 서비스) 가 사용되도록 설정되었는지 확인합니다.

연락처 세부 정보는 Active Directory 에서 가져온 조직 세부 정보 (Outlook 연락처) 를 기반으로 나타냅니다. 연락처에 대한 정확한 세부 정보를 표시하려면 관리자가 Active Directory 에서 조직 계층을 구성했는지 확인합니다.

참고:

이 기능은 IBM Lotus Notes 서버에서 지원되지 않습니다.

모임 시간 및 위치를 기본 일정으로 내보내기

Secure Mail 에서 모임 시간, 위치라는 새로운 값이 일정 내보내기 MDX 정책에 추가되었습니다. 이 개선을 통해 Secure Mail 일정 이벤트의 모임 시간 및 위치를 기본 일정으로 내보낼 수 있습니다.

여러 Exchange 계정

Secure Mail 내의 설정에서 여러 Exchange 전자 메일 계정을 추가하고 계정을 전환할 수 있습니다. 이 기능을 사용하면 모든 메일, 연락처 및 일정을 한 위치에서 모니터링할 수 있습니다. 관리 필수 구성 요소는 다음과 같습니다.

- 추가 계정을 구성하려면 사용자 이름과 암호가 필요합니다. 자동 등록 또는 자격 증명 저장소 구성은 앱의 첫 번째 계정 설정에만 적용됩니다. 모든 추가 계정에 대한 사용자 이름과 암호를 입력합니다.
- 처음 생성한 계정이 인증서 기반인 경우 추가 인증서 기반 계정을 추가할 수 없습니다. 추가 계정은 Active Directory 기반 인증을 사용해야 합니다. Secure Mail 은 여러 계정을 구성하는 경우 인증서 기반 인증을 지원하지 않습니다.
- 추가 계정에서 외부 네트워크의 도메인 또는 Exchange Server 에 연결할 수 있도록 하려면 Citrix ADC 에서 분할 터널링을 커집으로 설정해야 합니다.
- iOS 용 Secure Mail 은 Exchange 와 Office 365 메일 서버만 지원합니다.

이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [Exchange 계정 추가](#)를 참조하십시오.

연락처

연락처에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [연락처 보기 및 동기화](#)를 참조하십시오.

일정에서 색상 설정

이 일정 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [동기화된 Secure Mail 일정에 색상 설정](#)을 참조하십시오.

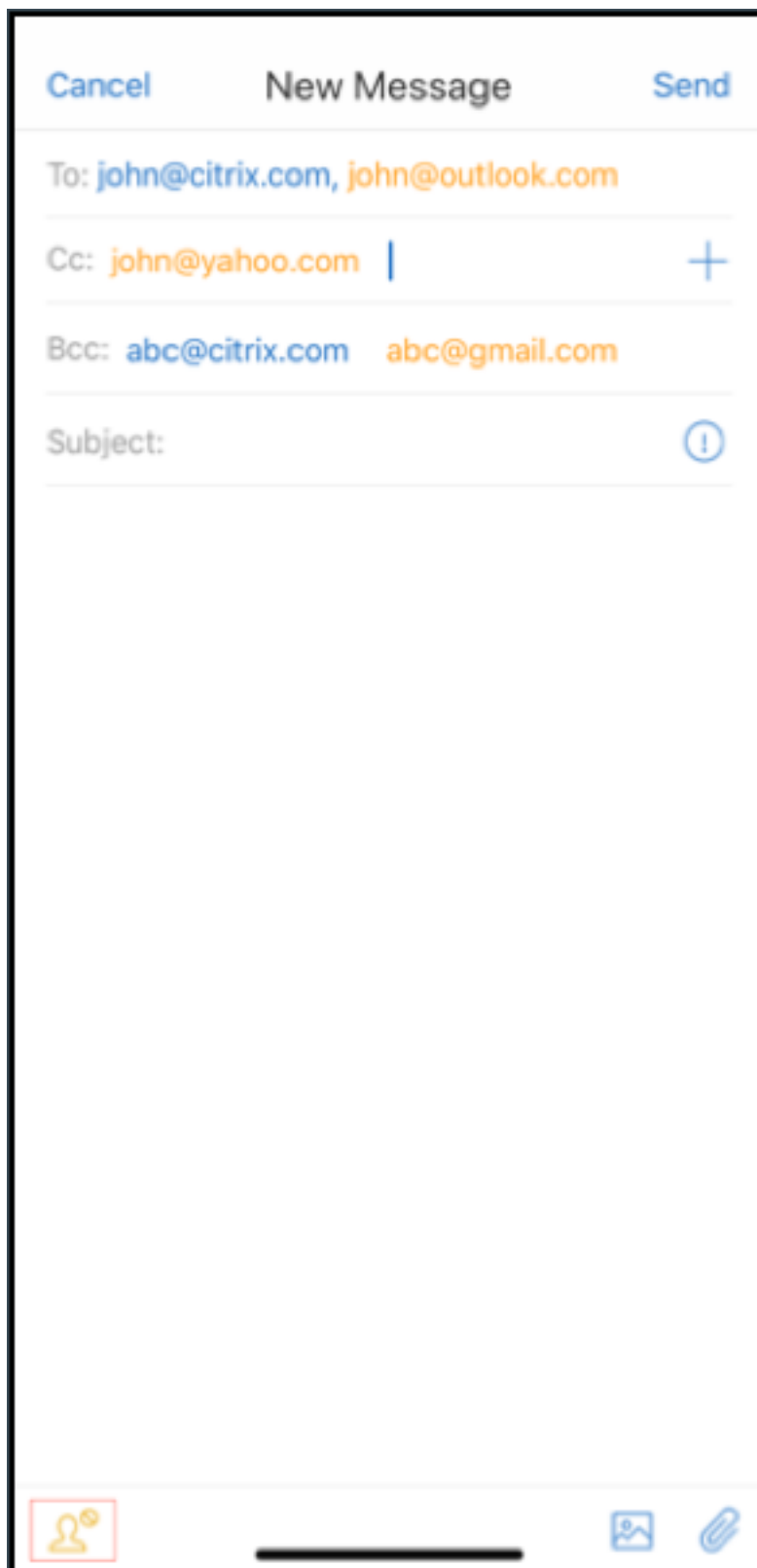
내부 도메인

외부 조직에 속한 메일 받는 사람을 식별하고 편집할 수 있습니다.

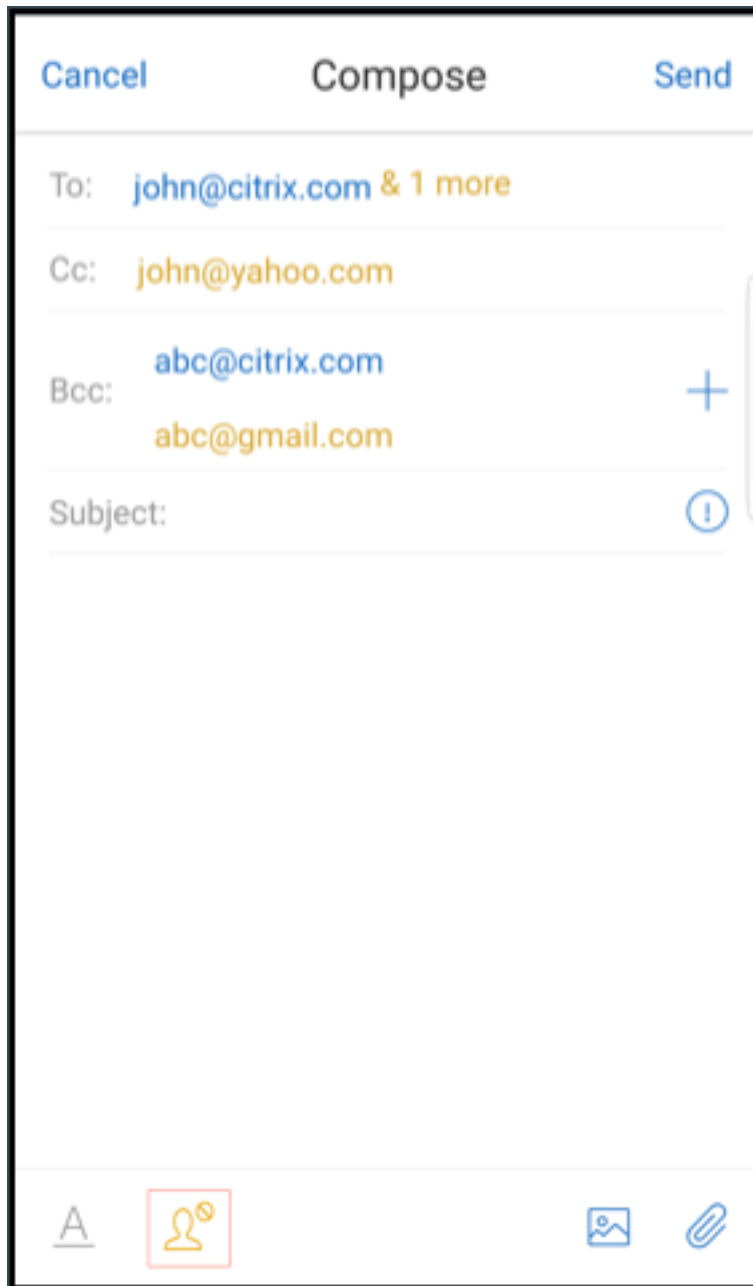
필수 구성 요소: Citrix Endpoint Management 에서 내부 도메인 정책을 사용하도록 설정하고 응용 프로그램을 다시 시작했는지 확인합니다.

전자 메일을 작성하거나, 회신하거나, 전달할 때 외부 받는 사람이 메일 그룹에서 강조 표시됩니다. 연락처 아이콘이 화면 왼쪽 아래에 경고로 나타납니다. 연락처 아이콘을 눌러 메일 그룹을 수정합니다.

iOS 를 실행하는 장치:

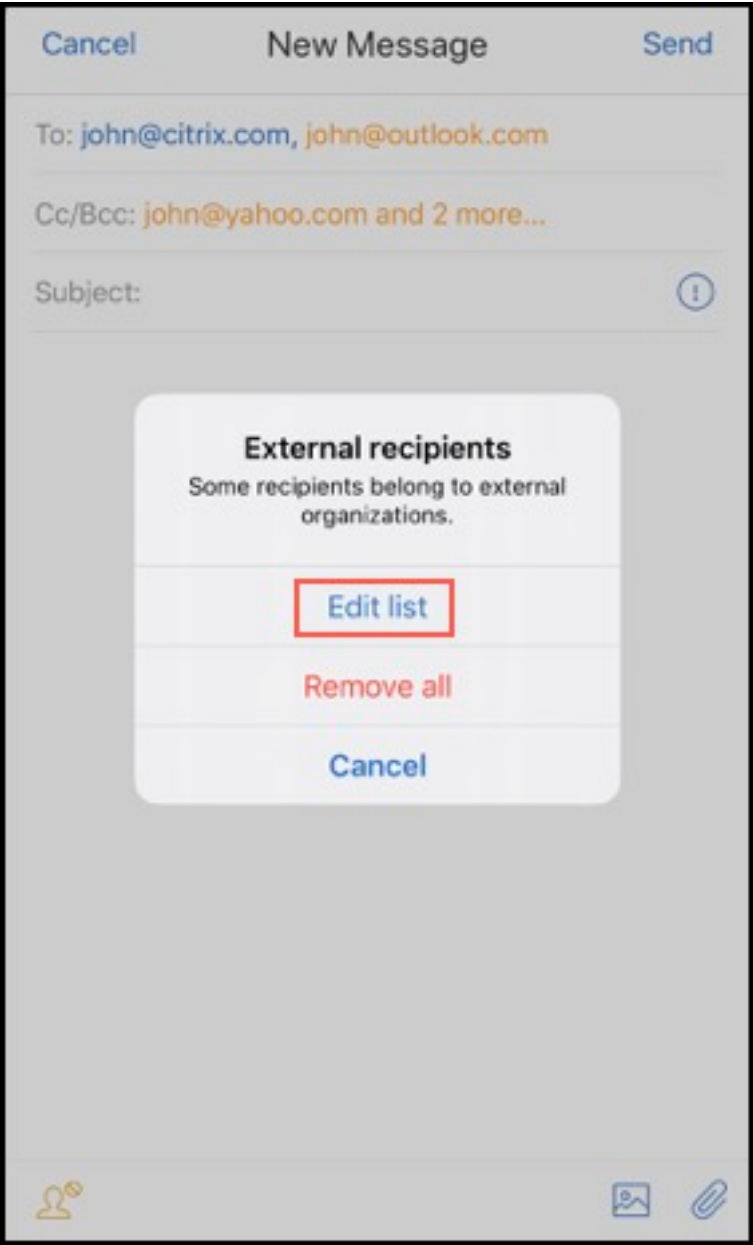


Android 를 실행하는 장치:



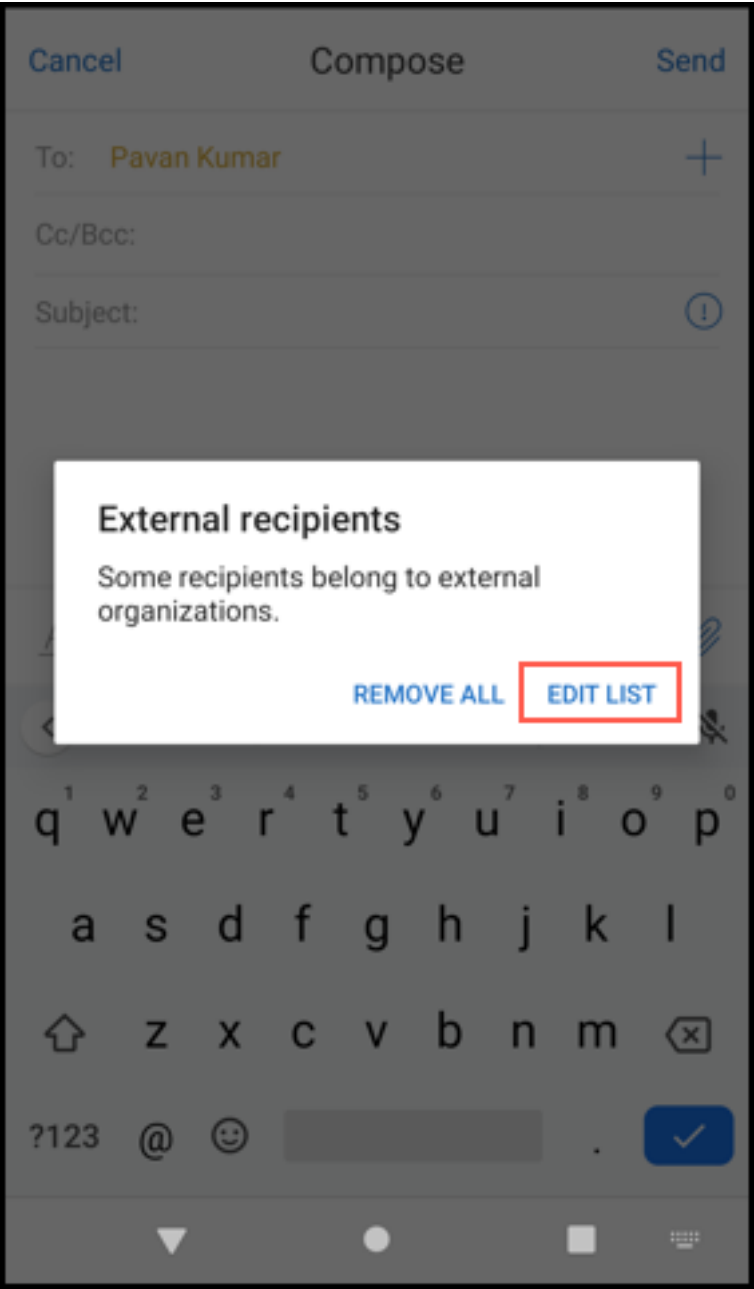
연락처 아이콘을 누르면 목록을 편집하거나 모두 제거할 수 있는 옵션이 있는 팝업 창이 나타납니다. 목록 편집을 눌러 제거할 받는 사람을 선택합니다. 받는 사람을 선택한 후 휴지통 아이콘을 누릅니다.

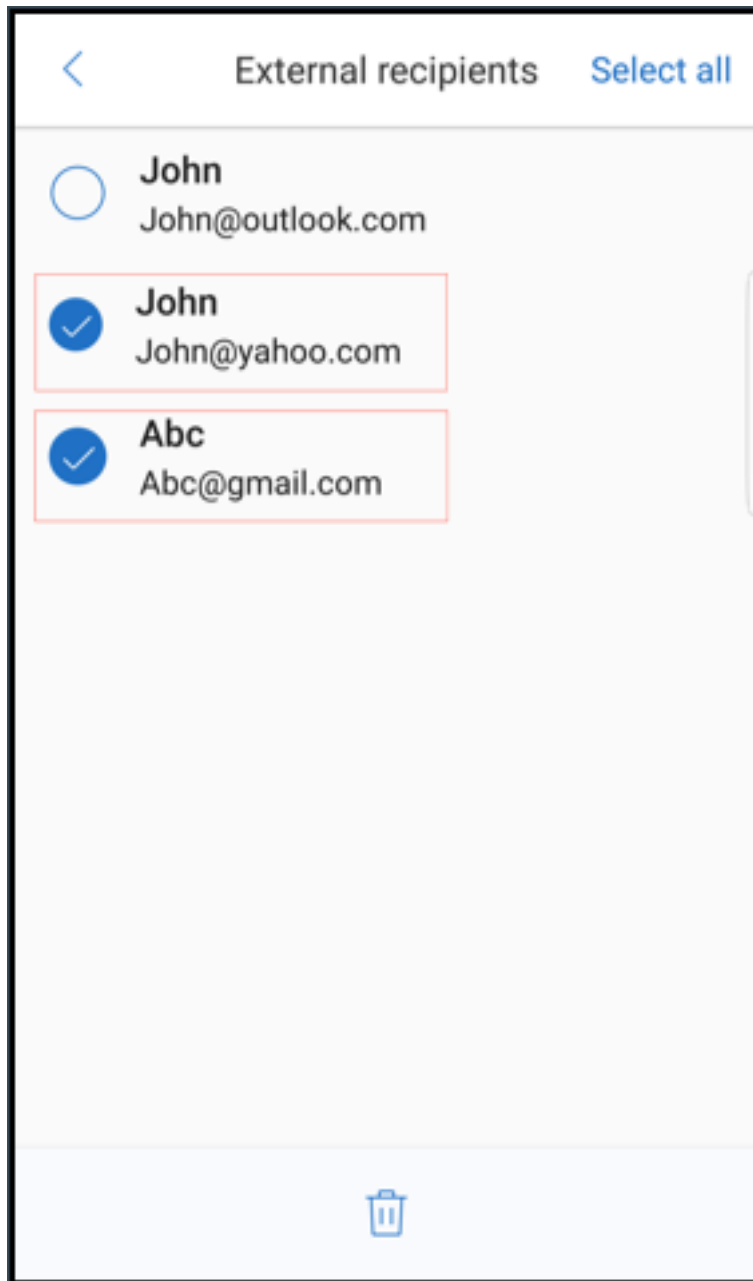
iOS 를 실행하는 장치:





Android 를 실행하는 장치:





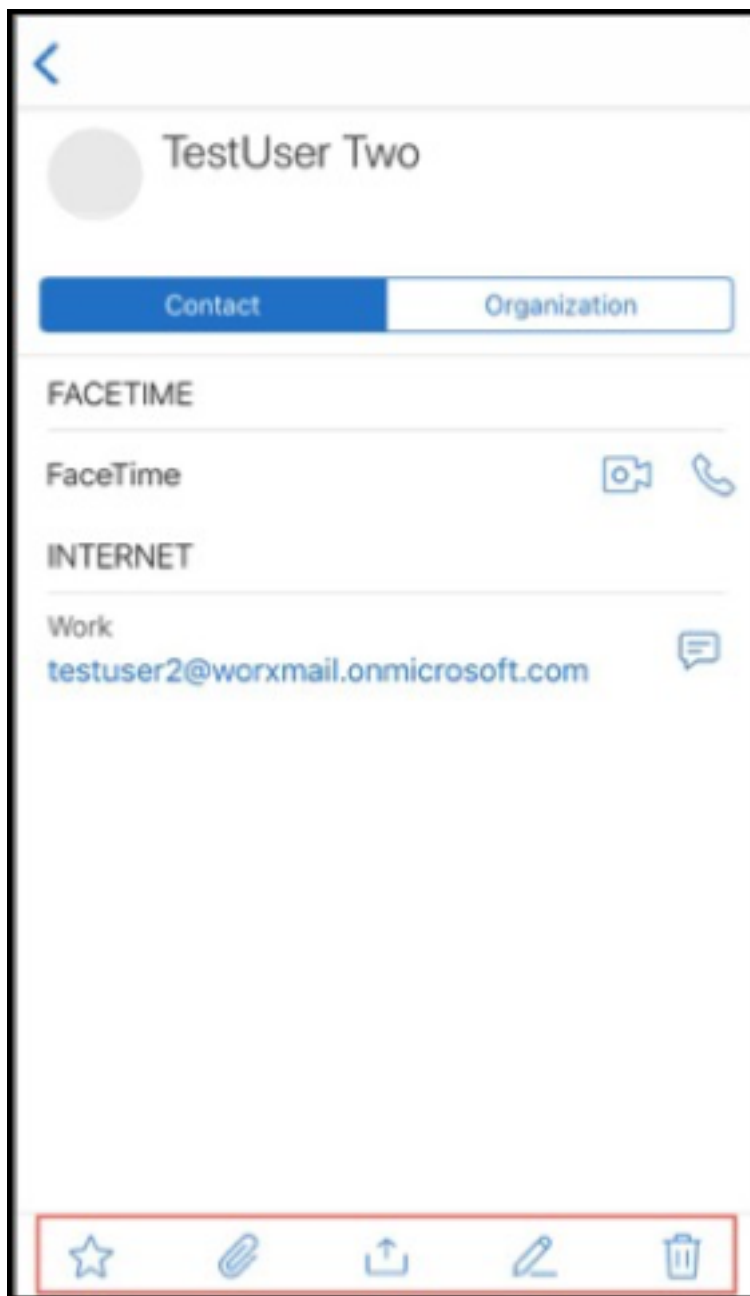
인체공학적 개선 사항

이 개선 사항에 따라 작업 단추가 화면 상단에서 하단으로 이동되어 쉽게 액세스할 수 있게 되었습니다. 이러한 변경 사항은 받은 편지함, 일정 및 연락처 화면에 적용됩니다.

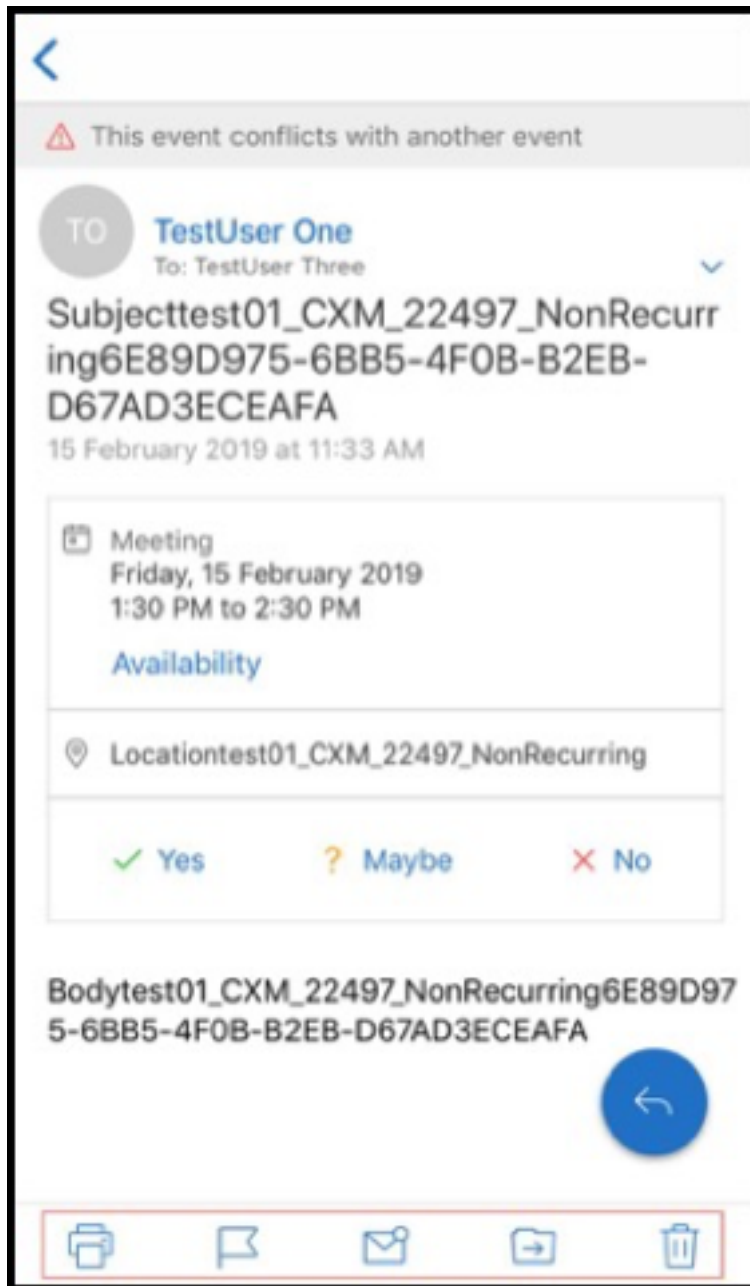
메모:

Android 의 경우 받은 편지함 및 일정 화면이 변경됩니다.

iOS 를 실행하는 장치



Android 를 실행하는 장치



응답 부동 작업 단추가 Citrix 브랜딩 및 스타일 가이드에 맞게 개선되었습니다.

또한 이 개선 사항으로 인해 열려 있는 전자 메일에서 기본 받은 편지함 화면의 단추에 액세스하는 옵션이 제거되었습니다. 피드, 일정, 연락처, 첨부 파일 같은 항목에 액세스하려면 열려 있는 전자 메일에서 나가야 합니다.

iOS의 바닥글 표시줄에 있는 옵션이 변경되어 iOS와 Android 간에 일관성이 개선되었습니다.

Secure Mail 과 Slack 통합 (미리 보기)

이제 iOS 또는 Android 를 실행하는 장치에서 전자 메일 대화를 Slack 앱으로 보낼 수 있습니다. 자세한 내용은 [Secure Mail 과 Slack 통합 \(미리 보기\)](#)을 참조하십시오.

피싱 전자 메일 보고 (전달을 통해)

Secure Mail 에서 피싱 메일 신고 기능을 통해 피싱으로 의심되는 전자 메일을 전달하여 보고할 수 있습니다. 관리자가 정책에 서 구성한 전자 메일 주소로 의심스러운 메시지를 전달하면 됩니다. 이 기능을 사용하려면 관리자가 피싱 보고 전자 메일 주소 정책을 구성하고 피싱 보고 메커니즘을 전달을 통해 보고로 설정해야 합니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [피싱 전자 메일 보고](#)를 참조하십시오.

Report a phishing email(피싱 전자 메일 보고)

관리자가 구성하는 정책에 따라 피싱 전자 메일을 보고할 수 있습니다. 관리 설정에 대한 세부 정보를 포함하여 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [피싱 전자 메일 보고](#)를 참조하십시오.

Secure Mail 일정 이벤트 내보내기

iOS 및 Android 용 Secure Mail 을 사용하여 Secure Mail 일정 이벤트를 장치의 기본 일정 앱으로 내보낼 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [Secure Mail 일정 이벤트 내보내기](#)를 참조하십시오.

개인 일정에 표시되는 일정 이벤트 필드에 다음 MDX 정책 값을 사용할 수 있습니다.

- 없음 (내보내지 않음)
- 모임 시간
- 모임 시간, 위치
- 모임 시간, 주제, 위치
- **(Android)** 모임 시간, 상태, 참석자, 주제, 위치, 메모
- **(iOS)** 모임 시간, 주제, 위치, 메모

Android 옵션:

Endpoint Management Analyze Manage **Configure**

Device Policies Apps Media Actions ShareFile Enrollment Profiles Delivery Groups

MDX

1 App Information

2 Platform Clear All

☒ iOS

☒ Android

☒ Windows Phone

☒ Windows Desktop/Tablet

3 Approvals (optional)

4 Delivery Group Assignments (optional)

Report Phishing Mail Addresses

Report Phishing Mechanism Report via Attachment

Skype For Business Meeting Domains

Export Calendar Meeting Time

OAuth Support for Office 365

Use Modern authentication for O365

Trusted Exchange Online Hostnames

Meeting Time

None (Don't Export)

Meeting Time, Location

Meeting Time, Subject, Location

Meeting Time, Availability, Attendees, Subject, Location

ios 옵션:

Endpoint Management Analyze Manage **Configure**

Device Policies Apps Media Actions ShareFile Enrollment Profiles Delivery Groups

MDX

1 App Information

2 Platform Clear All

☒ iOS

☒ Android

☒ Windows Phone

☒ Windows Desktop/Tablet

3 Approvals (optional)

4 Delivery Group Assignments (optional)

Report Phishing Mail Addresses

Report Phishing Mechanism Report via Attachment

Skype For Business Meeting Domains

Export Calendar Meeting Time

Caller Identification

OAuth Support for Office 365

Office 365 authentication mechanism Do not use OAuth

Meeting Time

None (Don't Export)

Meeting Time, Location

Meeting Time, Subject, Location

Meeting Time, Subject, Location, Notes

ios 의 경우

Secure Mail 에서 내보내는 일정 이벤트는 읽기/쓰기가 가능하지만 Secure Mail 외부에서는 이벤트에 대한 변경이 불가능합니다.

중요:

- 다음 중 하나에 해당하는 경우 Secure Mail 에서 이 기능은 표시되지만 사용되지 않도록 설정되어 있습니다.
 - 일정 내보내기 정책이 꺼짐으로 설정되어 있습니다.

- MDX 버전에 정책이 포함되어 있지 않습니다.
- 전자 메일 계정이 개인 일정 앱에 이미 구성되어 있고 iCloud 계정이 사용되지 않도록 설정된 경우 이 기능은 작동하지 않습니다. 이 기능은 개인 일정 앱에 다른 계정이 구성되지 않은 경우에 작동합니다.
- URL 을 시작하고 개인 일정에서 Secure Mail 일정 이벤트를 편집하려면 앱 URL 구성표 MDX 정책에 “**ctxevent:**” 값이 포함되어 있는지 확인합니다.

Android 의 경우

Secure Mail 에서 내보내는 일정 이벤트는 읽기 전용입니다. Secure Mail 이벤트를 편집하려면 일정 이벤트에서 **Secure Mail** 이벤트 링크를 누릅니다.

중요:

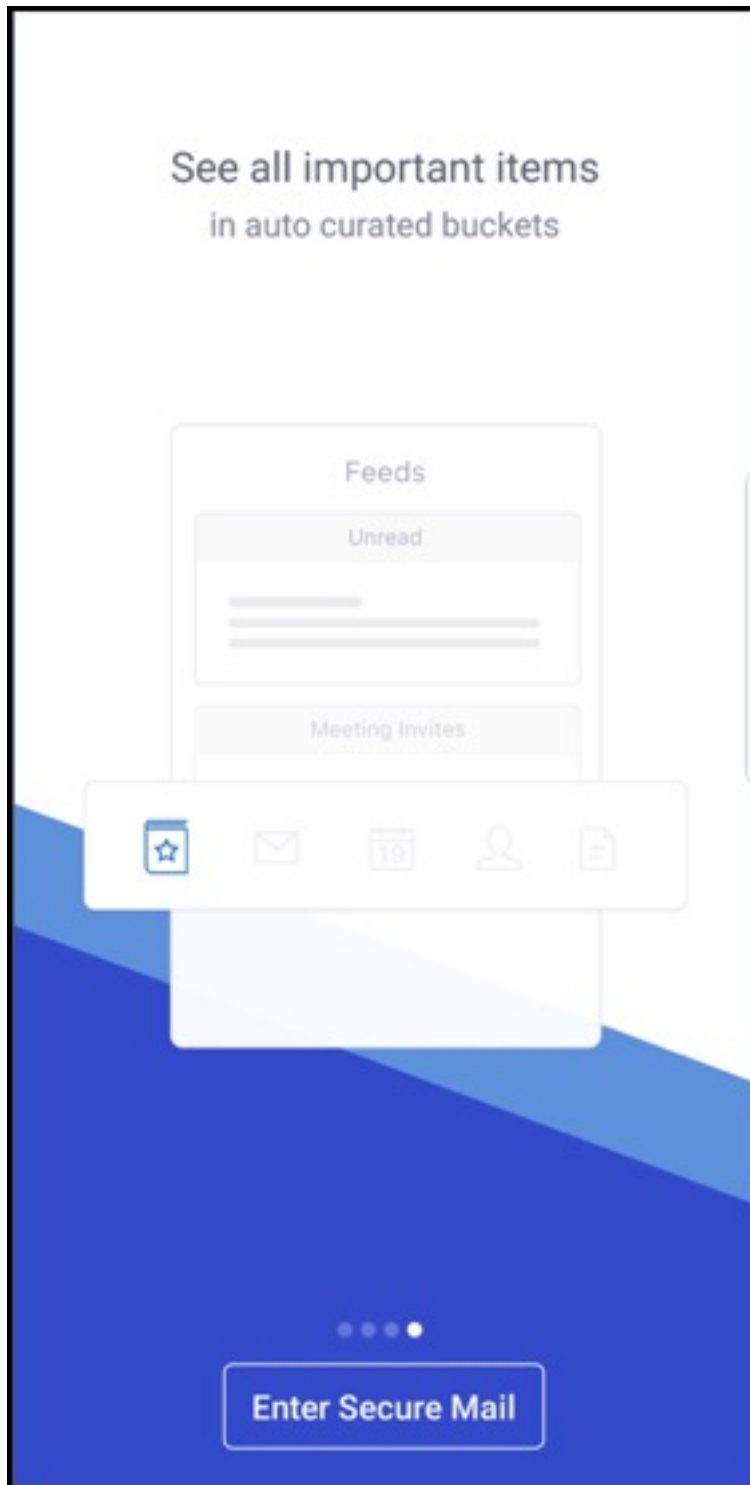
- 다음 중 하나에 해당하는 경우 Secure Mail 에서 이 기능은 표시되지만 사용되지 않도록 설정되어 있습니다.
 - 일정 내보내기 정책이 꺼짐으로 설정되어 있습니다.
 - MDX 버전에 정책이 포함되어 있지 않습니다.
- 인바운드 문서 교환 MDX 정책이 제한 없음으로 설정되어 있는지 확인합니다.
- Samsung 및 Huawei 장치에서는 Secure Mail 이벤트 링크를 사용할 수 없습니다.

피드 폴더

Secure Mail 의 피드 폴더에 모든 읽지 않은 전자 메일, 주의가 필요한 모임 초대 및 예정된 모임이 표시됩니다.

피드 카드를 보려면

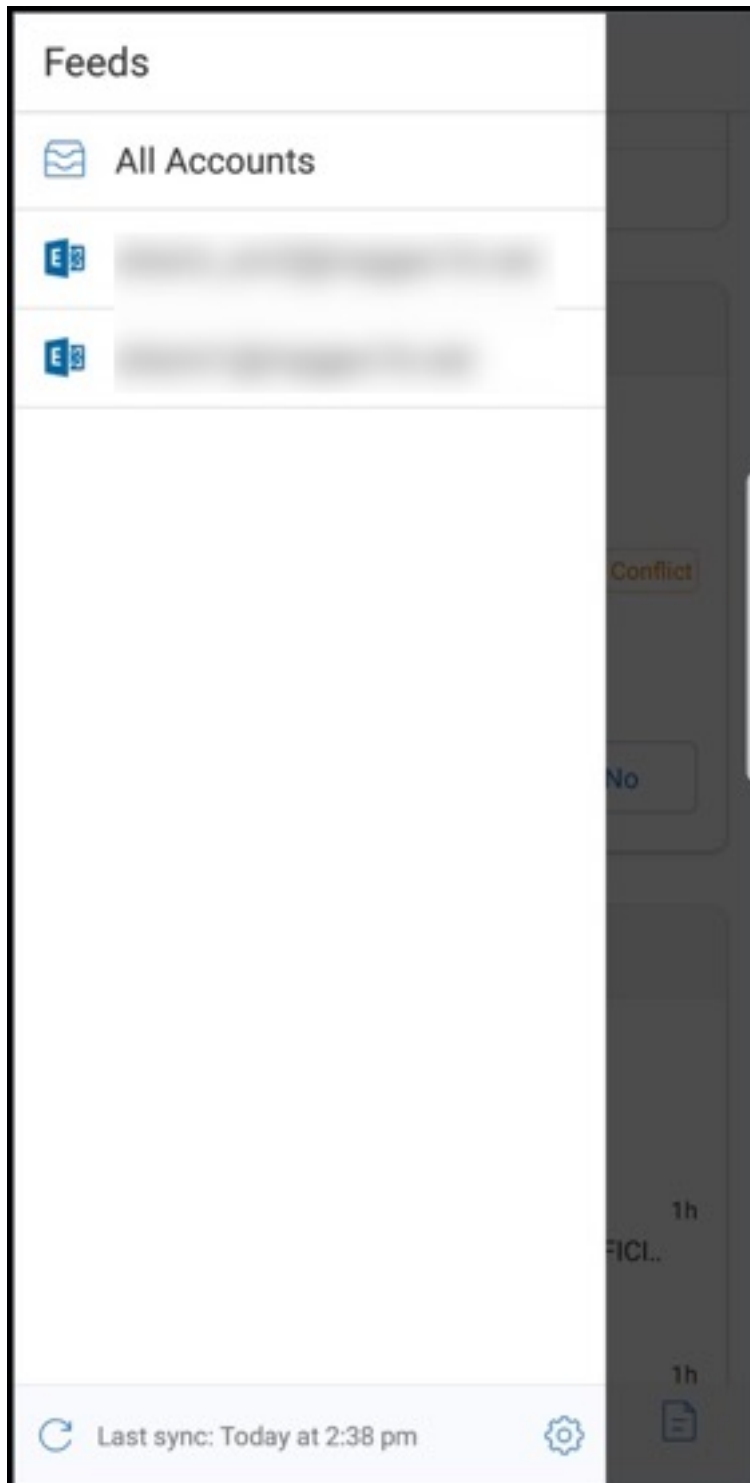
바닥글 탭 표시줄의 오른쪽 아래에서 피드 아이콘을 누릅니다.



다음 피드 카드가 나타납니다.

- 읽지 않음
- 모임 초대
- 예정된 모임

기본적으로 Secure Mail 은 기본 계정의 피드만 표시합니다. 계정을 둘 이상 구성한 경우 다른 계정의 피드를 볼 수 있습니다. 다른 계정의 피드를 보려면 피드를 누르고, 햄버거 아이콘을 누른 다음 해당하는 계정을 선택합니다.



항목의 타임스탬프를 기준으로 정렬된 피드가 다음 상한과 함께 나타납니다.

- 읽지 않은 전자 메일 5 개

- 모임 초대 2 개
- 예정된 모임 3 개

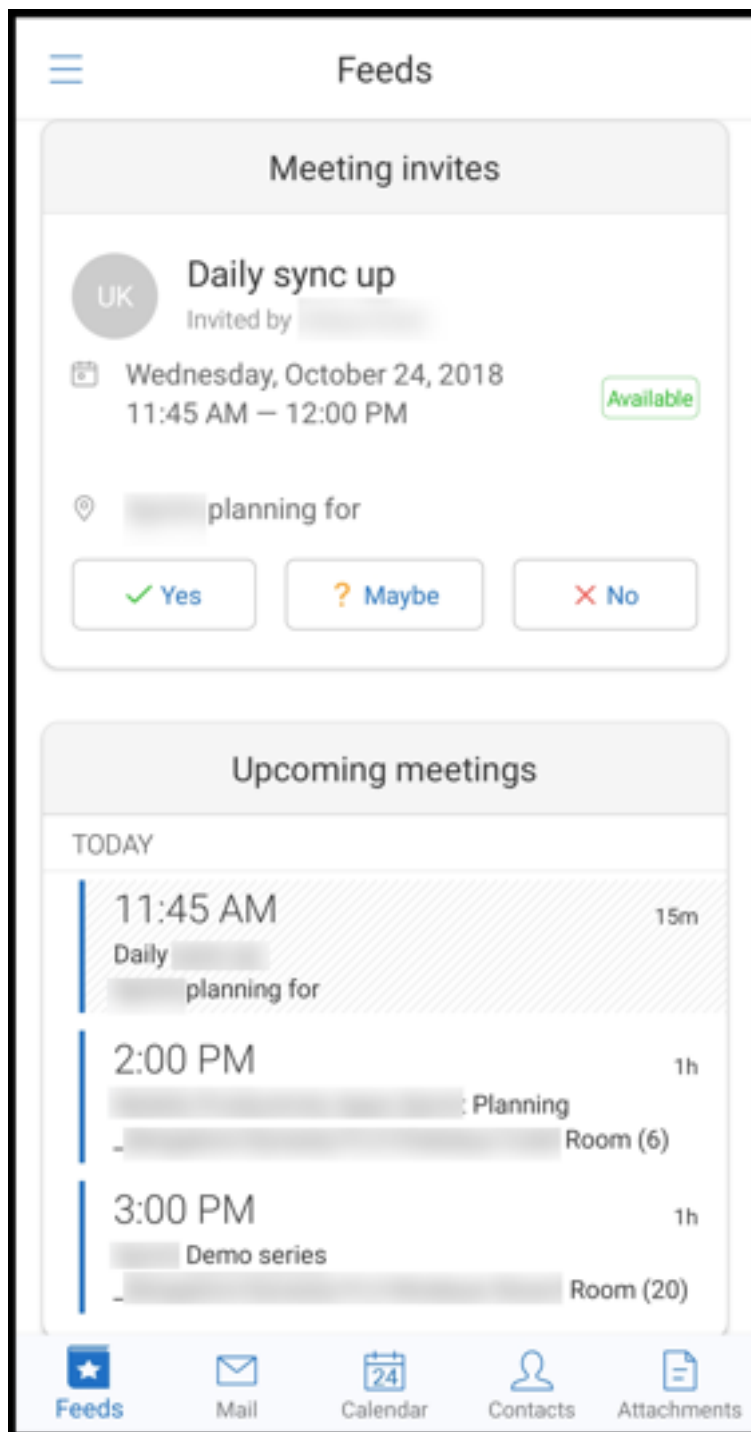
피드 카드에서 모든 항목을 보려면 모두 보기를 누릅니다.

참고 각 카드에 표시되는 피드 수는 장치에 설정된 메일 동기화 기간에 따라 달라집니다.

피드 폴더의 향상된 기능

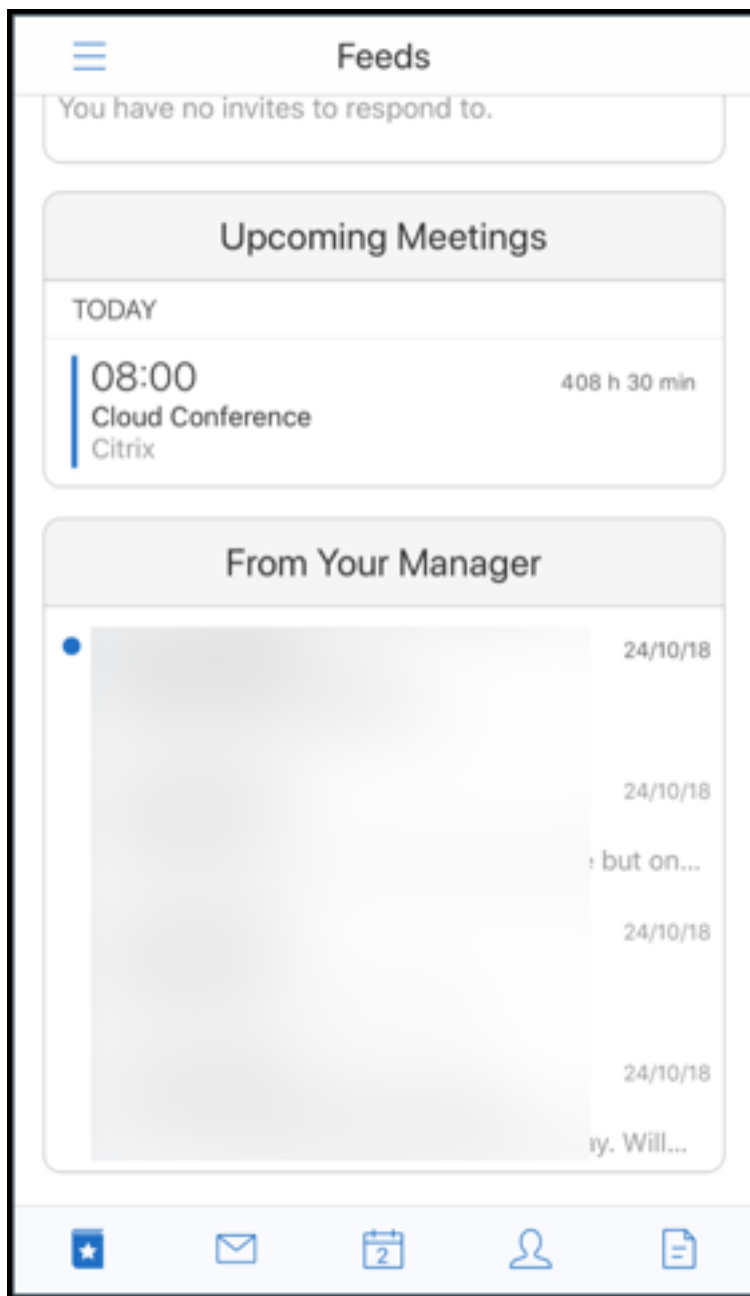
기존 피드 폴더의 향상된 기능은 다음과 같습니다.

- 자동으로 동기화된 모든 폴더의 모임 초대가 피드 카드에 표시됩니다.
- 피드 카드에 최대 5 개의 예정된 모임이 표시됩니다.
- 다음 24 시간 동안 예정된 모임이 피드 카드에 표시되고 오늘 및 내일 섹션으로 구분됩니다.



관리자의 피드

Secure Mail의 피드 화면에서 관리자의 전자 메일을 볼 수 있습니다. 관리자가 보낸 메일 피드에는 메일 동기화 기간 설정에 따라 최대 5개의 전자 메일이 나타납니다. 더 많은 관리자 전자 메일을 보려면 모두 보기를 누릅니다.



사전 요구 사항:

Exchange Server 에서 EWS(Exchange 웹 서비스) 가 사용되도록 설정되었는지 확인합니다.

관리자 카드는 Active Directory 에서 가져온 조직 세부 정보 (Outlook 연락처) 를 기반으로 나타냅니다. 관리자 피드에 정확한 세부 정보를 표시하려면 관리자가 Active Directory 에서 조직 계층을 구성했는지 확인합니다.

참고:

이 기능은 IBM Lotus Notes 서버에서 지원되지 않습니다.

일정에서 모임 참가

Secure Mail에서는 사용자가 일정에 있는 초대로부터 바로 모임에 참가할 수 있습니다. 다음 표에는 지원되는 모임 유형 및 전화 번호 형식이 나열되어 있고, 각각의 전화 접속 요구 사항도 나열되어 있습니다.

지원되는 모임 유형

모임 유형	식별 요구 사항	모임 참가를 누른 후의 작업
Microsoft Teams		Microsoft Teams 앱이 설치되어 있으면 앱이 열리고 사용자가 회의에 참가합니다. 앱이 설치되어 있지 않으면 앱 스토어에서 Microsoft Teams를 설치할 수 있는 옵션이 사용자에게 표시됩니다.
GTM(GoToMeeting)	모임 콘텐츠에서 다음 중 하나: 1) 다음 유형의 URL: https://www1.gotomeeting.com/join/1234567892 ; 2) 다음 형식 중 하나의 GTM 액세스 코드: GTM: 123456789, GTM -123456789, G2M -123456789, G2M: 123456789	GTM 앱이 설치된 경우 이 앱이 열리고 사용자가 모임에 참가하게 됩니다. 이 앱이 설치되지 않은 경우 앱 저장소로 이동하여 GTM을 설치할 수 있는 옵션이 사용자에게 표시됩니다. gotomeet.me/username 형식인 GTM의 경우 앱이 열리고 사용자가 모임에 참가하게 됩니다.
WebEx		Citrix Secure Web이 열리고 래핑되지 않은 WebEx 앱 (장치에 설치된 경우)을 엽니다. WebEx는 Android의 경우 Secure Web 제한된 열기 제외 목록에 그리고 iOS의 경우에는 허용된 URL 정책에 예외로 추가되어야 합니다.
Skype for Business		사용자는 Secure Web에서 열리는 링크를 클릭할 수 있고, Secure Web은 래핑되지 않은 Skype for Business 앱 (장치에 설치된 경우)을 엽니다. Android의 경우 Secure Web 제한된 열기 제외 목록 정책에서 Skype for Business 앱을 예외로 추가할 수 있습니다. iOS의 경우 허용된 URL 정책에 예외를 추가합니다.

다음 목록의 정책을 구성하면 사용자가 모임 링크를 눌러 해당하는 앱을 열 수 있습니다.

Microsoft Teams 앱

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

Zoom 앱

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

Webex(래핑되지 않은 앱)

- **iOS** - “URL 허용”정책: +^wbx: 예제 정책 문자열은 ^http:,^https:,^mailto:=ctxmail:,+^citrixreceiver:,+^telprompt:,+g2m-2:,+^col-g2w-2:,+^wbx:,+^maps:ios_addr:
- **Android** - “Open-in Exclusions” 정책: {action=android.intent.action.VIEW scheme=wbx package=com.cisco.webex.meetings}

Skype for Business

- **iOS** - “URL 허용” 정책 : +^lync:
- **Android** - “Open-in Exclusions” 정책: {action=android.intent.action.VIEW scheme=lync package=com.microsoft.office.lync15}

Skype

- **iOS** - “URL 허용” 정책 : +^skype:
- **Android** - “Open-in Exclusions” 정책: {action=android.intent.action.VIEW scheme=skype package=com.skype.raider}

전화 접속 사양

다음 목록은 모임의 유형과 각각에 대해 지원되는 전화 번호 형식과 회의 코드 형식을 나타냅니다.

GTM(GoToMeeting):

지원되는 전화 번호 형식:

- GTM 형식의 모든 전화 번호. 예:
 - 인도 (무료): 000 800 100 7855
 - 미국 (무료): 1 877 309 2073

- RFC 3966 형식 표준을 충족하는 모든 전화 번호 자세한 내용은 [인터넷 표준 추적 프로토콜 문서](#)를 참조하십시오.

지원되는 회의 코드 형식:

회의 코드는 모임 본문에서 다음 형식 중 하나로부터 얻습니다.

- URL(*.gotomeeting.com/join/123456789)
- URL([gotomeet.me](#)/username 형식)
- “GTM:123456789” 등의 “GTM” 형식
- “G2M:123456789” 등의 “G2M” 형식
- “Access Code: 123456789” 등의 형식

WebEx:

지원되는 전화 번호 형식:

- WebEx 전화 접속 형식의 모든 전화 번호. 예제 (Verizon 및 미국):
 - 1-866-652-5088
 - 1-517-466-3109
- WebEx 오디오 연결 형식의 모든 전화 번호. 예:
 - 1-650-479-3207(미국 유료)
- RFC 3966 형식 표준을 충족하는 모든 전화 번호

지원되는 회의 코드 형식:

모임 콘텐츠에 다음 형식 중 하나가 포함되어야 합니다.

- 모임 번호: 123 456 789
- 액세스 코드: 123 456 789

메모:

9 자리 이하인 회의 코드의 경우, 모임에 전화로 접속하기 위해 # 키가 자동으로 추가됩니다.

Skype for Business

지원되는 전화 번호 형식:

- RFC 3966 형식의 모든 전화 번호 자세한 내용은 [인터넷 표준 추적 프로토콜 문서](#)를 참조하십시오.

지원되는 회의 코드 형식:

모임 본문에는 “회의 ID: 123456789” 텍스트가 포함됩니다.

메모:

Skype for Business 모임의 경우 # 키가 자동으로 추가됩니다.

일반 오디오 회의 정보

지원되는 전화 번호 형식:

- RFC 3966 형식의 모든 전화 번호 자세한 내용은 [인터넷 표준 추적 프로토콜 문서](#)를 참조하십시오. 예:
 - 5555555555
 - (555) 555-5555
 - 555-555-5555
 - 555-555-555-5555(국가 코드가 있는 경우)
 - 1-555-555-5555
 - +1-555-555-5555

메모:

전화 번호에서 숫자 사이에 단일 구분 기호를 사용하십시오. 예를 들어 “) -” 를 사용하면 번호가 인식되지 않을 수 있습니다.

지원되는 회의 코드 형식:

권장 형식: “(전화 번호)” ,” (코드)”

최대 4 개의 심표를 지정할 수 있고 필요할 경우 # 키를 제공할 수 있습니다. 지원되는 형식의 목록은 이 문서의 뒷부분에 있는 표를 참조하십시오.

오디오 회의의 경우 다음 형식을 사용하여 사용자가 전화 접속을 누를 수 있습니다. 하지만 일정 모임의 본문에서 전화 번호를 누르는 경우에도 모임에 전화 접속할 수 있습니다. 이 경우 수동으로 회의 코드를 입력해야 합니다. 다음 전화 번호 및 회의 코드 형식이 지원됩니다.

지원되는 전화 번호 형식	회의 코드 구분 기호	예제
RFC 3966 형식의 모든 전화 번호 예: 5555555555, (555) 555-5555, 555-555-5555, 555-555-555-5555(국가 코드의 경우), 1-555-555-5555,+1-555-555-5555	참가자 코드	1-888-999-9999 참가자 코드: 99999999
	참가자 PIN	1-888-999-9999 참가자 PIN: 99999999

지원되는 전화 번호 형식	회의 코드 구분 기호	예제
	게스트 코드	1-888-999-9999 게스트 코드: 99999999
	게스트 PIN	1-888-999-9999 게스트 PIN: 99999999
	참가자/게스트 코드	1-888-999-9999 참가자/게스트 코드: 99999999
	의자 코드	1-888-999-9999 의자 코드: 99999999
	의자 PIN	1-888-999-9999 의자 PIN: 99999999
	사회자 코드	1-888-999-9999 사회자 코드: 99999999
	사회자 PIN	1-888-999-9999 사회자 PIN: 99999999
	호스트 PIN	1-888-999-9999 호스트 PIN: 99999999
	PIN	1-888-999-9999 PIN: 99999999
	액세스 코드	1-888-999-9999 액세스 코드: 99999999
	코드	1-888-999-9999 코드: 99999999
	회의 코드	1-888-999-9999 회의 코드: 99999999
	회의 ID	1-888-999-9999 회의 ID: 99999999
	,	+1 (631) 992-3240,958209234#
	”	+1 (631) 992-3240,,958209234#
	”,”	+1 (631) 992-3240,,,958209234#
	””	+1 (631) 992-3240,,,,958209234#
	암호	+1 (631) 992-3240 passcode 958209234#
	ext	+1 (631) 992-3240 ext:958209234#
	ext.	+1 (631) 992-3240 ext. 958209234#
	;ext=	+1 (631) 992-3240; ext. 958209234#

지원되는 전화 번호 형식	회의 코드 구분 기호	예제
	extn	+1 (631) 992-3240 extn 958209234#
	HC	+1 (631) 992-3240 HC 958209234#
	xtn	+1 (631) 992-3240 xtn 958209234#
	xt	+1 (631) 992-3240 xt 958209234#
	x	+1 (631) 992-3240 x 958209234#
	PC	+1 (631) 992-3240 PC 958209234#
	pc	+1 (631) 992-3240 pc 958209234#

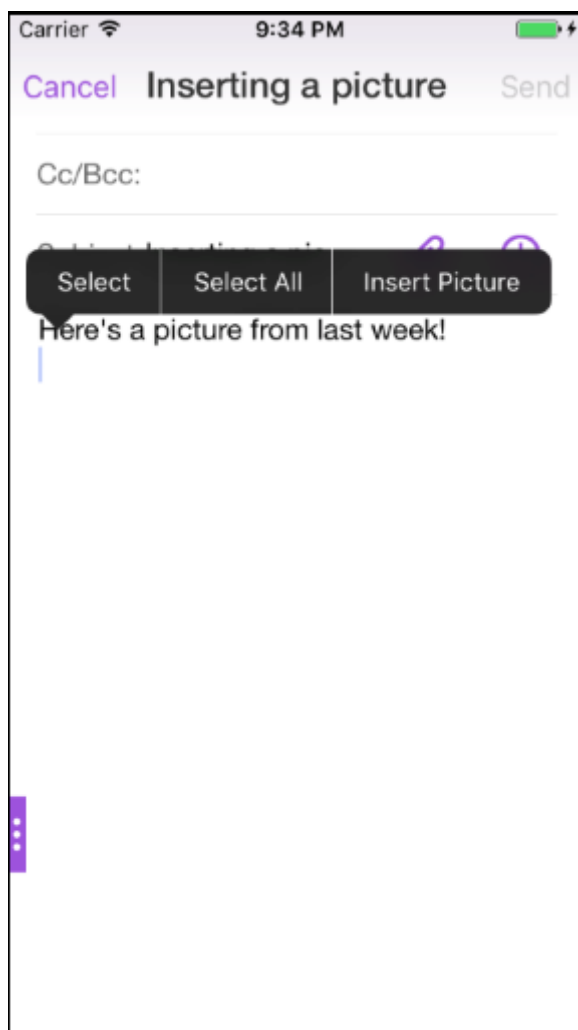
개인 일정 오버레이

iOS 및 Android 장치에서 기본 일정 앱에서 개인 일정을 가져오고 Secure Mail 에서 개인 이벤트를 확인할 수 있습니다. 이 일정 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [개인 일정 이벤트 보기](#)를 참조하십시오.

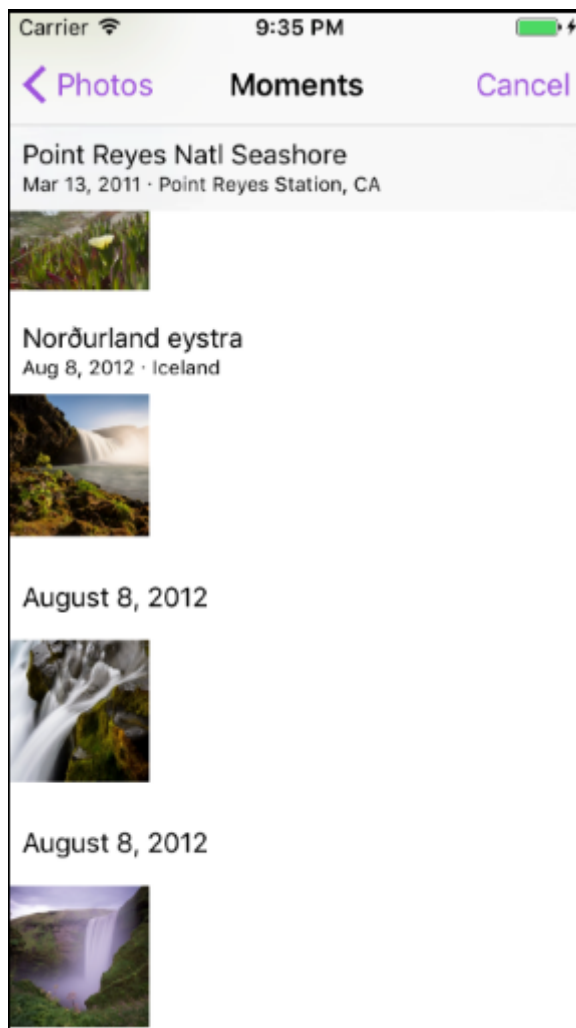
인라인 이미지 삽입

다음 절차는 인라인 이미지를 삽입하는 방법에 대해 설명합니다.

1. 전자 메일에 인라인 이미지를 첨부하려면 메일 본문을 길게 누르십시오. 나타나는 옵션에서 사진 삽입을 누르십시오.



2. Secure Mail 에서 사진에 액세스하라는 메시지가 나타날 수 있습니다. 사진 갤러리가 나타납니다. 갤러리로 이동한 후 삽입하려는 사진을 누릅니다.



3. 이제 메일에 선택한 이미지가 포함됩니다.



살짝 밀기 동작

iOS 및 Android 장치에서 전자 메일을 왼쪽 또는 오른쪽으로 살짝 밀어 동작을 수행할 수 있습니다. 이 기능에 대한 사용자 도움말 설명서는 Citrix User Help Center 문서 [살짝 밀기 동작 사용](#)을 참조하십시오.

iOS 및 Android 에서 Skype for Business 모임 참가

Secure Mail 을 통해 Skype for Business 모임에 원활하게 참가할 수 있습니다. 이 기능을 사용하려면 장치에 Skype for Business 앱이 설치되어 있어야 합니다.

Skype for Business 모임에 참가하려면

1. Skype for Business 모임 미리 알림 또는 일정 이벤트를 누릅니다.

2. 이벤트 세부 정보 화면에서 Skype 모임 참가를 누릅니다. 새 창에서 Skype for Business 모임이 시작됩니다.

장치에 Skype for Business 를 설치하지 않은 경우 **Skype** 설치를 눌러 이 앱을 설치합니다.

첨부 파일의 앱 내 미리 보기 및 첨부 파일에 대한 기타 개선 사항

이제 Secure Mail 앱 내에서 QuickEdit 같은 타사 앱을 사용하여 열지 않고 첨부 파일 (MS Office 및 이미지) 을 미리 볼 수 있습니다.

첨부 파일을 볼 때 다음 동작을 수행할 수 있습니다.

- 사서함에서 파일을 첨부할 기존 메시지를 선택합니다.
- 파일을 첨부할 새 메시지를 선택합니다.
- 오프라인 액세스를 위해 첨부 파일을 저장합니다.
- 오프라인 파일에서 첨부 파일을 삭제합니다.
- 다른 응용 프로그램을 사용하여 첨부 파일을 엽니다.
- 첨부 파일의 원본 전자 메일 또는 일정 이벤트를 봅니다.

메모:

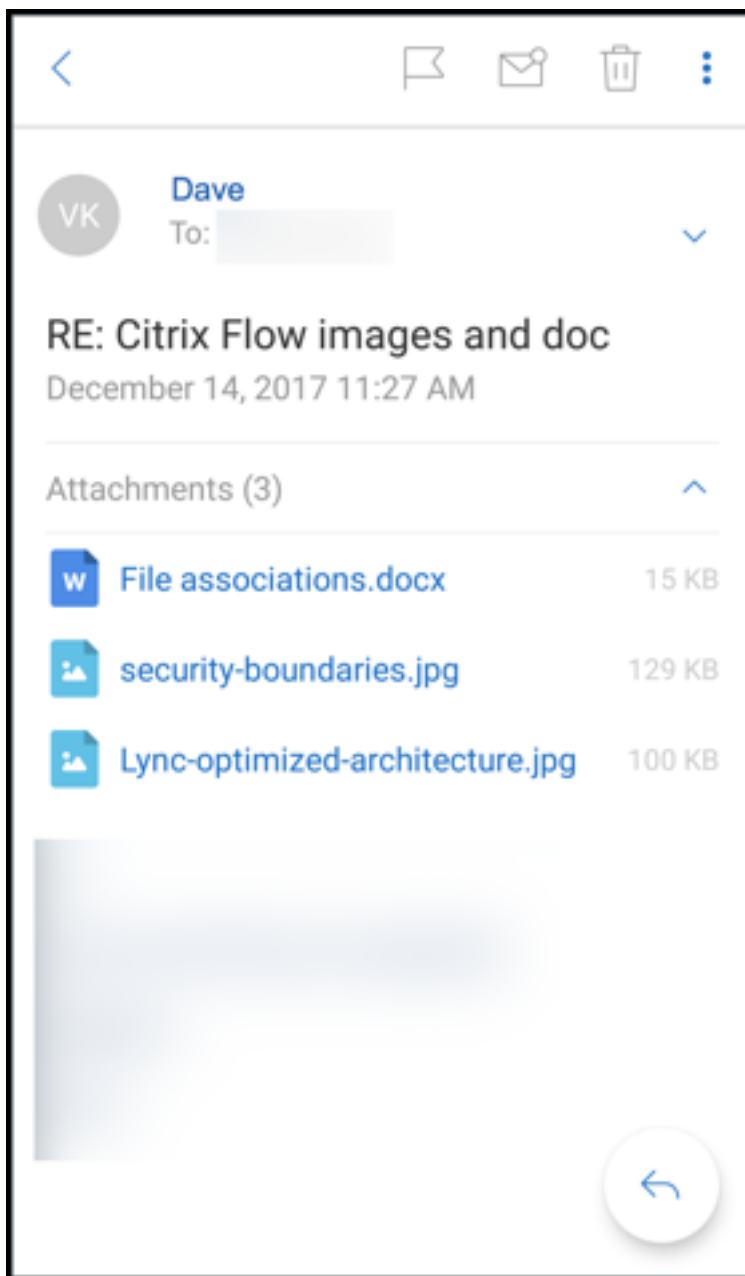
원본 전자 메일 또는 일정 이벤트는 첨부 파일 저장소에서 첨부 파일을 볼 때에만 볼 수 있습니다.

또한 다음의 경우 첨부 파일을 미리 볼 수 있습니다.

- 메시지 보기
- 새 메시지 작성
- 첨부 파일 폴더
- 일정 이벤트

파일을 첨부할 메시지를 선택하려면

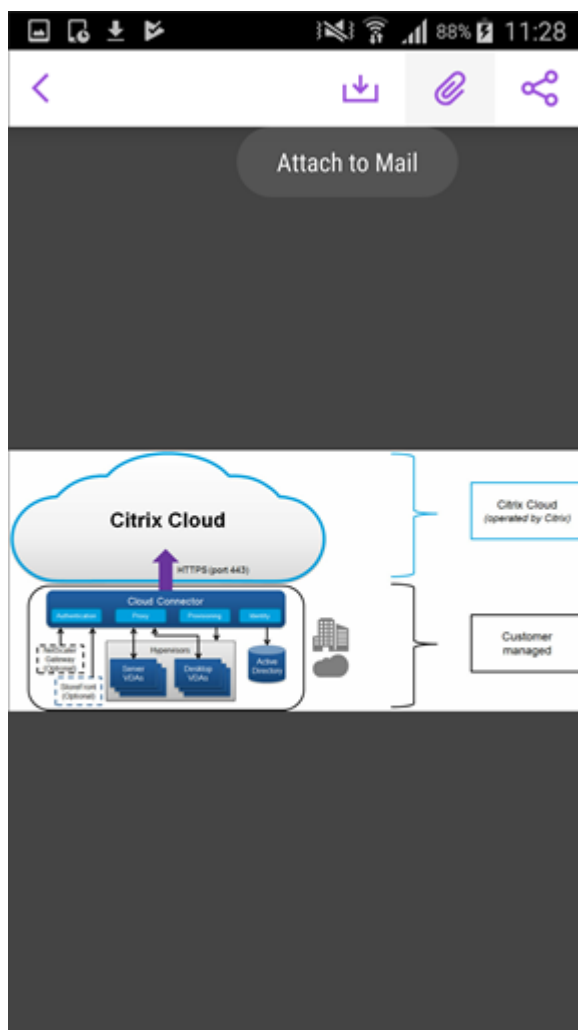
1. 첨부 파일이 포함된 전자 메일을 엽니다.



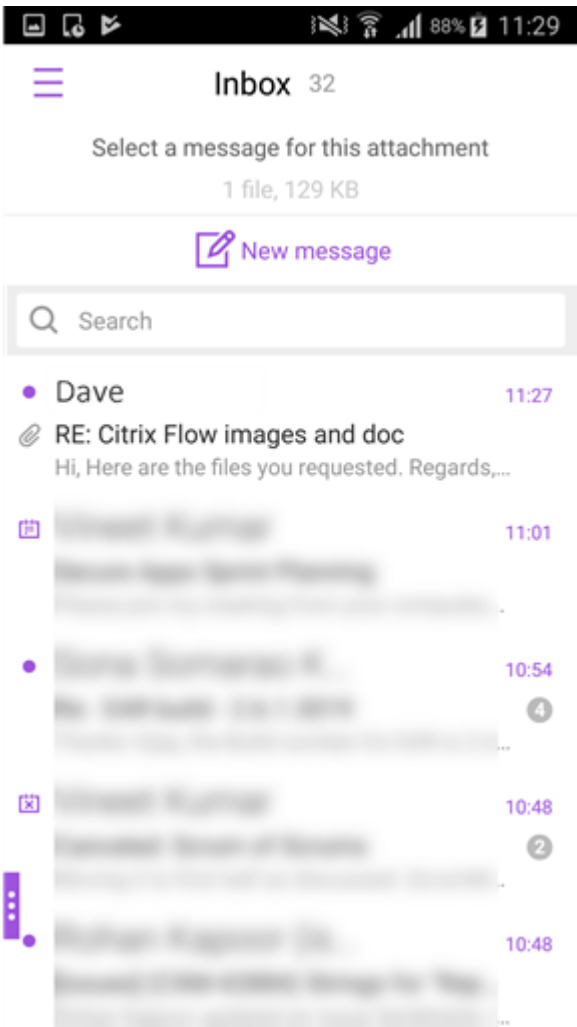
2. 첨부 파일을 누릅니다.

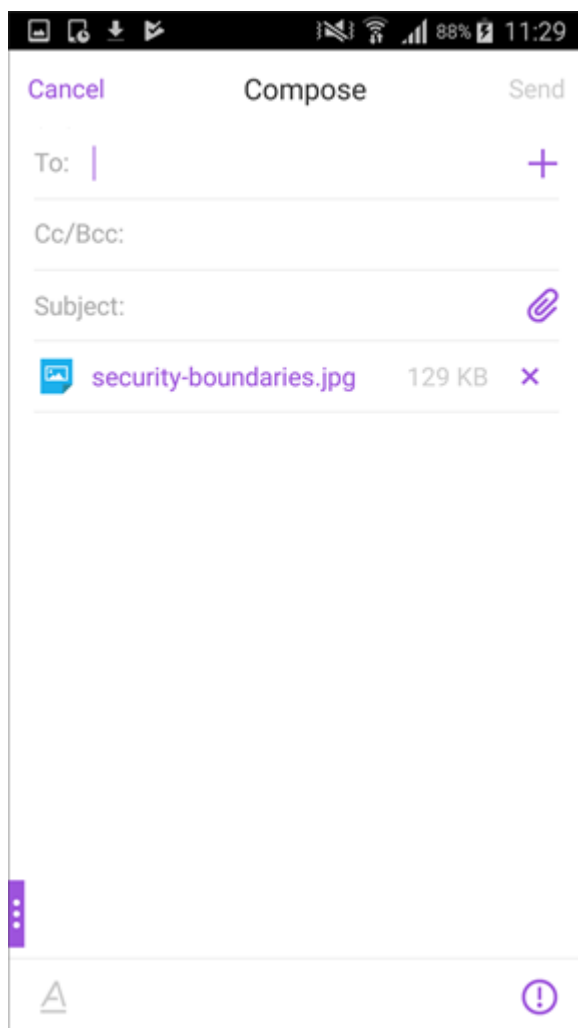
3. 첨부 아이콘을 누릅니다.

받은 편지함이 나타납니다.



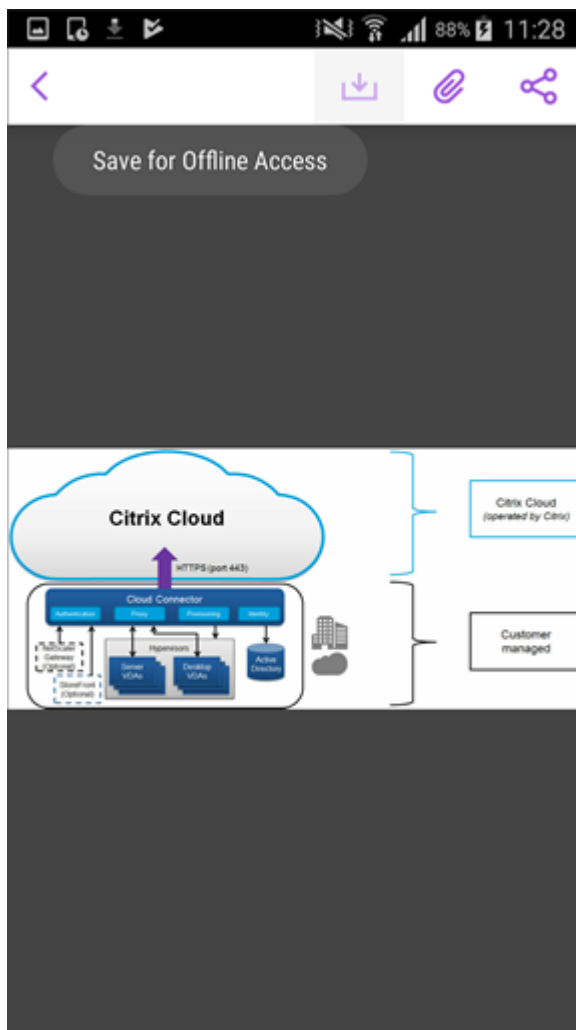
4. 이 파일을 첨부할 기존 메시지를 선택하거나 새 메시지를 눌러 이 파일을 새 메시지에 첨부합니다.





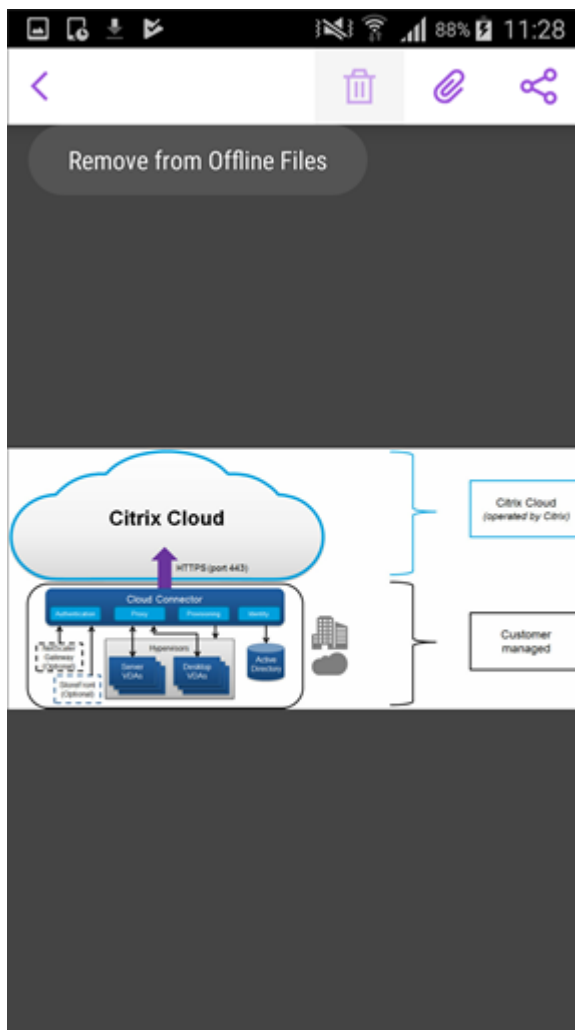
오프라인 액세스를 위해 첨부 파일을 저장하려면

1. 첨부 파일을 엽니다.
2. 페이지 오른쪽 위에 있는 자세히 아이콘을 누르고 오프라인 액세스를 위해 저장을 눌러 오프라인 액세스를 위해 첨부 파일을 저장합니다.



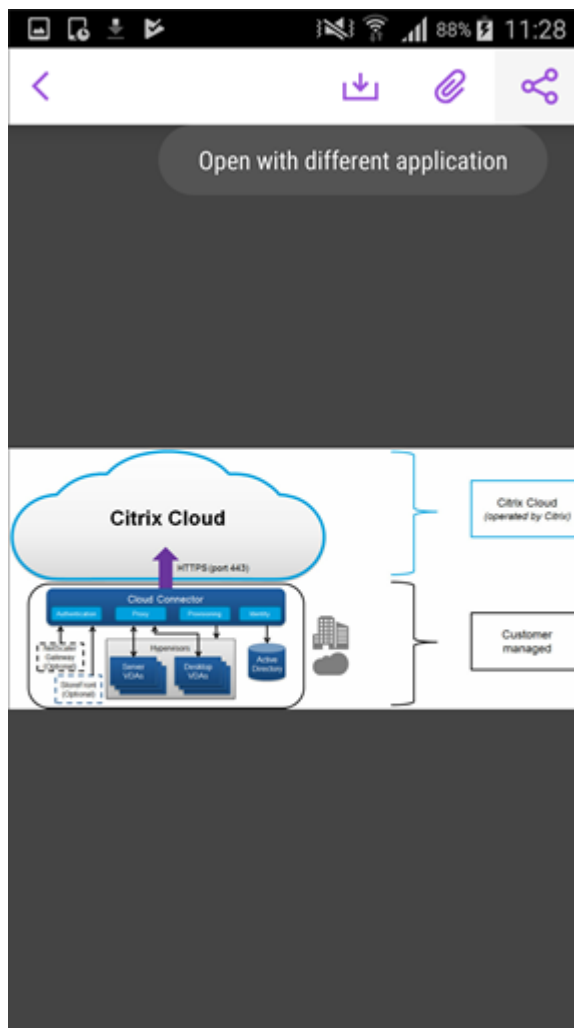
오프라인 파일에서 첨부 파일을 삭제하려면

1. 첨부 파일을 엽니다.
2. 페이지 오른쪽 위에 있는 자세히 아이콘을 누르고 오프라인 파일에서 제거를 눌러 첨부 파일을 오프라인 파일에서 삭제합니다.

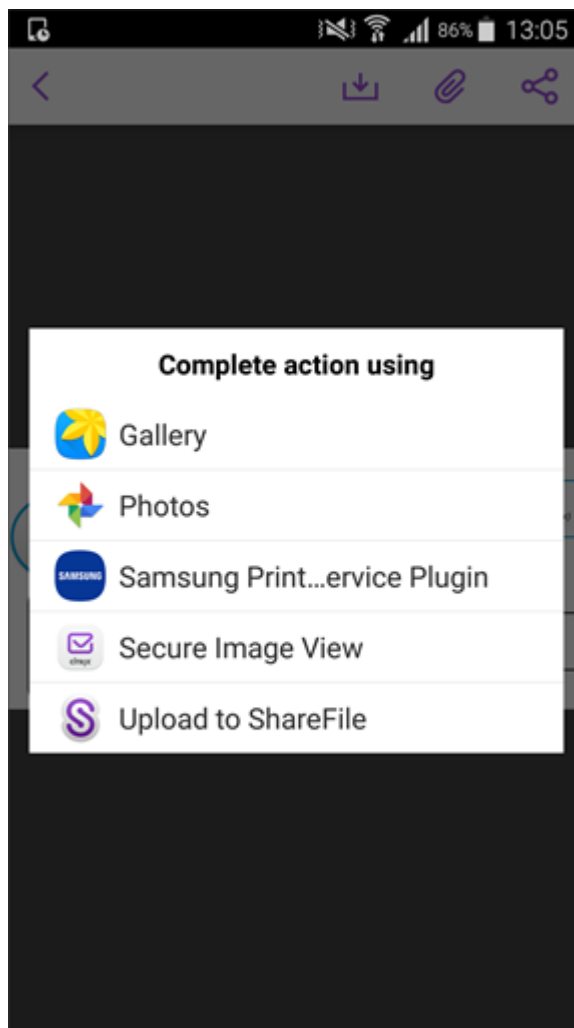


다른 응용 프로그램을 사용하여 첨부 파일을 열려면

1. 첨부 파일을 엽니다.
2. 페이지 오른쪽 위에 있는 자세히 아이콘을 누르고 다음으로 열기를 누릅니다. 다른 응용 프로그램을 사용하여 첨부 파일을 열려면

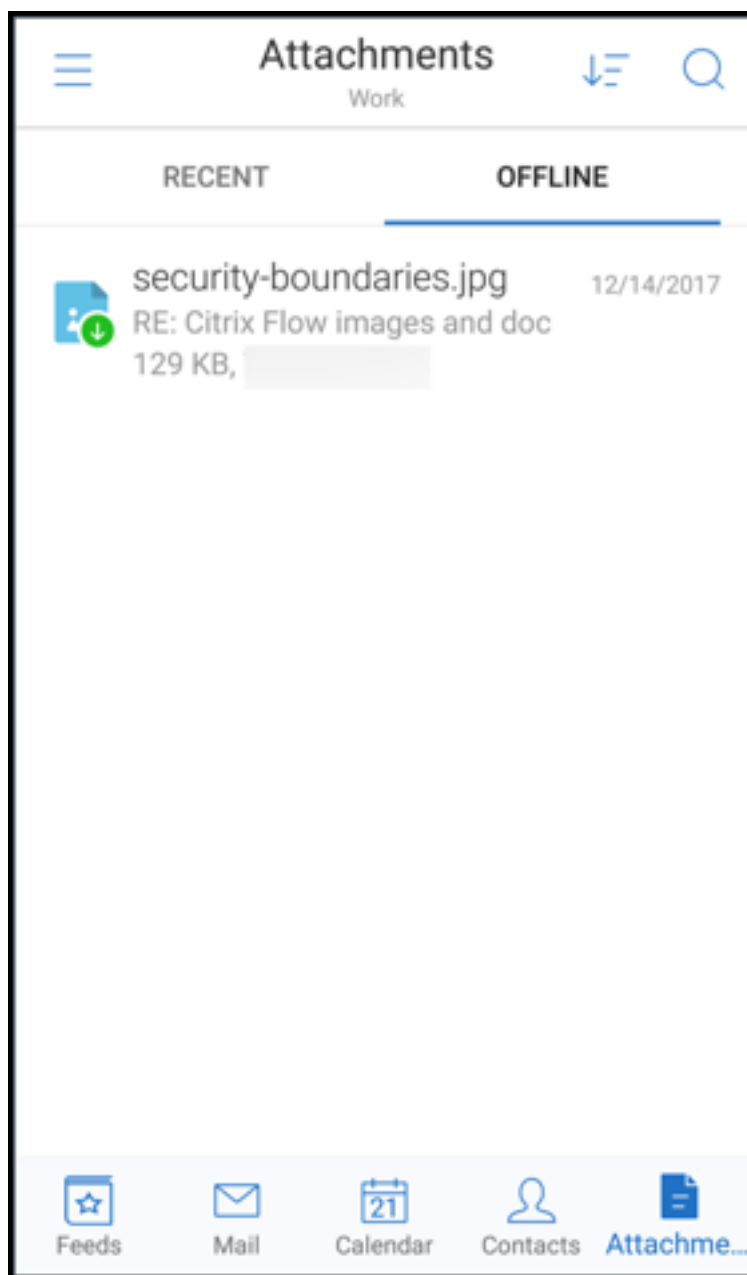


3. 표시되는 옵션에서 첨부 파일을 열 때 사용할 옵션 중 하나를 누릅니다.

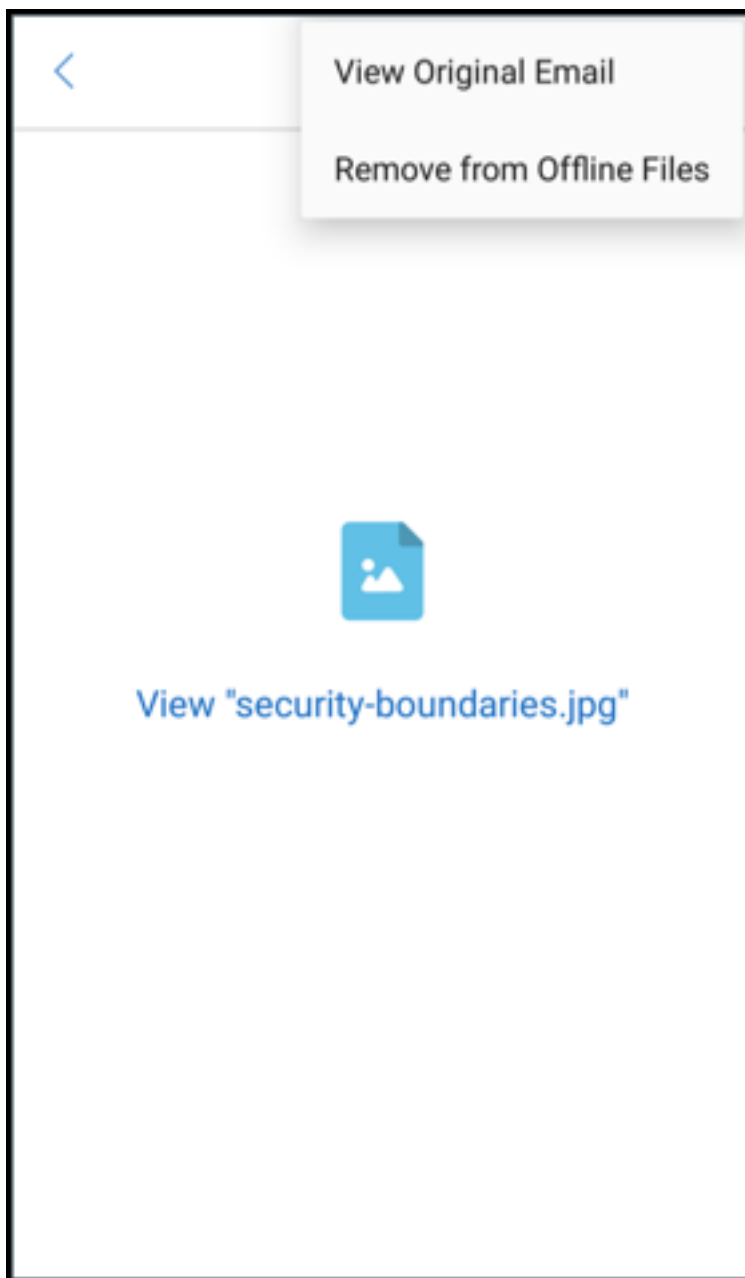


첨부 파일의 원본 전자 메일 또는 일정 이벤트를 보려면

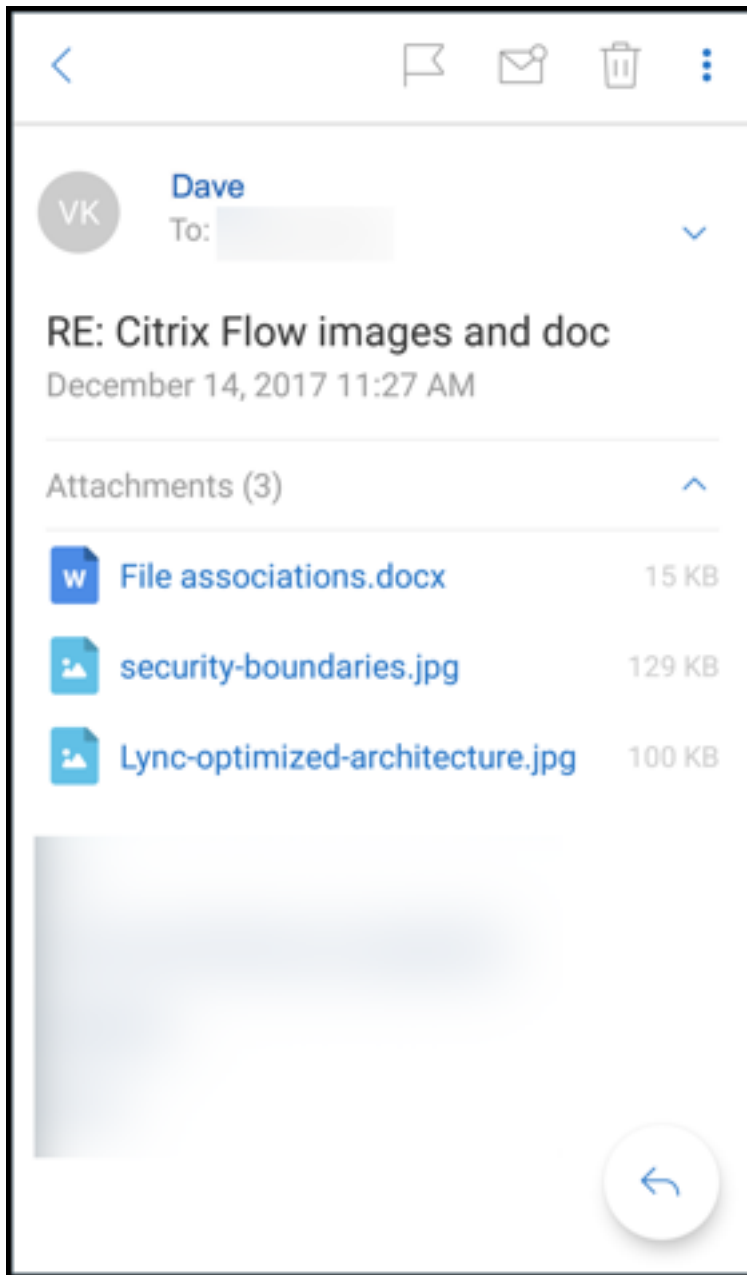
1. 화면 오른쪽 아래에 있는 첨부 파일 아이콘을 누릅니다.
2. 오프라인을 누릅니다.



3. 첨부 파일을 누르고 화면 오른쪽 위의 자세히 아이콘을 누릅니다.



4. 원본 전자 메일이 나타납니다.



전자 메일 주소 **(UPN)** 로 사용자 이름 마이그레이션

iOS 및 Android 용 Secure Mail 의 경우 Exchange 사용자 이름 및 암호 기반 인증에서 UPN 및 암호 기반 인증으로 마이그레이션할 수 있습니다.

이 기능을 사용하도록 설정한 경우 다음 중 아무 작업도 수행할 필요가 없습니다.

- Secure Mail 다시 설치
- Secure Mail 에서 계정 삭제 및 추가
- Secure Mail 에서 사용자 이름 변경

사전 요구 사항

마이그레이션을 진행하기 전에 사용자가 Secure Mail 버전 10.7.25 이상을 실행하는지 확인하십시오.

이 기능을 사용하려면 Attempt user name Migration On Auth Failure(인증 실패 시 사용자 이름 마이그레이션 시도) 정책을 사용하도록 설정해야 합니다.

UPN 기반 인증으로 마이그레이션하려면

1. Endpoint Management 에서 Attempt Username Migration On Auth Failure(인증 실패 시 사용자 이름 마이그레이션 시도) 정책을 사용하도록 설정합니다.
2. Exchange 사용자 계정을 사용자의 기본 SMTP 전자 메일 주소와 일치하는 새로운 UPN 으로 마이그레이션합니다. 마이그레이션하면 인증 실패가 트리거됩니다. Secure Mail 이 기본 SMTP 전자 메일 주소를 사용하여 인증을 시도합니다.

인증에 성공하면 사용자 계정이 업데이트된 UPN 으로 마이그레이션된 것입니다.

마이그레이션을 확인하려면

iOS 장치: 설정으로 이동하고 계정을 눌러 세부 정보를 표시합니다. 마이그레이션이 성공하면 기본 SMTP 전자 메일 주소가 계정 화면의 사용자 이름 필드에 나타납니다.

Android 장치: 설정으로 이동하고 계정을 눌러 세부 정보를 표시합니다. 마이그레이션이 성공하면 기본 SMTP 전자 메일 주소가 계정 세부 정보 화면의 사용자 이름 필드에 나타납니다.

개인 배포 목록

사전 요구 사항

- Exchange Server 에서 EWS(Exchange 웹 서비스) 가 사용되도록 설정되어 있어야 합니다.
- Microsoft Exchange Server 버전 10 SP1 이상.

iOS 및 Android 용 Secure Mail 은 개인 연락처 그룹을 지원합니다. Outlook 데스크톱 클라이언트에서 만든 연락처 그룹을 Secure Mail 에서 볼 수 있습니다. 생성된 연락처 그룹은 Secure Mail 의 연락처에 표시됩니다.

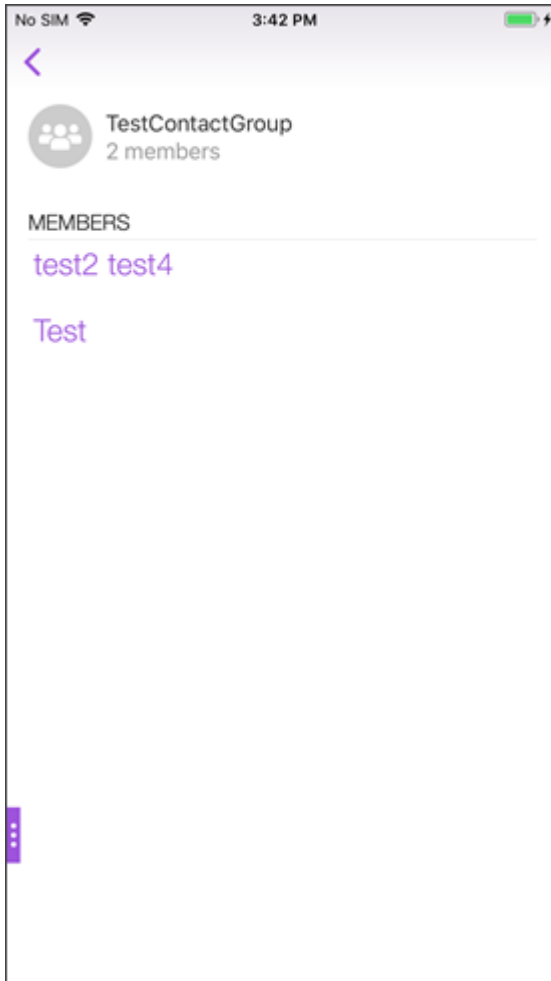
메모:

중첩된 연락처 그룹의 구성원은 Secure Mail 에서 볼 수 없습니다.

전자 메일을 작성하거나 일정 이벤트를 만들 때 개인 배포 목록을 사용할 수 있습니다. Exchange 를 사용하여 개인 연락처 그룹(배포 목록)을 만든 경우 Secure Mail 에서 목록을 볼 수 있습니다.

개인 배포 목록을 보려면

1. Secure Mail 에서 연락처를 엽니다.
2. 연락처 그룹의 이름을 입력합니다.
그룹이 검색 결과에 나타납니다.
3. 연락처 그룹을 누르면 구성원을 볼 수 있습니다.

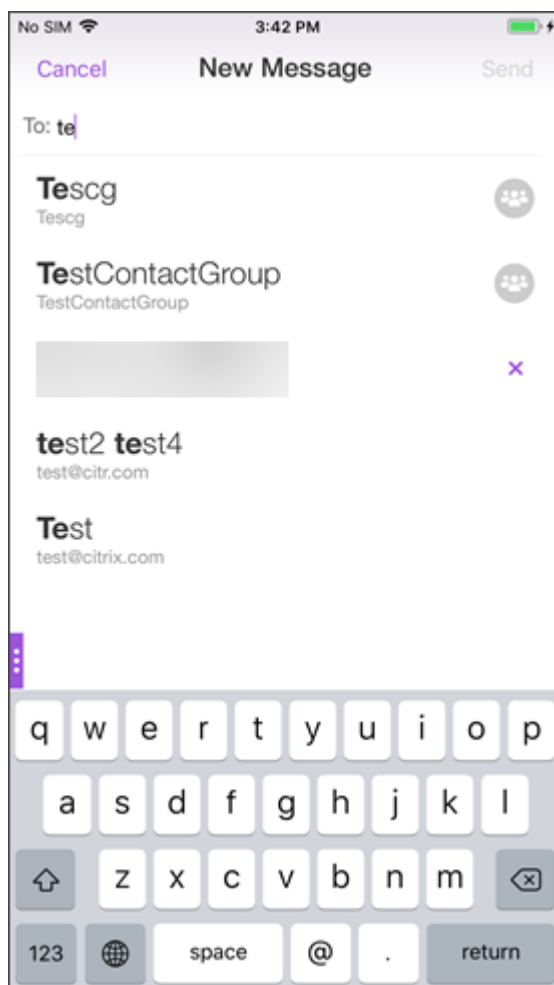


참고:

Secure Mail 에서 연락처 그룹을 편집할 수는 없습니다.

연락처 그룹에 보낼 메일을 작성하려면

1. Secure Mail 을 열고 편집 부동 작업 단추를 눌러 메일을 작성합니다.
2. 새 메시지 화면에서 받는 사람: 필드에 연락처 그룹의 이름을 입력합니다.
3. 표시되는 연락처 목록에서 연락처 그룹을 선택합니다.

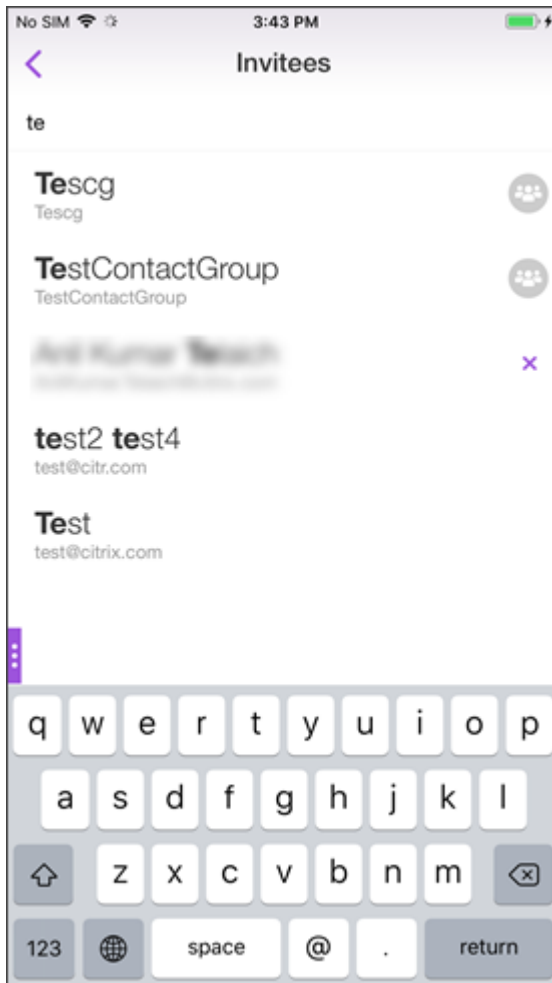


연락처 그룹은 다음 아이콘으로 표시됩니다.



연락처 그룹에 일정 초대를 보내려면

1. Secure Mail 을 열고 일정으로 이동합니다.
2. + 아이콘을 눌러 일정 이벤트를 만듭니다.
3. 새 이벤트 화면에서 초대할 사람을 눌러 구성원을 추가합니다.
4. 초대를 보낼 연락처 그룹의 이름을 입력합니다.



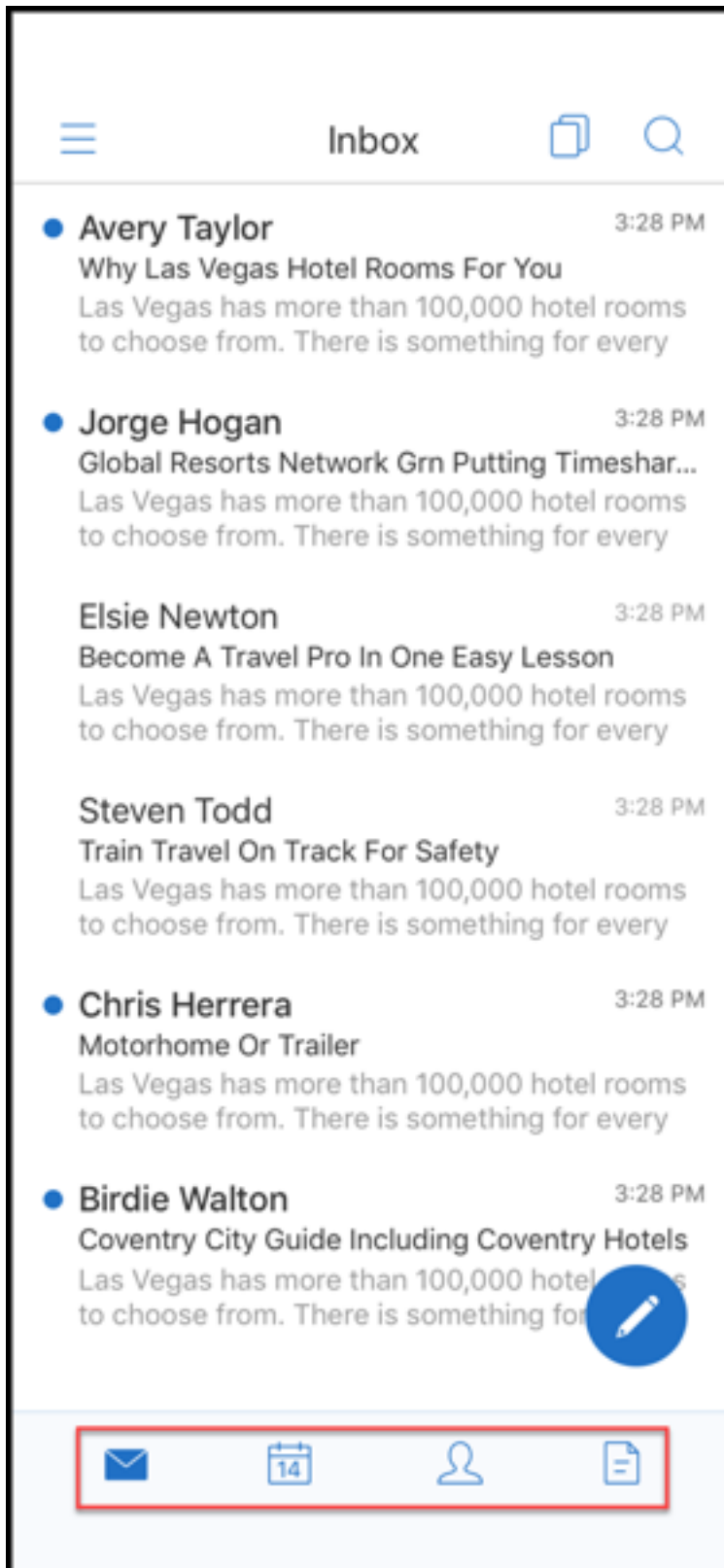
5. 표시되는 연락처 목록에서 연락처 그룹을 선택합니다.

폴더 동기화

iOS 및 Android 용 Secure Mail 에서 동기화 아이콘을 눌러 모든 Secure Mail 콘텐츠를 새로 고칠 수 있습니다. 동기화 아이콘은 사서함, 일정, 연락처, 첨부 파일 등 Secure Mail 의 슬라이드아웃에 표시됩니다. 동기화 아이콘을 누르면 사서함, 일정, 연락처 등 자동 새로 고침을 구성한 폴더가 업데이트됩니다. 동기화 아이콘의 옆에 마지막 동기화의 타임스탬프가 표시됩니다.

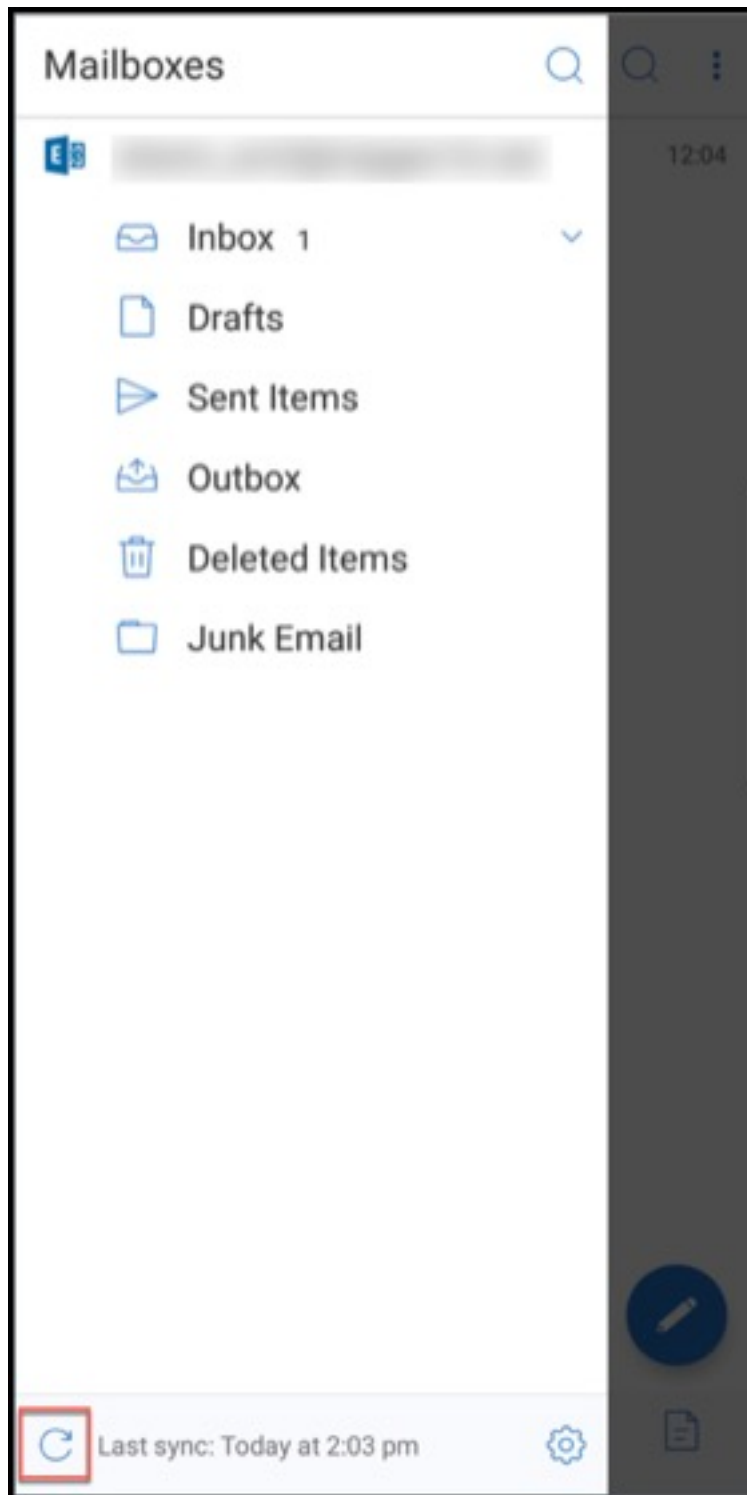
폴더를 동기화하려면

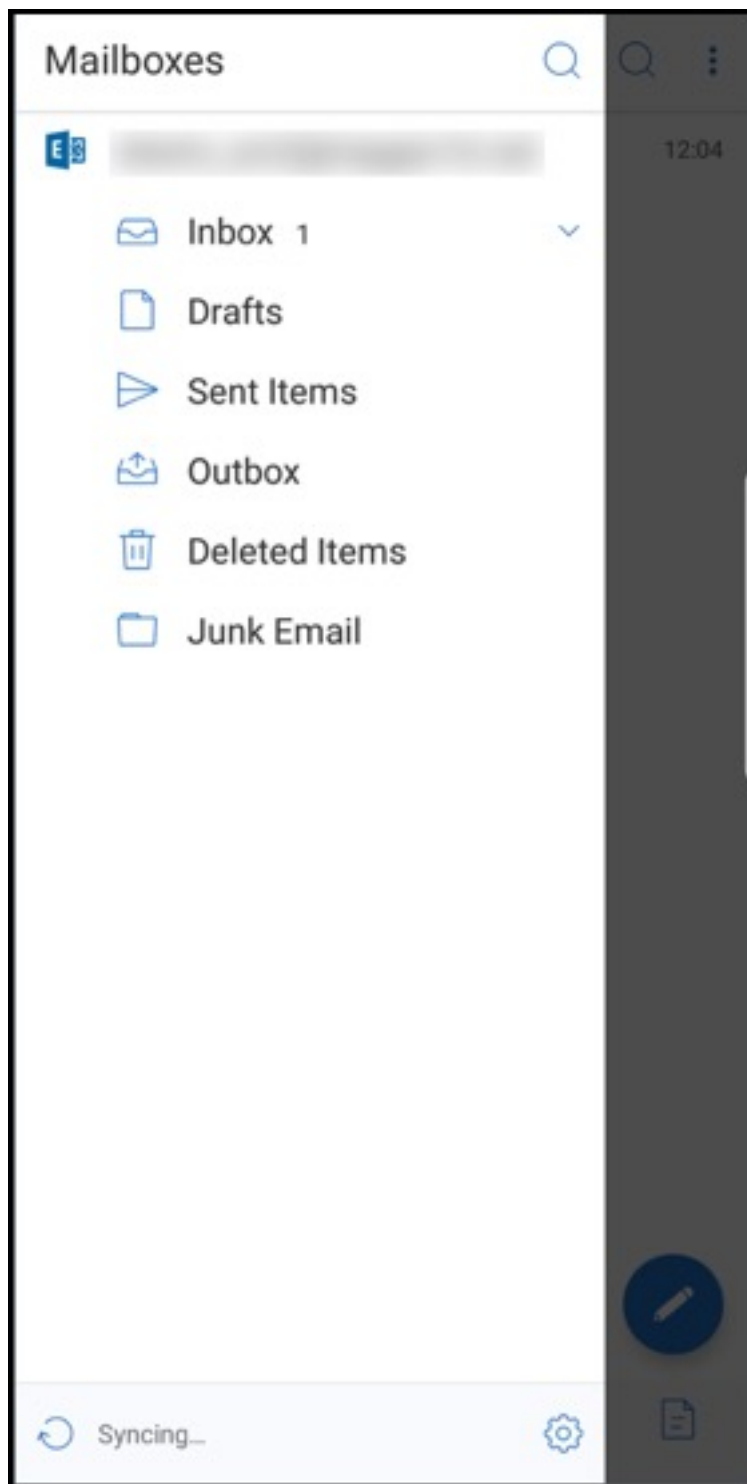
1. Secure Mail 을 엽니다.
2. 바닥글 탭 표시줄에 표시되는 사용 가능한 폴더 중에서 동기화하려는 폴더를 누릅니다.



3. 화면 왼쪽 위의 햄버거 아이콘을 누릅니다.

4. 화면 왼쪽 아래에서 동기화 아이콘을 누릅니다.





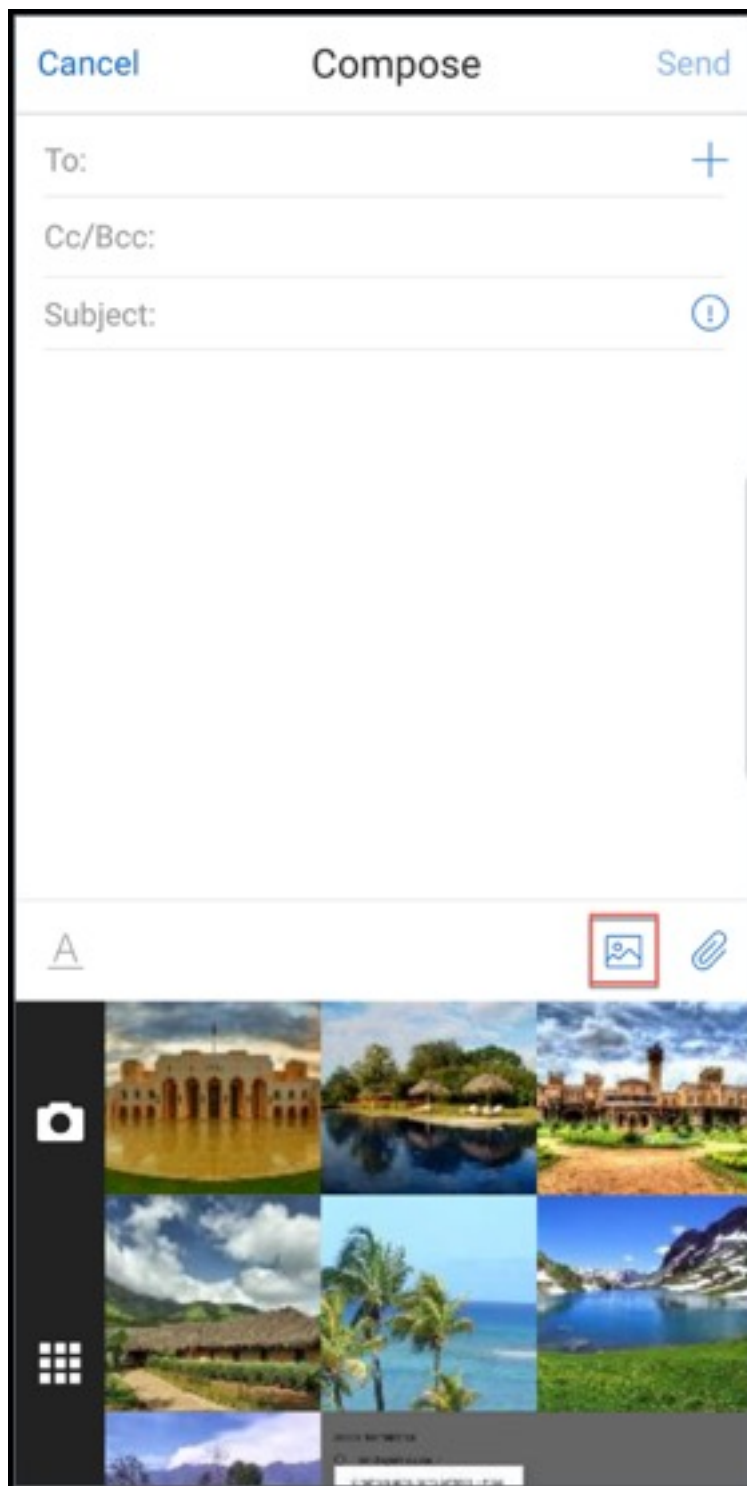
5. 폴더가 동기화되고 콘텐츠가 새로 고쳐집니다. 동기화 아이콘 옆에 타임스탬프가 표시됩니다.

사진 첨부 개선

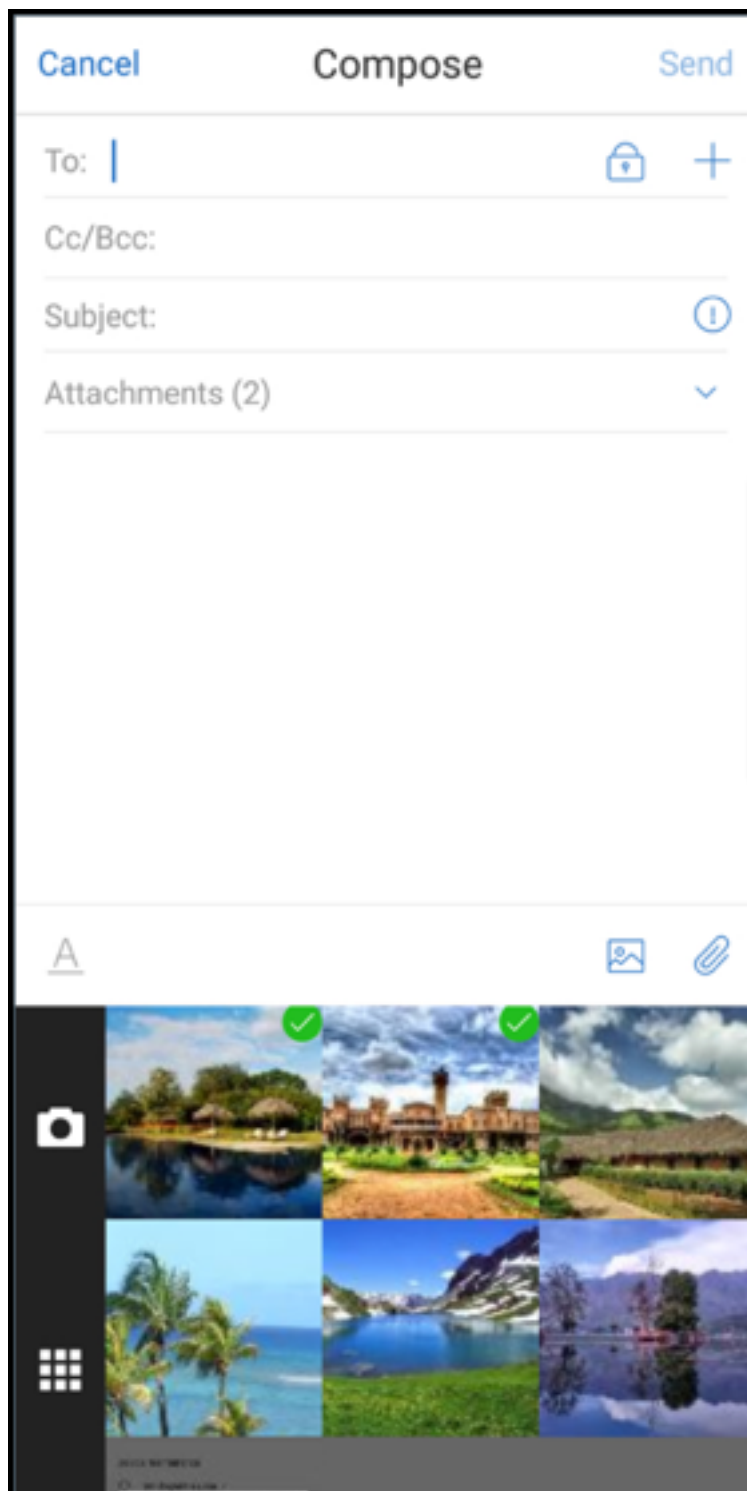
iOS 및 Android 용 Secure Mail 에서 새 갤러리 아이콘을 눌러 사진을 쉽게 첨부할 수 있습니다.

전자 메일에 사진을 첨부하려면

1. Secure Mail 을 엽니다.
2. 작성을 눌러 메일을 만들거나 응답 부동 작업 단추를 눌러 전자 메일에 회신합니다.
3. 화면 오른쪽 아래에 있는 첨부 파일 아이콘 옆의 갤러리 아이콘을 누릅니다.



4. 화면 아래에 카메라 및 날짜순 아이콘과 함께 갤러리가 나타납니다.
5. 갤러리에서 첨부할 이미지로 이동한 후 선택하거나 카메라 아이콘을 눌러 사진을 찍습니다.

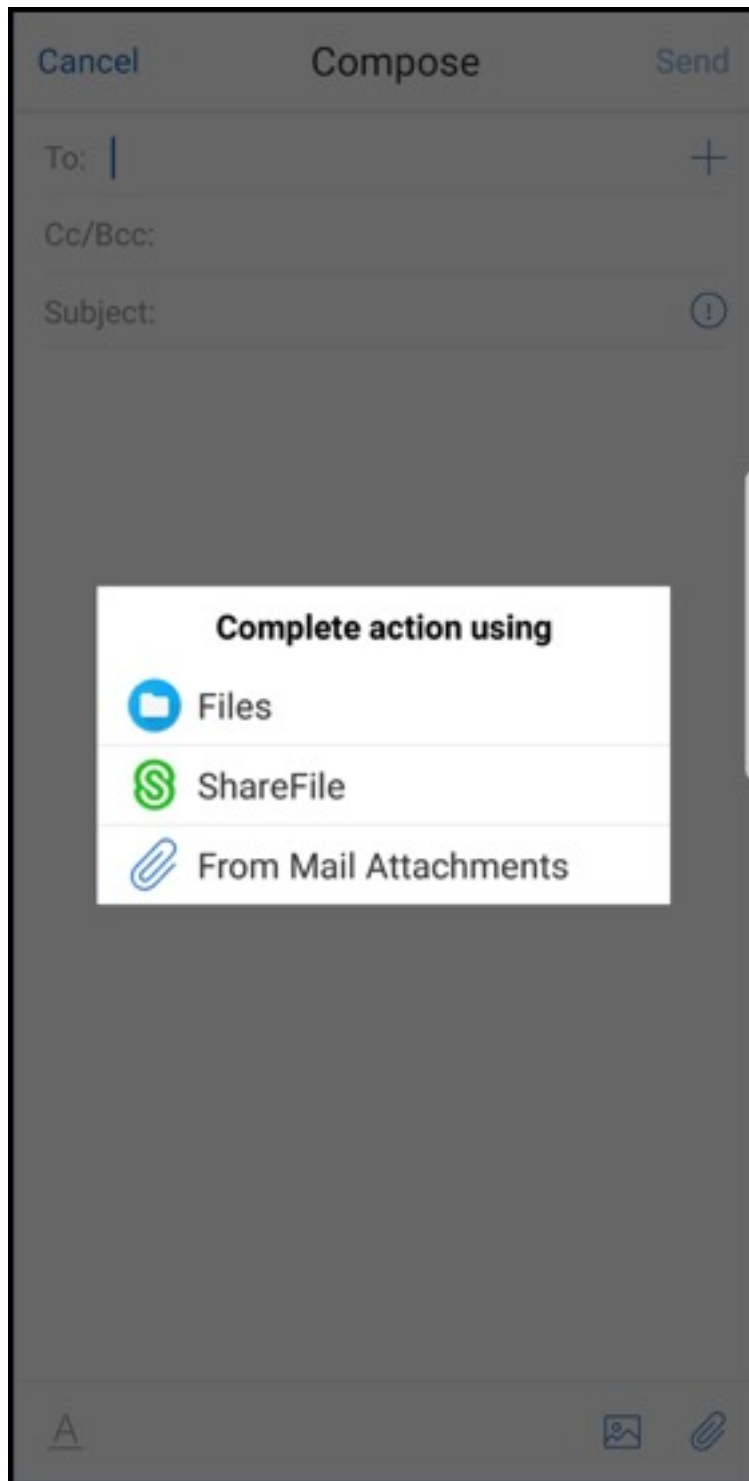


메모:

첨부 파일 아이콘을 누르면 다음 옵션이 나타납니다.

- Files

- ShareFile(현재 Citrix Files)
- 메일 첨부



전자 메일을 보는 동안 **Secure Mail** 이 포함된 리소스를 렌더링합니다

이미지 URL 이 내부 링크인 메일과 같이, 리소스가 내부 네트워크에 있는 경우 **Secure Mail** 은 내부 네트워크에 연결하여 콘텐츠를 가져오고 렌더링합니다.

최신 인증 지원

최신 인증은 사용자 이름 및 암호와 함께 OAuth 토큰 기반 인증을 적용합니다. 이 지원에는 Office 365 의 내부 및 외부 AD FS(Active Directory Federation Services) 또는 IdP(ID 공급자) 지원이 포함됩니다.

Secure Mail 에 대해 **Secure Web** 도메인 MDX 정책 허용

Secure Mail에서는 몇몇 외부 URL 을 **Secure Web** 이 아닌 기본 브라우저에 열어야 합니다. 따라서 모든 URL 은 기본적으로 기본 브라우저에서 열립니다. 그러나 **Secure Web** 에서 열고자 하는 특정 URL 의 목록을 만들 수 있습니다. 이렇게 하려면 Citrix Endpoint Management 콘솔에서 허용된 **Secure Web** 도메인이라는 이름의 MDX 정책을 구성합니다.

정책을 배포하면 심표로 구분된 URL 호스트 도메인 목록에서 응용 프로그램이 일반적으로 외부 처리기로 보내는 URL 의 호스트 이름 일부와 일치하는 호스트 도메인을 찾습니다. 일반적으로 관리자는 이 정책을 **Secure Web** 의 내부 도메인 목록으로 구성하여 처리합니다.

정책을 비워 두면 기본 설정으로 유지되고 필터링에서 명시적으로 URL 을 제외하거나 URL 을 리디렉션할 때까지 모든 웹 트래픽이 **Secure Web** 으로 전송됩니다. URL 을 리디렉션하려면 도메인 MDX 정책에 대해 URL 제외 필터를 구성합니다. 이 정책은 URL 을 기본 브라우저에서 열어야 함을 나타냅니다. 이 정책은 **Secure Web** 도메인 정책보다 우선합니다.

이러한 MDX 정책은 Android 및 iOS 에 대해 구성할 수 있습니다.

Secure Web 도메인 정책 구성의 예

다음 절차는 Android 용 **Secure Mail** 에서 기본 Chrome 브라우저 또는 **Secure Web** 을 사용하여 URL 을 열라는 메시지를 사용자에게 표시하는 방법을 보여줍니다. iOS 에서 이 단계는 일반적으로 Safari 브라우저에서 열리는 URL 이 자동으로 **Secure Web** 에서 열릴 수 있음을 보여줍니다.

Android 용 **Secure Mail** 의 경우

1. 앱 상호 작용 정책 목록의 제한된 열기 제외 목록에 `{package=com.android.chrome}` 을 입력합니다.
2. 앱 상호 작용 (아웃바운드 URL) 정책 목록의 **Secure Web** 도메인 허용에서 내부 사이트의 DNS 접미사를 추가합니다.

다른 타사 브라우저의 경우 다음 형식을 적절히 사용합니다.

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

iOS 용 Secure Mail 의 경우

1. 앱 상호 작용 (아웃바운드 URL) 정책 목록의 허용된 **URL** 에서 +^safari: 를 추가합니다.
2. 앱 **URL** 구성표에서 safari: 를 추가합니다.
3. **Secure Web** 도메인 허용에서 내부 사이트의 DNS 접미사를 추가합니다.

Secure Mail 과 Slack 통합

November 19, 2021

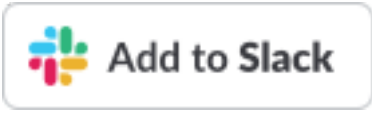
Citrix Secure Mail and its integration with Slack is not created by, affiliated with, or supported by Slack Technologies, Inc.

이제 iOS 또는 Android 를 실행하는 장치에서 전자 메일 대화를 Slack 앱으로 보낼 수 있습니다.

이 기능을 사용하면 다음을 수행할 수 있습니다.

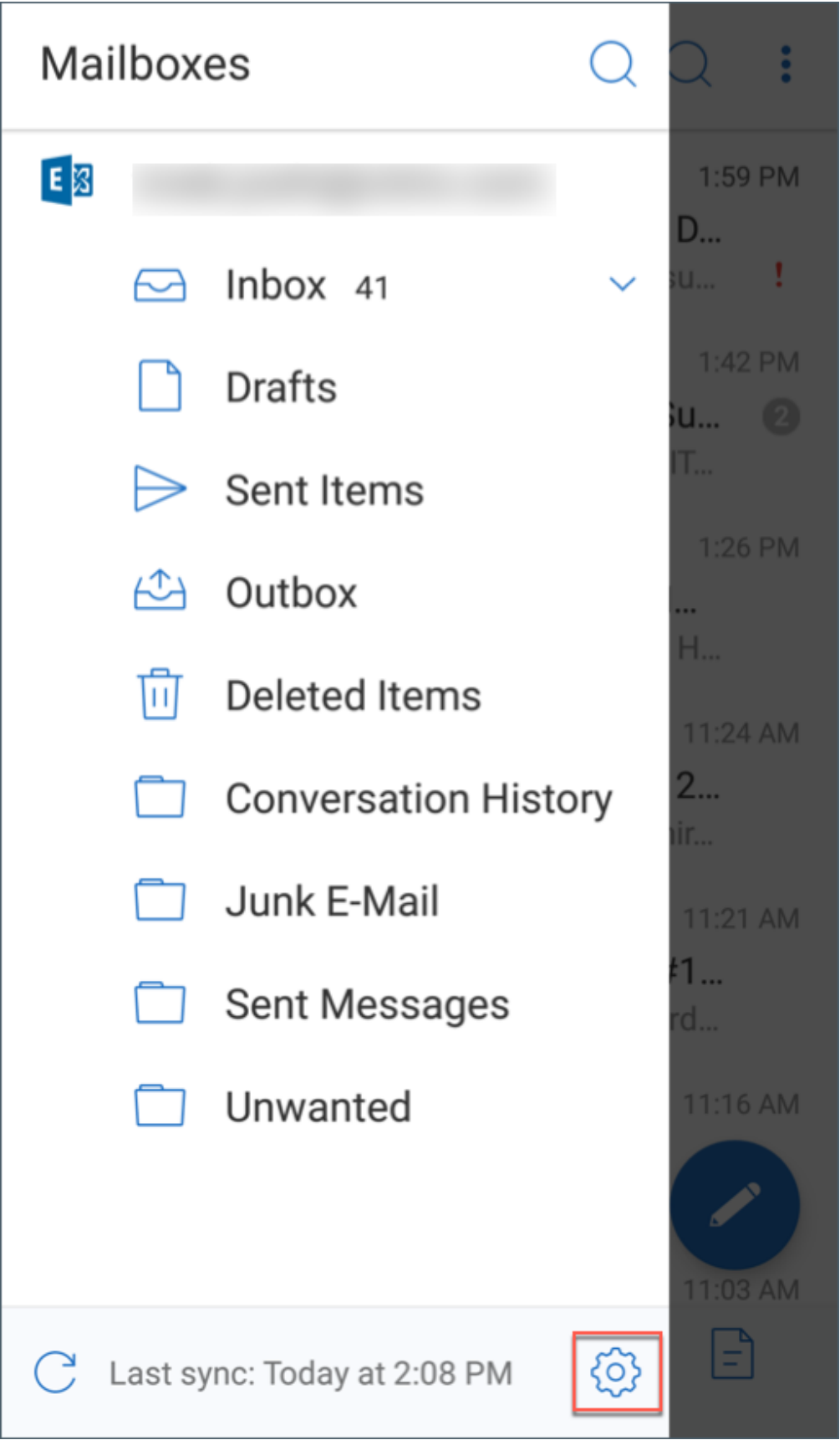
- 전자 메일을 Slack 대화로 원활하게 전환합니다.
- 전자 메일 받는 사람이 참여하는 Slack 그룹 대화를 만듭니다.
- Slack 에서 전자 메일 받는 사람에게 보낼 직접 메시지를 만듭니다.

사전 요구 사항

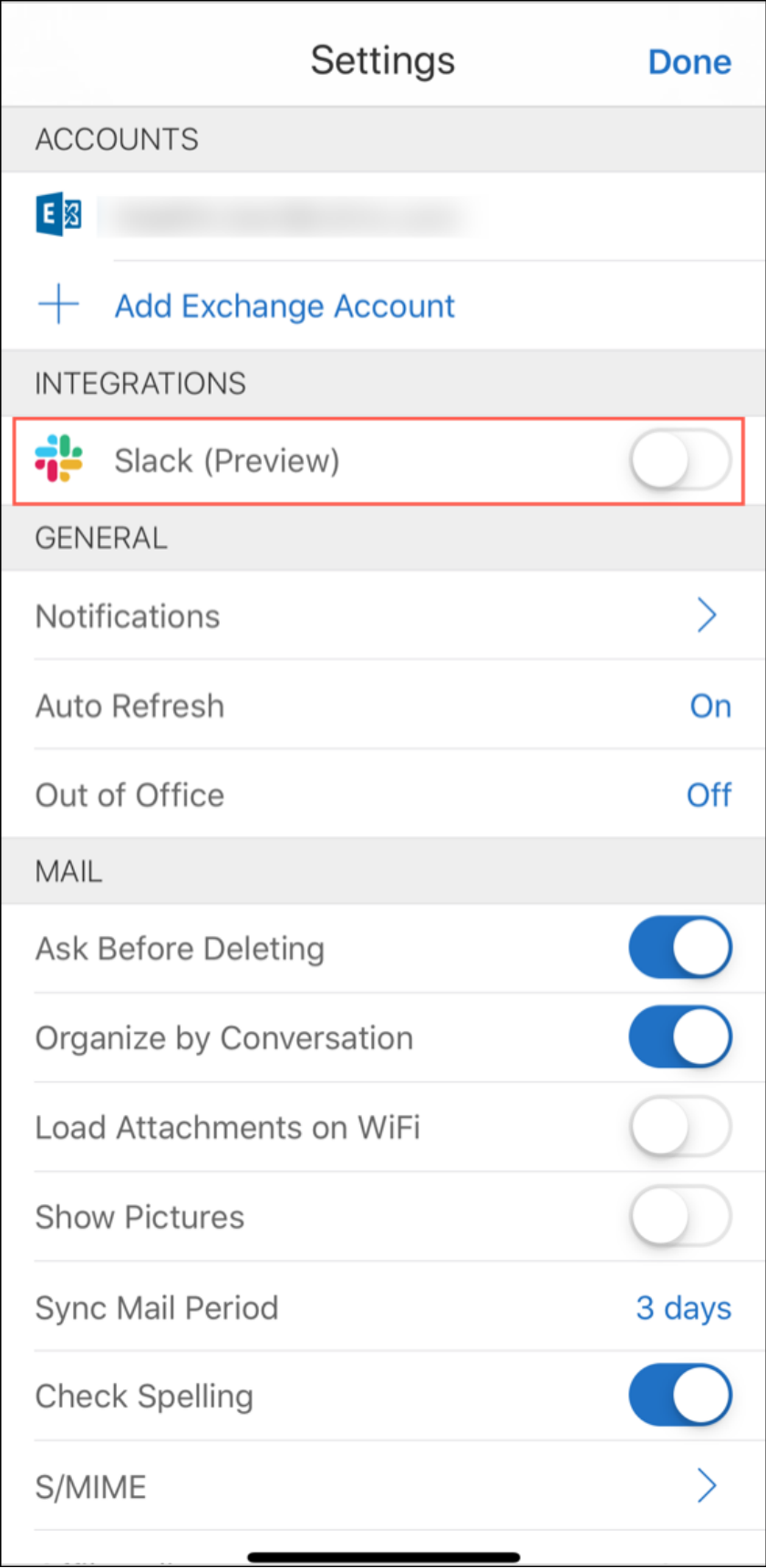
- 관리자:
 - Slack 작업 공간에 Secure Mail 이 설치되었는지 확인합니다. 아래 **Add to Slack(Slack 에 추가)** 단추를
 클릭합니다.
 - **Enable Slack(Slack 사용)** 정책이 켜짐으로 설정되어 있는지 확인합니다. 정책에 대한 자세한 내용은 다음을 참조하십시오.
 - * [iOS 에 Slack 정책 사용](#)
 - * [Android 에 Slack 정책 사용](#)
- 사용자: 계속하기 전에 Slack 계정이 있고 Slack 앱이 장치에 설치되었는지 확인합니다.

장치에서 이 기능을 사용하려면

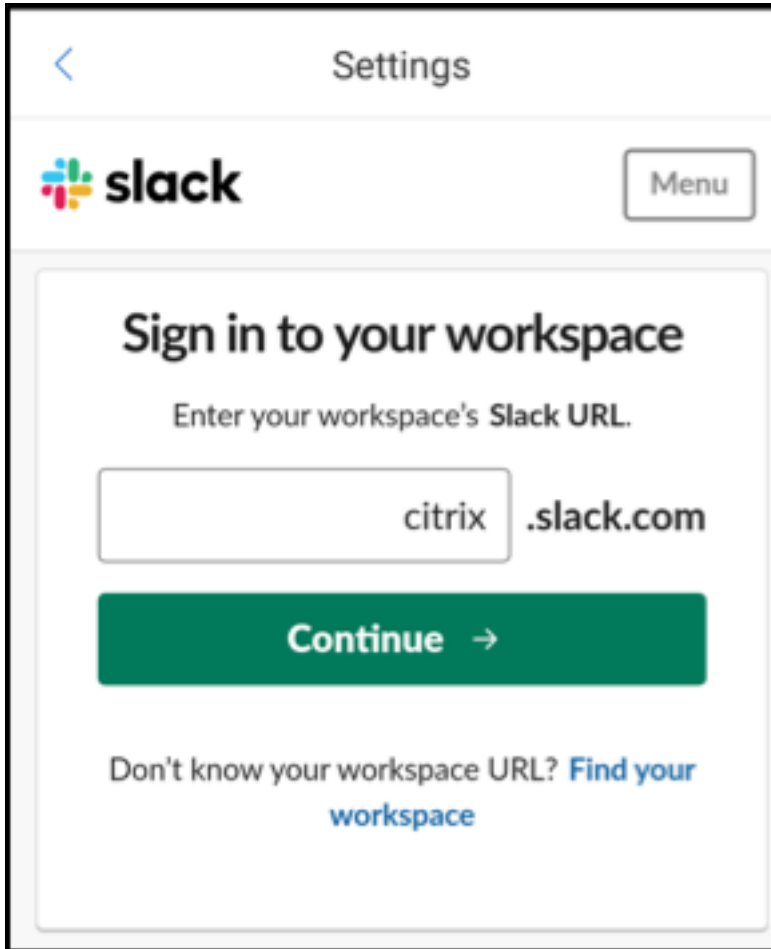
1. Secure Mail 을 열고 햄버거 아이콘을 누릅니다.
2. **Mailboxes(사서함)** 화면에서 화면 오른쪽 아래의 설정 아이콘을 누릅니다.



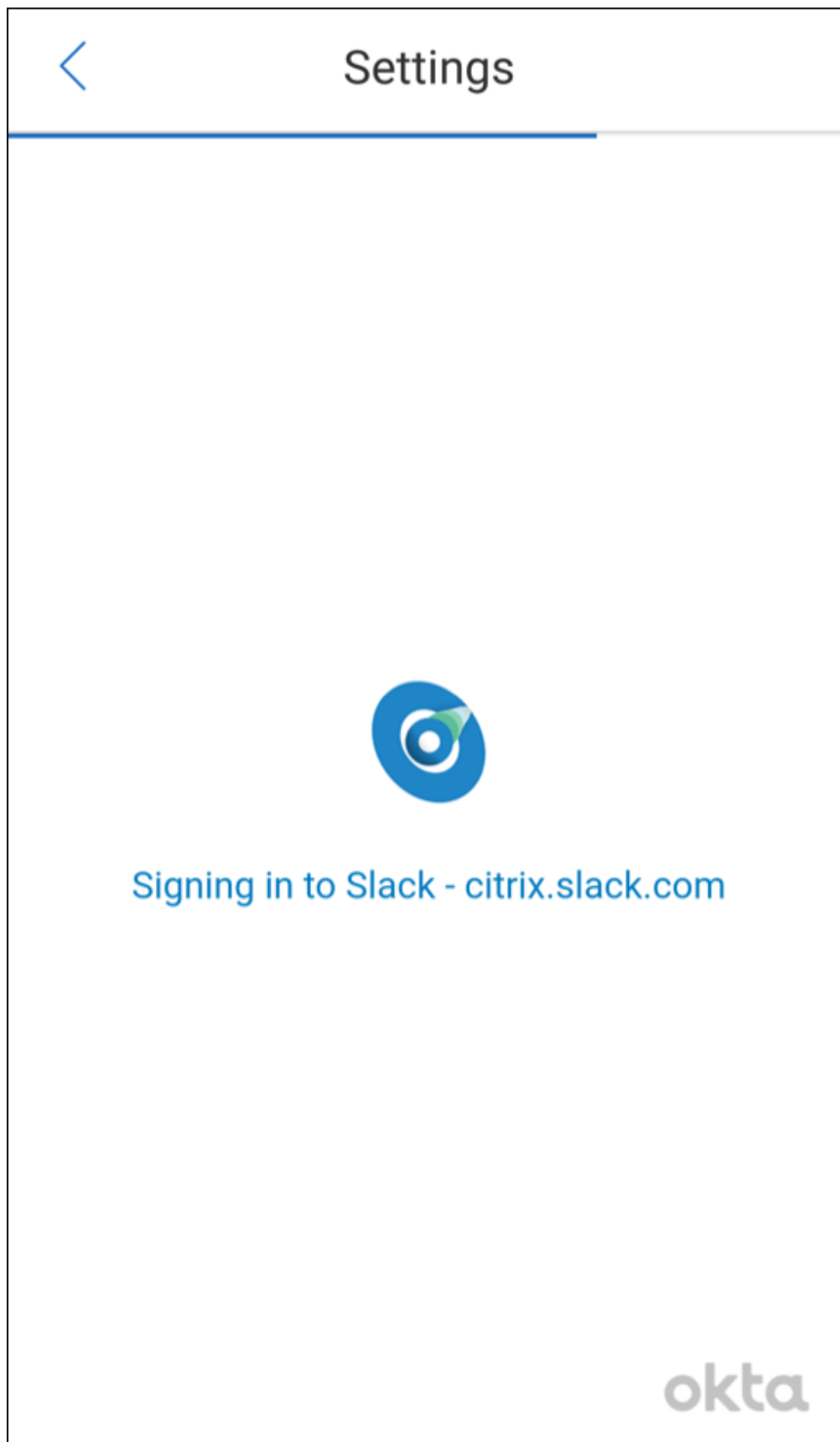
3. **Settings**(설정) 화면에서 **Integrations**(통합) 아래에 나열된 **Slack** 을 누릅니다.



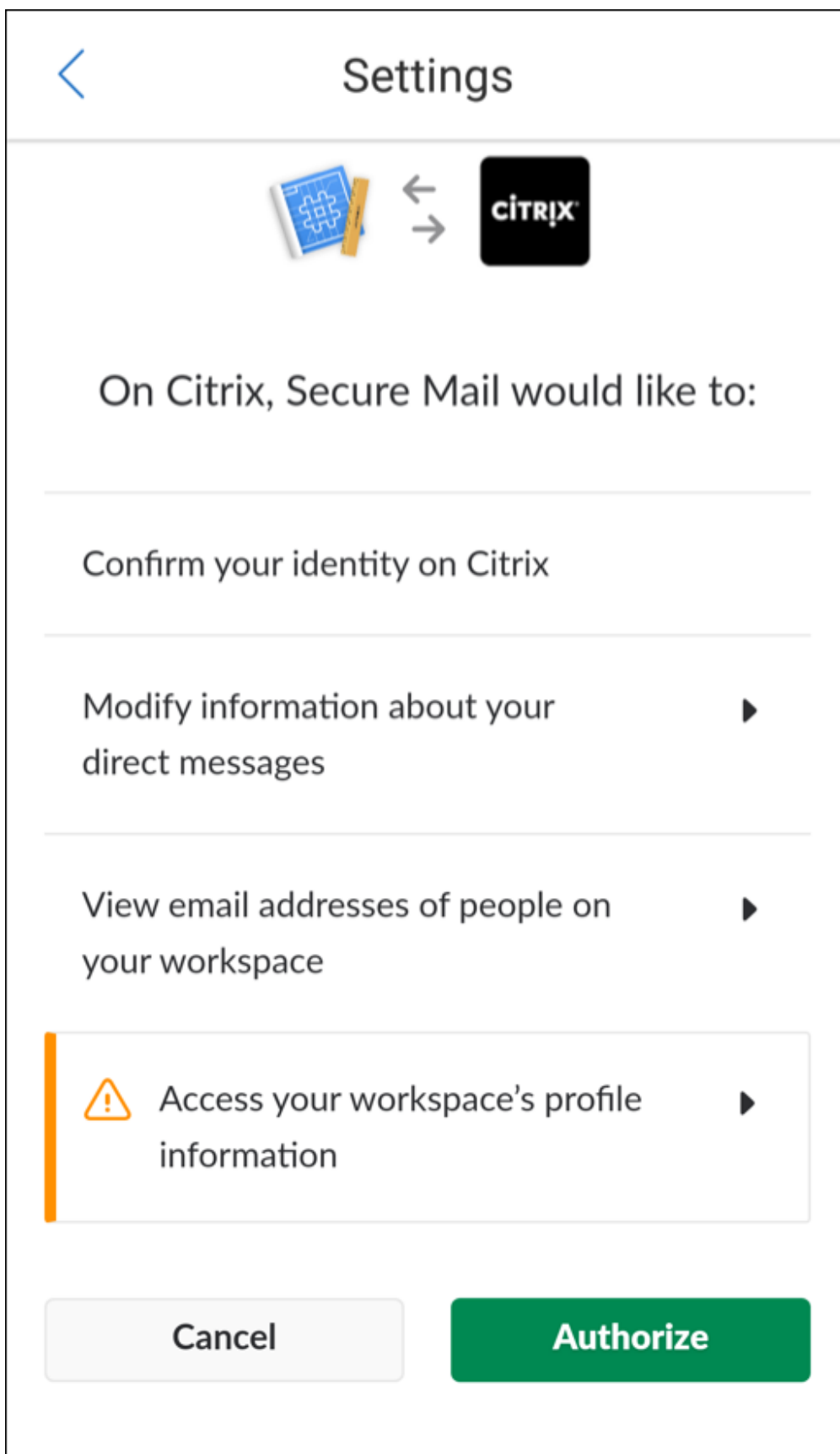
4. 작업 공간 Slack URL 을 제공하고 **Continue**(계속) 를 누릅니다.

A screenshot of the Slack mobile app's 'Sign in to your workspace' screen. The screen is titled 'Settings' at the top. Below the title is the Slack logo and a 'Menu' button. The main heading is 'Sign in to your workspace'. Below this, it says 'Enter your workspace's Slack URL.' There is a text input field containing 'citrix' and a label '.slack.com' to its right. Below the input field is a large green button with the text 'Continue →'. At the bottom, it says 'Don't know your workspace URL? Find your workspace' with 'Find your workspace' in blue text and a link icon.

5. 자격 증명을 제공하고 **Sign In**(로그인) 을 누릅니다.



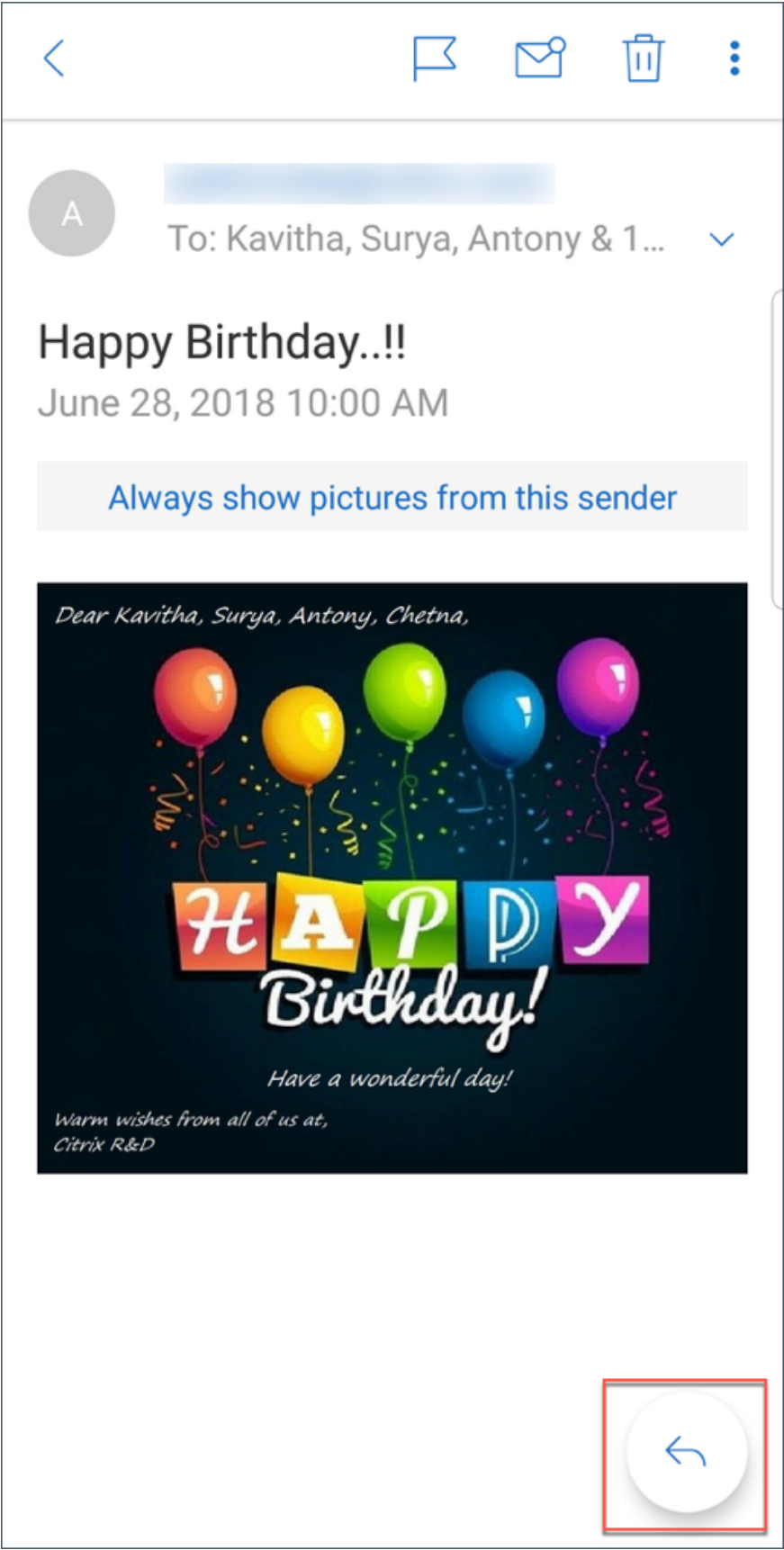
6. Secure Mail 에 정보 액세스를 위한 권한을 부여하라는 메시지가 표시되면 **Authorize(승인)** 를 누릅니다.



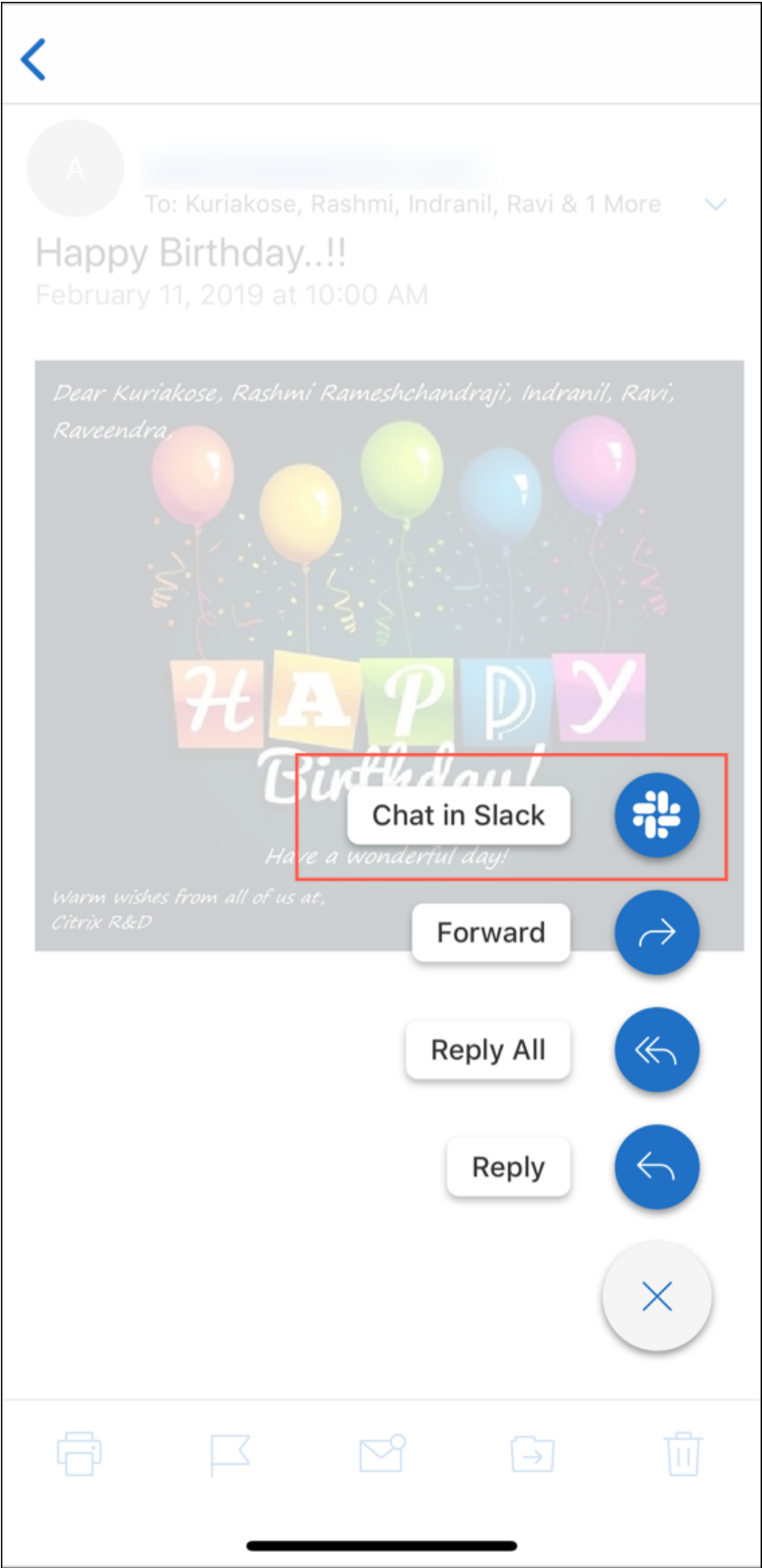
이제 Slack 에 연결되었습니다.

이 기능을 사용하려면

1. Secure Mail 에서 전자 메일 대화를 열고 부동 동작 단추를 누릅니다.



2. 사용 가능한 옵션 중에서 **Chat in Slack(Slack** 에서 채팅) 을 누릅니다.



3. 전자 메일의 받는 사람을 사용하여 대화가 Slack 으로 전환됩니다.



다음 사항에 유의하십시오.

- iOS 또는 Android 용 Secure Mail 을 실행하는 장치에서 최대 8 명의 전자 메일 받는 사람이 참여하는 Slack 대화를 만들 수 있습니다. 전자 메일의 받는 사람이 8 명을 초과하는 경우 Secure Mail 은 기본적으로 전자 메일 대화에 포함된 처음 8 명을 선택합니다.

알림 및 동기화

December 10, 2021

이 문서에서는 Secure Mail 의 알림 및 전자 메일 동기화 기능과 구성에 대해 설명합니다.

iOS 용 Secure Mail 백그라운드 앱 새로 고침

APNs 가 아니라 iOS 백그라운드 앱 새로 고침을 통해 알림을 제공하도록 iOS 용 Secure Mail 이 구성된 경우, Secure Mail 전자 메일 새로 고침은 다음과 같은 방식으로 작동됩니다.

- 사용자가 장치의 설정 메뉴에서 백그라운드 앱 새로 고침을 사용하도록 설정하고 Secure Mail 이 백그라운드에서 실행 중이면 메일이 서버와 동기화됩니다. 동기화 빈도는 다양한 요인에 따라 달라집니다.
- 사용자가 백그라운드 앱 새로 고침이 사용되지 않도록 설정하면 앱은 백그라운드에서 실행 중인 동안 전자 메일을 전혀 받지 않습니다.
- 사용자가 Secure Mail 을 백그라운드로 전환하면 앱은 일시 중단되기 전에 유예 기간 내에서 계속 실행됩니다.
- 포그라운드에서 실행 중인 동안 Secure Mail 은 백그라운드 앱 새로 고침 설정과 상관없이 실시간 전자 메일 활동을 표시합니다.

Secure Mail 및 ActiveSync

Secure Mail 은 ActiveSync 메시징 프로토콜을 통해 Exchange Server 와 동기화됩니다. 이 기능은 사용자에게 Outlook 메일, 연락처, 일정 이벤트, 자동으로 생성된 사서함 및 사용자가 생성한 폴더에 대한 실시간 액세스를 제공합니다.

참고:

ActiveSync 는 Exchange 공용 폴더 동기화를 지원하지 않습니다. Exchange Server 2013 의 경우, ActiveSync 가 임시 보관함 폴더를 동기화하지 않습니다.

사용자가 생성한 폴더를 동기화하려면 다음 단계를 따르십시오.

iOS

1. 설정 > 자동 새로 고침으로 이동합니다.

2. 자동 새로 고침을 켜짐으로 설정합니다.
3. 켜짐을 누릅니다. 모든 사서함의 목록이 나타납니다.
4. 동기화하려는 폴더를 누릅니다.

Android

1. 사서함 목록으로 이동합니다.
2. 동기화하려는 사서함을 누릅니다.
3. 오른쪽 위 모서리에서 자세히 아이콘을 클릭합니다.
4. 동기화 옵션을 누릅니다.
5. 확인 빈도 아래에서 폴더 동기화 빈도를 선택합니다.

Secure Mail 에서 연락처 내보내기

Secure Mail 사용자는 연락처를 주소록과 지속적으로 동기화할 수 있습니다. 주소록으로 개별 연락처 일회성 내보내기를 수행하거나 연락처를 vCard 첨부 파일로 공유합니다.

이러한 기능을 허용하려면 Endpoint Management 콘솔에서 Secure Mail 에 대해 연락처 내보내기 정책을 켜짐으로 설정합니다.

정책이 켜짐으로 설정되어 있으면 다음과 같은 옵션을 Secure Mail 에서 사용할 수 있게 됩니다.

- 설정에 있는 로컬 연락처와 동기화
- 개별 연락처 내보내기
- vCard 첨부 파일로 연락처 공유

연락처 내보내기 정책이 꺼짐으로 설정되어 있으면 이러한 옵션은 앱에서 나타나지 않습니다.

이 정책을 사용하도록 설정한 후에 메일 서버에서 주소록으로 연락처가 지속적으로 동기화되도록 하려면 사용자가 로컬 연락처와 동기화를 켜짐으로 설정해야 합니다. 로컬 연락처와 동기화가 켜짐이면 Exchange 또는 Secure Mail 에서 연락처가 업데이트 될 때 로컬 연락처도 업데이트됩니다.

Android 제한 사항으로 인해 Exchange 또는 Hotmail 계정이 로컬 연락처와 동기화되도록 이미 설정된 경우 Secure Mail 은 연락처를 동기화할 수 없습니다.

iOS 에서는 Secure Mail 연락처를 내보내고 전화 연락처와 동기화할 수 있습니다. 사용자가 장치에서 Hotmail 또는 Exchange 를 설정한 경우에도 연락처를 내보내고 동기화할 수 있습니다. 이 기능은 Endpoint Management 에서 Override Native Contacts Check policy for Secure Mail(Secure Mail 에 대한 기본 연락처 확인 정책 재정의) 을 통해 구성합니다. 이 정책은 Secure Mail 이 기본 연락처 앱에 구성된 Exchange/Hotmail 계정의 연락처에 대한 확인을 재정의할지 여부를 결정합니다. 이 정책이 켜짐이면 기본 연락처 앱에 Exchange/Hotmail 계정이 구성된 경우에도 앱이 연락처를 장치에 동기화합니다. 꺼짐이면 앱이 계속 연락처 동기화를 차단합니다. 기본값은 켜짐입니다.

제한 사항:

로컬 연락처와 동기화를 사용하도록 설정하면 기본 연락처 폴더만 동기화됩니다. 하위 폴더는 동기화된 연락처에 포함되지 않습니다.

Secure Mail 알림

다음 표에는 Secure Mail 이 포그라운드 또는 백그라운드에서 실행 중일 때 지원되는 모바일 장치에서 알림이 어떻게 처리되는 지가 나열되어 있습니다.

Secure Mail 이 포그라운드 또는 백그라운드에서 실행 중인 경우		
	알림이 iOS 에 대해 처리됨	알림이 Android 에 대해 처리됨
포그라운드	Secure Mail 이 전자 메일 및 일정 활동을 동기화하기 위해 지속적인 ActiveSync 연결을 유지합니다.	Secure Mail 이 전자 메일 및 일정 활동을 동기화하기 위해 지속적인 ActiveSync 연결을 유지합니다.
백그라운드 또는 종료됨	Secure Mail 이 iOS 백그라운드 앱 새로 고침을 통해 또는 APNs(구성된 경우)를 통해 알림을 받습니다.	Secure Mail 이 지속적인 ActiveSync 연결을 유지합니다.

구성에 대한 자세한 내용은 [iOS 용 Secure Mail 을 위한 푸시 알림](#)을 참조하십시오.

Secure Mail 을 위한 푸시 알림

February 27, 2024

iOS 및 Android 용 Secure Mail 은 앱이 백그라운드에서 실행되거나 닫힐 때 전자 메일 및 일정 활동에 대한 알림을 받을 수 있습니다. iOS 용 Secure Mail 은 APNs(Apple 푸시 알림 서비스)를 통해 제공되는 원격 푸시 알림을 지원합니다. Android 용 Secure Mail 은 FCM(Firebase Cloud Messaging) 서비스를 통해 제공되는 알림을 지원합니다.

푸시 알림 작동 방식

iOS 및 Android 에서 푸시 알림을 제공하기 위해 Citrix 는 AWS(Amazon Web Services)에서 수신기 서비스를 호스팅하여 다음과 같은 기능을 수행합니다.

- 받은 편지함 활동이 있을 때 Exchange Server 가 보내는 EWS(Exchange 웹 서비스) 푸시 알림을 수신합니다. Exchange 는 어떠한 메일 콘텐츠도 Citrix 서비스로 보내지 않습니다.
개인 식별 정보는 Citrix 서비스에 의해 저장되지 않습니다. 대신, 장치 토큰 및 구독 ID 식별자를 통해 Secure Mail 내에서 업데이트될 특정 장치 및 받은 편지함 폴더가 식별됩니다.
- 배지 카운트만 포함하는 APNs 알림을 iOS 장치의 Secure Mail 로 보냅니다.

- FCM 알림을 Android 장치의 Secure Mail 로 보냅니다.

Citrix 수신기 서비스는 메일 데이터 트래픽에 영향을 미치지 않으므로 메일 데이터 트래픽은 ActiveSync 를 통해 사용자 장치와 Exchange Server 간에 계속 흘러갑니다. 고가용성 및 재해 복구를 위해 구성된 수신기 서비스는 세 지역에서 사용 가능합니다.

- 아메리카
- EMEA(유럽, 중동 및 아프리카)
- APAC(아시아 태평양)

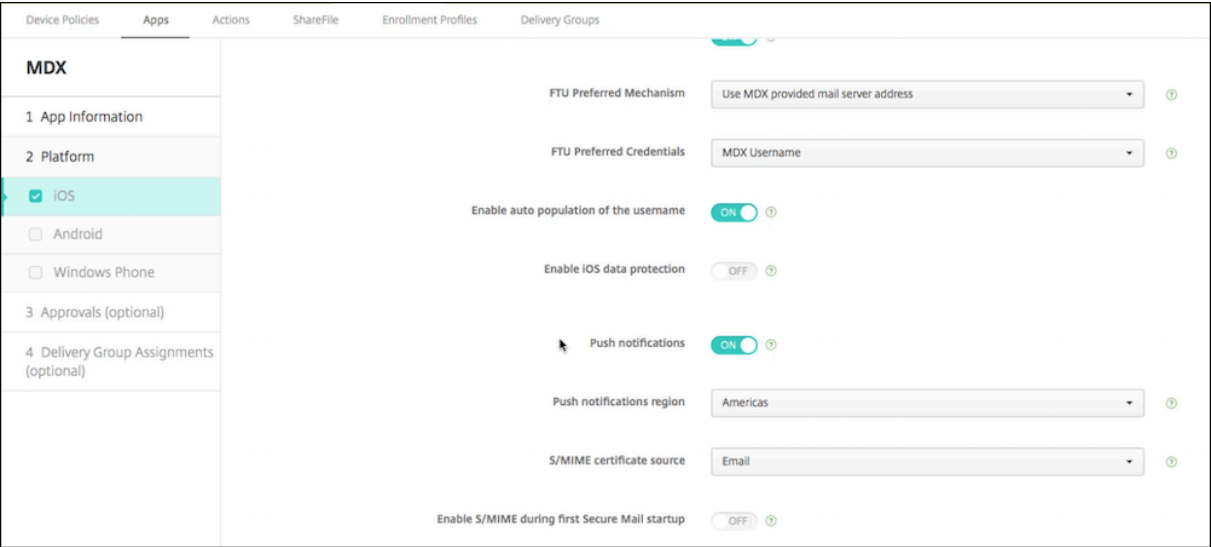
푸시 알림 시스템 요구 사항

Citrix Gateway 구성이 STA(Secure Ticket Authority) 를 포함하고 분할 터널링이 꺼져 있으면 Citrix Gateway 는 (Secure Mail 에서 터널링되는 경우) 다음 Citrix 수신기 서비스 URL 로의 트래픽을 허용해야 합니다.

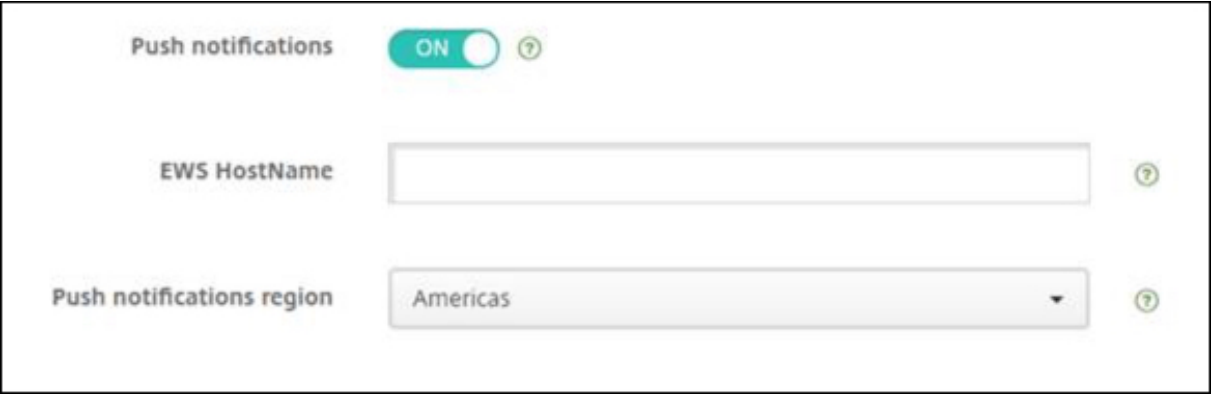
지역	URL	IP 주소
아메리카	https://us-east-1.pushreg.xm.citrix.com	52.7.65.6; 52.7.147.0
EMEA	https://eu-west-1.pushreg.xm.citrix.com	54.154.200.233; 54.154.204.192
APAC	https://ap-southeast-1.pushreg.xm.citrix.com	52.74.236.173; 52.74.25.245

푸시 알림을 위한 **Secure Mail** 구성

앱 스토어 배포를 위해 Secure Mail 에 대한 Apple 푸시 알림 또는 FCM 을 설정하려면 Endpoint Management 콘솔에서 푸시 알림을 커짐으로 설정한 다음 지역을 선택하십시오. 다음 그림에서는 iOS 의 설정을 보여 줍니다.



Android 의 경우 iOS 와 동일한 푸시 알림 설정은 다음 그림과 같습니다. 또한 EWS 가 메일 서버가 상주하는 지역과 다른 지역에서 호스팅되는 경우 **EWS** 호스트 이름 설정을 완료합니다. 기본 설정은 비어 있습니다. 설정을 빈 상태로 두면 Endpoint Management 에서 메일 서버의 호스트 이름을 사용합니다.



트래픽이 수신기 서비스로 흐를 수 있도록 Exchange 및 Citrix ADC 를 구성합니다.

Exchange Server 구성

Exchange Server 가 위치하는 지역에 대해 방화벽에서 Citrix 수신기 서비스 URL 로의 아웃바운드 SSL(포트 443) 을 허용합니다. 예:

지역	URL	IP 주소
아메리카	https://us-east-1.mailboxlistener.xml.citrix.com	52.6.252.176; 52.4.180.132

지역	URL	IP 주소
EMEA	https://eu-west-1.mailboxlistener.xml.citrix.com	54.77.174.172; 52.17.147.220
APAC	https://ap-southeast-1.mailboxlistener.xml.citrix.com	52.74.231.240; 54.169.87.20

EWS(Exchange 웹 서비스) 와 Citrix 수신기 장치 사이에 프록시 서버가 있는 경우 다음 중 하나를 수행할 수 있습니다.

- 프록시를 통해 수신기 장치로 EWS 트래픽을 보냅니다.
- 프록시를 우회하여 수신기 장치로 직접 향하도록 EWS 트래픽의 경로를 지정합니다.

프록시 서버를 통해 EWS 트래픽을 보내려면 ClientAccess\exchweb\ews 폴더에 있는 EWS web.config 파일을 다음과 같이 구성합니다.

```

1 <configuration>
2 <system.net>
3 <defaultProxy>
4 <proxy usesystemdefault="true" bypassonlocal="true" />
5 </defaultProxy>
6 </system.net>
7 </configuration>

```

프록시 구성에 대한 자세한 내용은 [프록시 구성](#)을 참조하십시오.

Exchange 2013 환경의 경우 [system.net](#) 섹션을 web.config 파일에 수동으로 추가해야 합니다. 그렇지 않으면 이 문서에서 설명한 구성이 Exchange 2013 에 적용됩니다. 문제를 해결하려면 Exchange 관리자에게 문의하십시오.

프록시 서버를 우회하려면 Exchange 에서 Citrix 수신기 서비스에 연결할 수 있도록 우회 목록을 구성합니다.

Secure Hub 가 인증서 기반 인증으로 등록되면 Exchange Server 를 인증서 기반 인증에 맞게 구성해야 합니다. 자세한 내용은 [Endpoint Management 고급 개념](#) 문서를 참조하십시오.

Citrix Gateway 구성

Exchange Server 는 수신기 서비스로의 트래픽을 허용해야 하지만 Citrix ADC 는 등록 서비스로의 트래픽을 허용해야 합니다. 이러한 방식으로 장치가 푸시 알림에 등록하기 위해 연결할 수 있습니다.

EWS 서버와 ActiveSync 서버가 서로 다른 경우, EWS 트래픽을 허용하도록 Citrix ADC 트래픽 정책을 구성합니다. Citrix Endpoint Management 와 Citrix Gateway 의 통합에 대한 자세한 내용은 [Citrix Gateway 및 Citrix ADC 의 통합](#) 섹션을 참조하십시오.

문제 해결

아웃바운드 연결 문제를 해결하려면 구독 요청 또는 구독 알림이 올바르게 작동하거나 실패할 경우에 로그 항목을 포함하는 Exchange 이벤트 로그를 살펴봅니다. 또한 Exchange Server 에서 Wireshark 추적을 실행하여 Citrix 수신기 서비스로의 아웃바운드 트래픽을 추적할 수 있습니다.

Secure Mail 푸시 알림 FAQ

언제 **Android** 가 **Secure Mail** 에 알림을 제공합니까

Android 에서는 알림이 항상 Secure Mail 에 제공됩니다.

FCM 은 잠금 화면에 나타나는 전자 메일 알림에 어떤 영향을 미칩니까

장치의 잠금 화면에 나타나는 새 메일 알림은 Secure Mail 에 의해 장치에 동기화되는 데이터를 기반으로 생성됩니다. 이 정보가 수신기 서비스로부터 제공되는 것이 아니라는 점에 유의하십시오.

새 메일 알림을 표시하려면 Secure Mail 이 알림 생성에 사용 가능한 정보를 갖기 위해 Exchange 로부터 데이터를 동기화할 수 있어야 합니다.

새 메일을 받은 경우 새 메시지가 있습니다라는 FCM 알림이 나타납니다. 백그라운드에서 전자 메일 동기화가 완료되면 새 메일이 Secure Mail 에 표시됩니다.

APNs 는 잠금 화면에 나타나는 전자 메일 알림에 어떤 영향을 미칩니까

장치의 잠금 화면에 나타나는 새 메일 알림은 Secure Mail 에 의해 장치에 동기화되는 데이터를 기반으로 생성됩니다. 이 정보가 수신기 서비스로부터 제공되는 것이 아니라는 점에 유의하십시오.

새 메일 알림을 표시하려면 Secure Mail 은 알림 생성에 사용 가능한 정보를 갖기 위해 Exchange 로부터 데이터를 동기화할 수 있어야 합니다.

APNs 알림이 백그라운드의 Secure Mail 에 제공되지 않는 경우, Secure Mail 은 알림을 감지하지 못하고 따라서 새 데이터를 동기화하지 못합니다. 새 데이터를 Secure Mail 에서 사용할 수 없기 때문에 APNs 알림이 제공되지 않더라도 장치 잠금 화면에서 전자 메일 알림이 생성되지 않습니다.

백그라운드 앱 새로 고침이 **Secure Mail** 및 **APNs** 에 어떤 영향을 미칩니까

사용자가 백그라운드 앱 새로 고침을 끄면 다음과 같은 상황이 발생합니다.

- Secure Mail 이 백그라운드 앱인 경우 Secure Mail 은 알림을 받지 않습니다.

참고:

이 상황은 다양한 방식의 푸시 알림이 비활성화되어 있는 경우에만 발생합니다. 다양한 방식의 푸시 알림에 대한 자세한 내용은 [iOS 용 Secure Mail 을 위한 다양한 방식의 푸시 알림](#)을 참조하십시오.

- Secure Mail 이 잠금 화면을 새 전자 메일 알림으로 업데이트하지 않습니다.

백그라운드 앱 새로 고침을 사용하지 않도록 설정하면 Secure Mail 의 동작에 큰 영향을 미칩니다. 앞에서 언급했듯이 APNs 에 기반한 배지 업데이트는 계속 발생하지만, 이 모드에서는 전자 메일이 장치에 동기화되지 않습니다.

절전 모드가 **Secure Mail** 및 **APNs** 에 어떤 영향을 미칩니까

절전 모드에서 Secure Mail 과 관련된 시스템의 동작은 백그라운드 앱 새로 고침을 사용하지 않도록 설정한 경우의 동작과 동일합니다. 절전 모드에서 장치는 주기적인 새로 고침을 위해 앱을 활성화하지 않으며, 백그라운드의 앱에게 알림을 제공하지 않습니다. 따라서 부작용은 위의 백그라운드 앱 새로 고침 섹션에 나열된 것과 동일합니다. 절전 모드에서도 배지는 APNs 알림에 기반하여 계속 업데이트됩니다.

백그라운드에서 **FCM** 기반 동기화 실패를 유도할 수 있는 다른 문제로는 무엇이 있습니까

다음은 비롯한 다양한 문제로 인해 FCM 기반 동기화 요청이 실패할 수 있습니다.

- 유효하지 않은 STA 티켓
- Secure Mail 이 doze 모드에서 활성화된 경우, 이 앱은 10 초간 서버로부터 모든 데이터를 동기화합니다.

위에서 언급한 상태 중 하나가 발생하면 Secure Mail 이 데이터를 동기화할 수 없습니다. 따라서 잠금 화면에 알림이 표시되지 않습니다.

백그라운드에서 **APNs** 기반 동기화가 실패하도록 할 수 있는 다른 문제로 무엇이 있습니까

다음과 같은 여러 가지 문제로 인해 APNs 기반 동기화 요청이 실패할 수 있습니다.

- 유효하지 않은 STA 티켓
- 느린 네트워크 연결 Secure Mail 이 백그라운드에서 활성화된 경우, 이 앱은 30 초간 서버로부터 모든 데이터를 동기화합니다.
- 데이터 보호 정책을 사용하도록 설정되어 있고 APNs 알림에 의해 Secure Mail 이 활성화된 경우, 장치가 잠겨 있으면 Secure Mail 에서 데이터 저장소에 액세스할 수 없고 동기화가 발생하지 않습니다. 이는 시스템에서 Secure Mail 콜드 시작을 시도하는 유일한 경우입니다. 사용자가 장치를 잠근 후 일정 시점에 Secure Mail 을 이미 시작한 경우, APNs 기반 동기화는 장치가 잠겨 있어도 성공합니다.

위에서 언급한 상태 중 하나가 발생하면 Secure Mail 은 데이터를 동기화할 수 없고 따라서 잠금 화면 알림을 표시할 수 없습니다.

알림이 제공되지 않거나 **APNs**가 사용 중이 아닐 때 **Secure Mail**에서 잠금 화면 알림을 생성하는 다른 방법은 무엇입니까

APNs를 사용하지 못하도록 설정한 경우에도 백그라운드 앱 새로 고침을 사용하도록 설정되어 있고 절전 모드가 꺼져 있으면 iOS로부터의 주기적인 백그라운드 앱 새로 고침 이벤트에 의해 **Secure Mail**이 활성화됩니다.

이러한 활성화 이벤트 중에 **Secure Mail**은 Exchange Server로부터 새 전자 메일을 동기화합니다. 이 새 전자 메일은 잠금 화면에서 전자 메일 알림을 생성하는 데 사용될 수 있습니다. 따라서 APNs 알림이 제공되지 않거나 APNs를 사용하지 않도록 설정한 경우, **Secure Mail**이 백그라운드에서 데이터를 동기화할 수 있습니다.

APNs가 사용 중일 때 그리고 APNs 알림이 **Secure Mail**로 제공될 때에 비해서는 실시간성이 떨어진다는 점에 유의해야 합니다. iOS가 APNs 알림을 **Secure Mail**로 라우팅하면 이 앱은 서버로부터 데이터를 즉시 동기화하고 잠금 화면 알림이 실시간으로 나타납니다.

백그라운드 앱 새로 고침 활성화가 필요한 경우 잠금 화면 알림은 실시간으로 발생하지 않습니다. 이 경우 **Secure Mail**은 일정 빈도로 활성화되고, 이 빈도는 전적으로 iOS가 결정합니다. 따라서 다음 두 상황 사이에 약간의 시간 차이가 발생할 수 있습니다.

- 전자 메일이 Exchange 사용자의 받은 편지함에 도착할 때
- **Secure Mail**에서 해당 메시지를 동기화하고 잠금 화면 알림을 생성할 때

APNs가 사용 중인 경우에도 **Secure Mail**이 이와 같이 주기적으로 활성화된다는 점에도 유의하십시오. 백그라운드 앱 새로 고침이 **Secure Mail**을 활성화하는 모든 경우에 **Secure Mail**은 Exchange로부터 데이터를 동기화하려고 시도합니다.

잠금 화면에 콘텐츠를 표시하는 다른 앱과 **Secure Mail**의 차이점은 무엇입니까

혼동하기 쉬운 중요한 차이점은 **Secure Mail**이 항상 실시간으로 잠금 화면에 새 전자 메일을 표시하지는 않는다는 것입니다. 이 동작은 Gmail, Microsoft Outlook 및 기타 앱과 다릅니다. 이러한 차이점의 주된 이유는 바로 보안입니다. 다른 앱의 동작에 맞게 조정하려면 Citrix 수신기 서비스에서 사용자 자격 증명을 사용하여 Exchange에 인증해야 합니다. 전자 메일 콘텐츠를 가져오려면 자격 증명도 필요합니다. 이 전자 메일 콘텐츠를 Citrix 수신기 서비스와 Apple APNs 서비스로 전달하는 데에도 자격 증명도 필요합니다. Citrix의 APNs 알림 접근 방식에서는 사용자 암호를 얻거나 저장하기 위해 Citrix 수신기 서비스가 필요하지 않습니다. 수신기 서비스는 사용자의 사서함 또는 암호에 액세스하지 않습니다.

네이티브 iOS 메일 앱에 대한 참고 사항: iOS는 자체 전자 메일 앱이 메일 서버와의 지속적인 연결을 유지할 수 있게 하여 알림이 항상 전달되도록 합니다. 네이티브 메일 이외의 타사 앱은 이 기능에 허용되지 않습니다.

Gmail 앱 동작: Gmail 앱 및 Gmail 서버는 Google에서 소유 및 통제합니다. 이 동작은 Google이 메시지 콘텐츠를 읽을 수 있고 해당 메시지 콘텐츠를 APNs 알림 페이로드에 포함할 수 있음을 의미합니다. iOS가 이 APNs 알림을 Gmail로부터 받으면 iOS는 다음을 수행합니다.

- 응용 프로그램 배지를 알림 페이로드에 지정된 값으로 설정합니다.
- 알림 페이로드에 포함된 메시지 텍스트를 사용하여 잠금 화면 알림을 표시합니다.

이는 중요한 차이점입니다. 페이로드에 포함된 데이터에 기반하여 잠금 화면 알림을 표시하는 것은 Gmail 앱이 아니라 iOS입니다. 실제로 iOS는 Gmail 앱을 전혀 활성화하지 않을 수 있고, 이는 알림 도착 시에 iOS가 **Secure Mail**을 활성화하지 않을

수 있는 것과 유사합니다. 한편 페이로드에 메시지 조각이 포함되어 있기 때문에 메일 데이터를 장치에 동기화하지 않아도 iOS 는 잠금 화면 알림을 표시할 수 있습니다.

Secure Mail 에서는 이 상황이 다릅니다. Secure Mail 이 잠금 화면 알림을 표시하려면 먼저 Secure Mail 앱이 Exchange 로부터 메시지 데이터를 동기화해야 합니다.

iOS 용 Outlook 앱 동작: iOS 용 Outlook 은 Microsoft 에서 통제합니다. 그러나 데이터를 가져오는 Exchange Server 를 제어하는 것은 사용자가 속해 있는 조직입니다. 이 설정에도 불구하고 Outlook 은 APNs 알림에서 Microsoft 가 제공하는 데이터에 기반하여 잠금 화면 알림을 표시할 수 있습니다. iOS 용 Outlook 에는 Microsoft 가 사용자 자격 증명을 저장하는 모델이 사용되기 때문입니다. Microsoft 는 클라우드 서비스에서 사용자의 사서함에 직접 액세스하고 새 메일이 있는지 확인합니다.

사용 가능한 새 메일이 있으면 Microsoft 클라우드 서비스는 새 메일 데이터를 포함하는 APNs 알림을 생성합니다. 이 모델은 Gmail 모델과 비슷한 방식으로 작동합니다. Gmail 모델에서는 iOS 가 단순히 데이터를 가져와 해당 데이터 기반으로 잠금 화면 알림을 생성합니다. Outlook iOS 앱은 이 프로세스에 관련되지 않습니다.

iOS 용 Outlook 에 대한 중요 보안 참고 사항: iOS 용 Outlook 접근 방식은 보안에 분명한 영향을 미칩니다. 조직에서는 사용자의 암호를 사용하여 Microsoft 를 신뢰해야 합니다. 이 신뢰를 통해 Microsoft 는 사용자의 사서함에 액세스할 수 있는데 이로 인해 보안 위험이 발생합니다.

푸시 알림의 관리자에 관한 추가적인 FAQ 는 이 [Support Knowledge Center 문서](#)를 참조하십시오. 사용자에게 관한 추가적인 FAQ 는 이 [Support Knowledge Center 문서](#)를 참조하십시오.

iOS 용 Secure Mail 에 대한 다양한 방식의 푸시 알림

December 10, 2021

iOS 용 Secure Mail 은 다양한 방식의 푸시 알림을 지원합니다. 다양한 방식의 알림을 통해 Secure Mail 이 백그라운드에서 실행 중이지 않을 때에도 받은 편지함에서 잠금 화면 알림을 받을 수 있습니다. 이 기능은 암호 기반 인증과 클라이언트 기반 인증 설정에서 지원됩니다.

참고:

이 기능을 지원하도록 아키텍처가 변경되어 VIP 전용 메일 알림 기능은 더 이상 사용할 수 없습니다.

서식 있는 푸시 알림 기능을 사용하려면 다음 사전 요구 사항을 충족해야 합니다.

- Endpoint Management 콘솔에서 푸시 알림을 켜짐으로 설정합니다.
- 네트워크 액세스 정책을 제한 없음 또는 내부 네트워크로 터널링됨으로 설정합니다. 네트워크 액세스 정책이 내부 네트워크로 터널링됨으로 설정된 경우 EWS(Exchange 웹 서비스) 호스트가 백그라운드 네트워크 서비스 정책에 구성되어 있어야 하며, EWS 와 ActiveSync 호스트가 동일한 경우 ActiveSync 호스트가 백그라운드 네트워크 서비스 정책에 구성되어 있어야 합니다.
- 잠금 화면 알림 제어 정책이 허용 또는 전자 메일 보낸 사람 또는 이벤트 제목으로 설정되어 있습니다.
- **Secure Mail > 설정 > 알림**으로 이동하여 메일 알림을 사용하도록 설정합니다.

다음 설정 중 하나를 실행하는 경우 이 기능이 지원되지 않습니다.

- Microsoft Office 365 를 통한 최신 인증
- Endpoint Management 의 Microsoft Intune/EMS 통합 기능을 통해 관리되는 앱
- 파생된 자격 증명을 사용하여 등록된 장치

Secure Mail iOS 에서 푸시 알림이 작동하는 방식

Secure Mail 은 다음과 같은 받은 편지함 작업에 대한 푸시 알림을 수신합니다.

- 새 메일, 미팅 요청, 미팅 취소, 미팅 업데이트: APNs 가 iOS Secure Mail 로 원격 알림을 푸시하면 Secure Mail 이 자동 새로 고침으로 표시된 모든 폴더를 업데이트합니다.

참고:

기본적으로 받은 편지함, 일정 및 연락처 폴더는 자동 새로 고침으로 표시됩니다. 사용자는 **Secure Mail > 설정 > 자동 새로 고침**에서 다른 모든 메일 폴더를 자동 새로 고침에 대해 선택할 수 있습니다.

- Secure Mail 아이콘은 Exchange 받은 편지함 폴더에 있는 읽지 않은 메시지 및 새 메시지에 대해서만 총 수를 표시합니다. Secure Mail 은 사용자가 데스크톱 또는 랩톱 컴퓨터에서 전자 메일을 읽은 후에 아이콘을 업데이트합니다.
- 설치 또는 업그레이드 중에 iOS 용 Secure Mail 은 푸시 알림 허용을 사용자에게 요청합니다. 사용자는 iOS 설정 사용하여 나중에 푸시 알림을 허용할 수도 있습니다.

다양한 방식의 푸시 알림을 지원하지 않는 푸시 알림 동작

iOS 의 다양한 방식의 푸시 알림 기능이 지원하지 않는 구성의 경우에도 Secure Mail 은 동기화 기간에 읽지 않은 받은 편지함 이메일 수를 제공합니다. 잠긴 화면 알림 제어 정책이 켜진 경우, 동기화 수행을 위해 iOS 가 Secure Mail 을 활성화한 후에 푸시 알림이 잠긴 장치 화면에 나타납니다.

Secure Mail iOS 푸시 알림 FAQ

언제 iOS 가 Secure Mail 에 알림을 제공합니까

다양한 방식의 푸시 알림 기능이 사용되는 경우 iOS 는 Secure Mail 로 원격 알림을 전송합니다. 이러한 알림은 앱이 백그라운드에서 실행되지 않거나 저전력 모드에 있는 경우에도 전송됩니다.

참고:

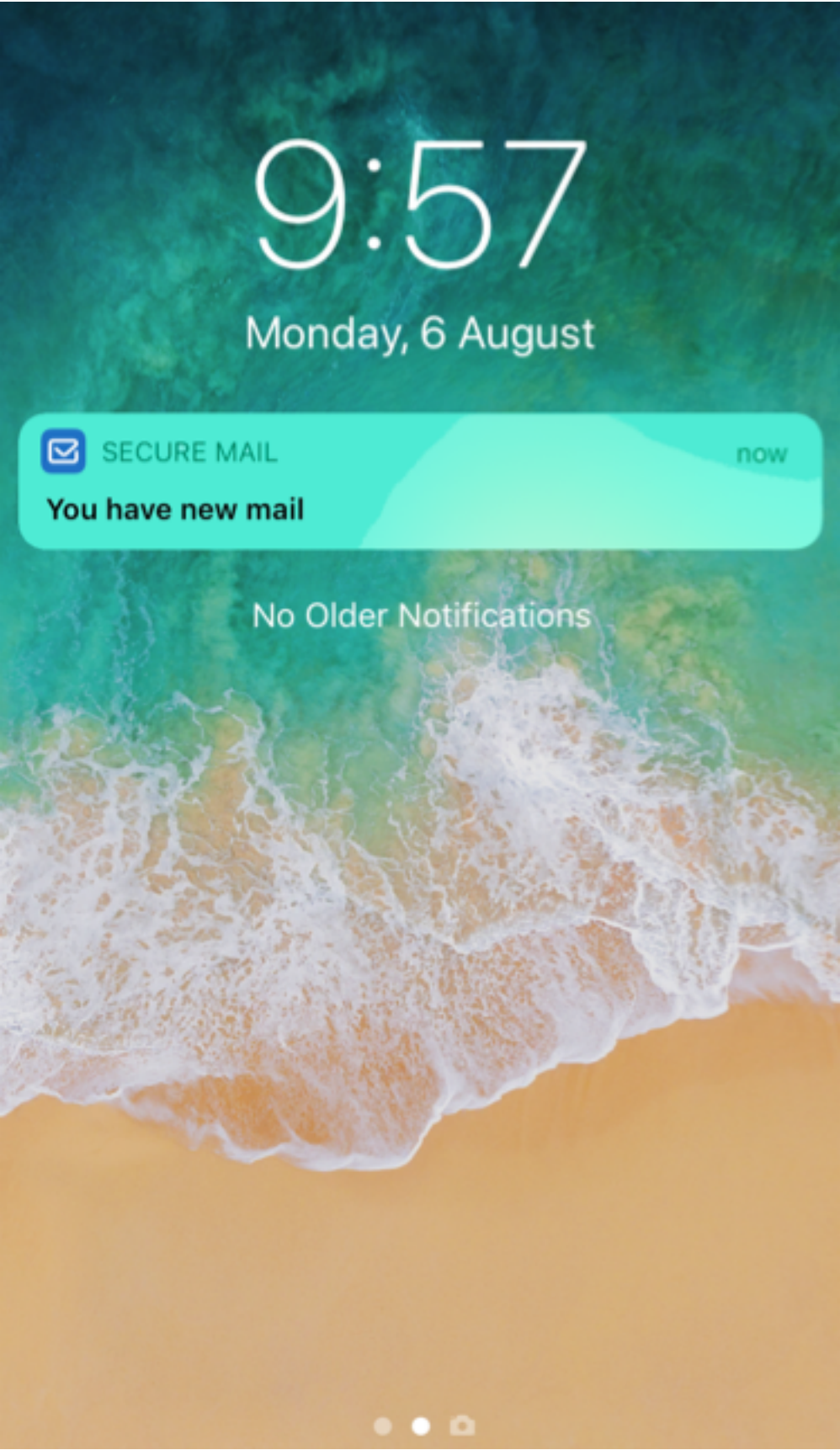
다양한 방식의 푸시 알림이 사용되지 않는 경우 Secure Mail 이 활성 상태가 아니면 Secure Mail 로 알림이 배달되지 않을 수 있습니다. 이 상황은 다음과 같은 여러 가지 이유로 발생합니다.

- 장치가 저전력 모드이고 Secure Mail 이 백그라운드에 있는 경우: 알림이 배달되지 않는 가장 일반적인 경우입니다.

- 백그라운드 앱 새로 고침이 Secure Mail 에 대해 꺼져 있고 Secure Mail 이 백그라운드에 있는 경우: 사용자가 이 설정을 제어합니다.
- 장치의 네트워크 연결이 좋지 않은 경우: 이 상황은 iOS 장치에 따라 다릅니다.

“새 메일이 있습니다.” 알림이 **ios** 장치에 나타나는 이유

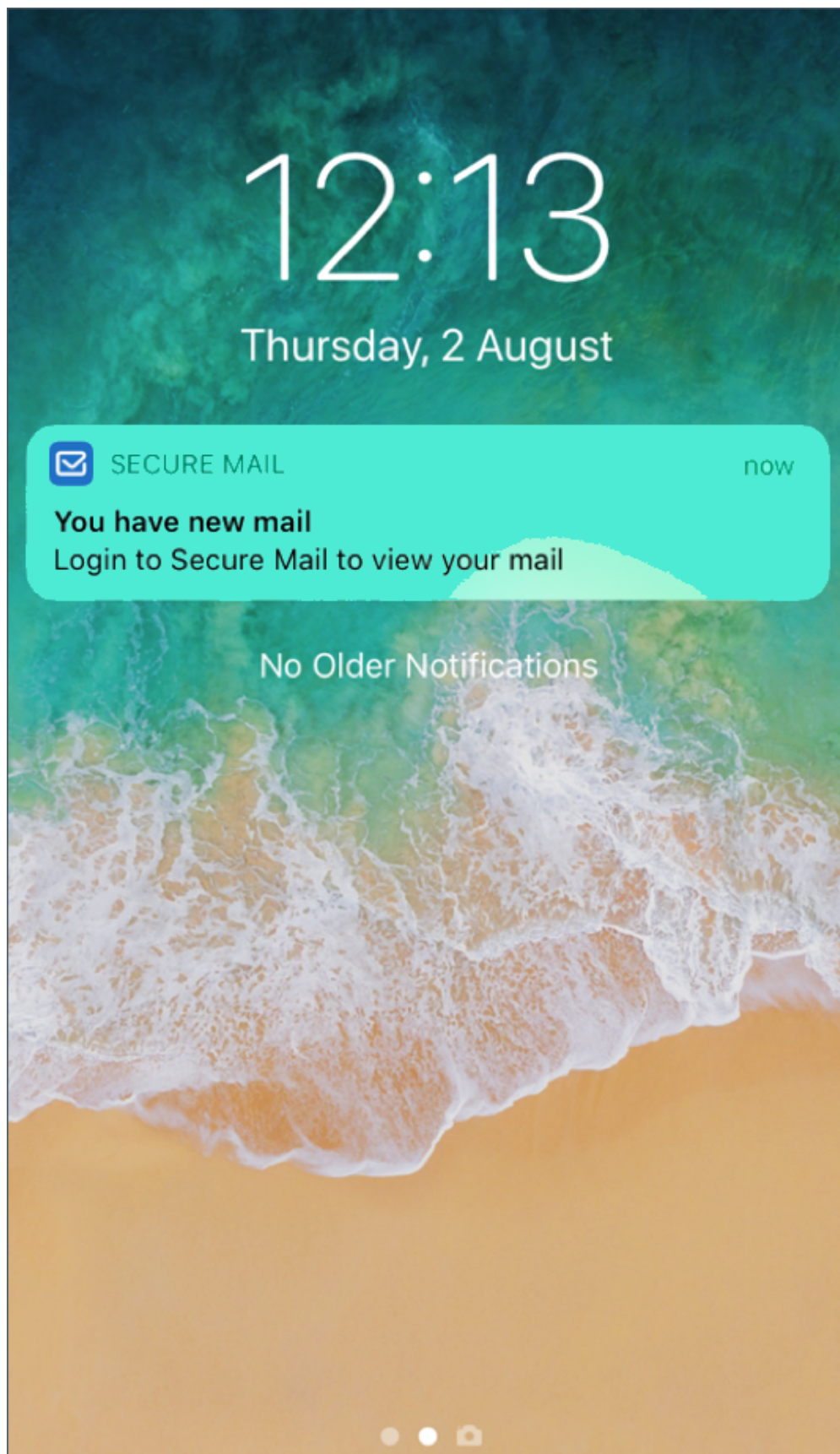
지정된 시간 내에 Secure Mail 에 EWS(Exchange 웹 서비스) 의 응답이 수신되지 않으면 “새 메일이 있습니다.” 알림이 iOS 장치에 나타납니다. 메시지 세부 정보를 가져오는 데 필요한 시간은 30 초입니다.



Wi-Fi 또는 데이터 연결 상태가 좋지 않을 경우에도 장치에서 이 동작이 발생할 수 있습니다.

EWS 응답 지연 외에 Secure Mail 에 “새 메일이 있습니다.” 알림이 표시되는 상황은 다음과 같습니다.

- Secure Mail 이 보안 컨테이너에서 필요한 정보를 읽지 못합니다. 이 시나리오는 일반적으로 장치를 다시 시작한 후 장치 잠금을 해제하기 전에 발생합니다.
- Secure Mail 이 Citrix Gateway 또는 EWS 를 통해 보안 채널에 연결하지 못하거나 보안 채널을 설정하지 못합니다.
- 자격 증명이 만료되었거나 자격 증명을 수정한 후 Secure Mail 에서 자격 증명이 업데이트되지 않았습니다. 다음 그림은 이 시나리오에서 알림이 표시되는 방식을 보여 줍니다.



- 올바른 Secure Mail 요청에 대해 Exchange Server 가 예기치 않은 응답을 전송합니다. EWS 응답 코드에 대한 자세한 내용은 Microsoft 개발자 설명서를 참조하십시오.

iOS 용 Secure Mail 의 푸시 알림 실패 메시지

iOS 용 Secure Mail 에서는 장치의 알림 센터에 해당하는 푸시 알림 실패 메시지가 나타납니다. 이러한 알림은 알림 실패 유형에 따라 표시됩니다.

다음과 같은 여러 실패 시나리오에 따라 다음과 같은 알림 메시지가 나타납니다.

- **Secure Mail** 에서 조직의 네트워크에 연결할 수 없습니다. 이 알림은 Secure Mail 에서 Citrix Gateway 에 대한 SOCKS5 연결을 설정하지 못할 때 나타납니다.
- **Secure Mail** 에서 조직의 네트워크에 연결할 수 없습니다. 관리자에게 문의하십시오. 이 알림은 Citrix Gateway 에 연결할 수 없는 경우 나타납니다. Citrix ADC 가 올바르게 구성되어 있고 외부 네트워크에서 연결할 수 있는지 확인합니다.
- **Secure Mail** 에서 조직의 네트워크에 안전하게 연결할 수 없습니다. 관리자에게 문의하십시오. 이 알림은 Secure Mail 에서 Citrix Gateway 에 대한 SSL 연결을 설정하지 못할 때 나타납니다. SSL 인증서가 올바른지 확인합니다.
- **Secure Mail** 에서 메일 서버에 안전하게 연결할 수 없습니다. 관리자에게 문의하십시오. 이 알림은 Secure Mail 에서 Exchange Server 에 대한 SSL 연결을 설정하지 못할 때 나타납니다. Exchange Server 의 SSL 인증서가 올바른지 확인합니다. 인증서가 올바르지 않음에도 불구하고 Exchange Server 에 앱을 연결하려면 모든 SSL 인증서 수락 MDX 정책을 사용하도록 설정했는지 확인합니다.
- **Secure Mail** 에서 메일 서버 오류로 인해 메시지를 가져올 수 없습니다. 관리자에게 문의하십시오. 이 알림은 Secure Mail 에서 Exchange Server 의 EWS 응답을 구문 분석할 수 없는 경우 나타납니다.
- **Secure Mail** 에서 요청 시간이 초과되어 메시지를 가져올 수 없습니다. 이 알림은 Secure Mail 이 30 초 내에 서버의 응답을 수신하지 못한 경우 나타납니다. 이 알림은 장치의 데이터 또는 Wi-Fi 연결이 불량한 경우 나타날 수 있습니다. 몇 분간 기다린 후 다시 시도하십시오.
- 메시지를 가져올 수 없습니다. **Secure Mail** 을 여십시오. 이 알림은 Secure Mail 이 보안 컨테이너의 자격 증명을 읽을 수 없는 경우 나타납니다. 이 알림은 장치가 다시 시작되었지만 잠금 해제되지 않은 경우 나타날 수 있습니다. 장치 잠금을 해제하여 Secure Mail 에서 보안 컨테이너에 자동으로 액세스할 수 있도록 합니다. 그래도 이 알림이 수신되면 Secure Mail 을 열어 보안 컨테이너의 자격 증명을 자동으로 업데이트합니다.

Secure Mail 과 다른 모바일 생산성 앱 및 Citrix Files 의 상호 작용

July 18, 2023

Secure Mail 이 다른 모바일 생산성 앱 및 Citrix Files 와 상호 작용하기 때문에 사용자는 조직 정책에 의해 설정된 보안 환경을 벗어나지 않으면서 원활하게 문서를 액세스하고 편집하고 공유하고 저장할 수 있습니다. 예를 들어 Secure Mail 에서 링크를

누르면 사이트가 Secure Web 에서 열립니다. 사용자는 Citrix QuickEdit for Endpoint Management 를 사용하여 첨부 파일을 열고 편집할 수 있습니다. 첨부 파일은 사용자의 Citrix Files for Endpoint Management 공간으로 다운로드됩니다.

각 플랫폼별 Secure Mail 기능의 전체 목록은 [플랫폼별 기능](#)을 참조하십시오.

참고:

- XenMobile 용 Citrix Files 는 2023 년 7 월 1 일에 EOL 에 도달했습니다. 자세한 내용은 [EOL 및 더 이상 사용되지 않는 앱](#)을 참조하십시오.

Secure Mail 테스트 및 문제 해결

May 9, 2023

Secure Mail 이 올바르게 작동하지 않는 경우 일반적으로 연결 문제가 원인입니다. 이 문서는 연결 문제를 방지하는 방법에 대해 설명합니다. 문제가 발생한 경우 문제를 해결하기 위해 이 문서를 사용할 수 있습니다.

ActiveSync 연결, 사용자 인증 및 APNs 구성 테스트

Endpoint Management Analyzer 를 사용하여 Secure Mail 자동 검색 서비스 확인을 수행할 수 있습니다. 이는 Endpoint Management Exchange ActiveSync 테스트 응용 프로그램 다운로드 과정을 안내해줍니다. 이 메일 테스트 옵션은 메일 서버의 기본적인 연결 설정을 확인합니다. 또한 이 도구는 ActiveSync 서버 문제를 해결하여 Endpoint Management 환경 내에 배포할 수 있도록 준비하는 데 도움이 됩니다. 자세한 내용은 [Endpoint Management Analyzer 도구](#)를 참조하십시오.

Analyzer 의 메일 테스트 옵션에서는 다음을 확인합니다.

- iOS 및 Android 장치와 Microsoft Exchange 또는 IBM Traveler 서버와의 연결.
- 사용자 인증.
- Exchange Server, EWS(Exchange 웹 서비스), Citrix Gateway, APNs 인증서 및 Secure Mail 을 비롯한 iOS 에 대한 푸시 알림 구성. 푸시 알림 구성에 대한 내용은 [iOS 용 Secure Mail 을 위한 푸시 알림](#)을 참조하십시오.

이 도구는 문제 해결을 위한 포괄적인 권장 사항 목록을 제공합니다.

참고:

Mail Test App, MailTest.ipa 는 사용되지 않습니다. 대신 Endpoint Management Analyzer 에서 동일한 기능에 액세스하십시오.

테스트 사전 요구 사항

- 네트워크 액세스 정책이 차단되어 있지 않도록 확인합니다.
- 전자 메일 작성 차단 정책을 꺼짐으로 설정합니다.

Secure Mail 로그를 사용하여 연결 문제 해결

Secure Mail 로그를 보려면 다음을 수행하십시오.

1. **Secure Hub** > 도움말 > 문제 보고로 이동합니다.

2. 앱 목록에서 **Secure Mail** 을 선택합니다.

해당 조직의 지원 센터로 보내지는 전자 메일이 열립니다.

3. 문제에 대해 설명하는 몇 개의 단어로 제목 줄 및 본문을 채웁니다.

4. 문제가 발생한 시간을 선택합니다.

5. 로그 설정은 지원 팀의 지시가 있는 경우에만 변경합니다.

6. **Send(보내기)** 를 클릭합니다.

압축된 로그 파일이 첨부된 상태로 완성된 메시지가 열립니다.

7. 보내기를 다시 클릭합니다.

전송되는 zip 파일에는 다음 로그가 포함되어 있습니다.

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

앱 정보 로그에는 장치와 앱에 대한 정보가 포함됩니다. 사용 중인 하드웨어 모델 및 플랫폼 버전이 지원되는지 확인하십시오. 사용 중인 Secure Mail 및 MDX Toolkit 의 버전이 최신 버전이고 호환되는지 확인합니다. 자세한 내용은 [Secure Mail 시스템 요구 사항](#) 및 [Endpoint Management 호환성](#)을 참조하십시오.

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

VPN 구성 로그는 Secure Hub 에만 제공됩니다. Citrix ADC 버전 (**ServerBuildVersion**) 을 점검하여 최신 Citrix ADC 릴리스가 사용되고 있는지 확인합니다. **SplitDNS** 및 **SplitTunnel** 설정을 다음과 같이 확인합니다.

- 분할 DNS 가 원격, 로컬 또는 둘 다로 설정된 경우, DNS 를 통해 메일 서버 FQDN 이 올바르게 해결되는지 확인합니다. 분할 DNS 는 Android 에 설치된 Secure Hub 에서만 사용 가능합니다.
- 분할 터널링이 켜짐으로 설정된 경우, 백엔드에서 액세스 가능한 인터넷 앱 중 하나로 메일 서버가 나열되는지 확인합니다.
- CtxLog_AppPolicies.xml(iOS), Policy.xml(Android 및 Windows Phone)

정책 로그는 로그를 얻은 시점에 Secure Mail 에 적용된 모든 MDX 정책의 값을 제공합니다. 연결 문제의 경우, <**BackgroundServices**> 및 <**BackgroundServicesGateway**> 정책의 값을 확인합니다.

- 진단 로그 (diagnostics 폴더에 있음)

Secure Mail 의 초기 구성에서 가장 흔히 발생하는 문제는 “현재 회사 네트워크에 액세스할 수 없습니다” 입니다. 진단 로그를 사용하여 연결 문제를 해결하려면 다음을 수행하십시오.

진단 로그에서 주요 열은 Timestamp, Message Class 및 Message 입니다. 오류 메시지가 Secure Mail 에서 나타나면 **Timestamp** 열에서 관련 로그 항목을 신속히 찾을 수 있도록 시간을 기록해 둡니다.

장치에서 Citrix Gateway 로의 연결이 성공했는지 여부를 확인하려면 AG Tunneler 항목을 검토합니다. 다음 메시지는 성공적인 연결을 나타냅니다.

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

Citrix Gateway 에서 Endpoint Management 의 연결이 성공했고 STA 티켓의 유효성을 검사할 수 있는지 여부를 확인하려면 Secure Hub 진단 로그로 이동하고 Message Class 아래에서 장치 등록 시점의 INFO (4) 항목을 검토합니다. 다음 메시지는 Secure Hub 가 Endpoint Management 로부터 STA 티켓을 얻었음을 나타냅니다.

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

참고:

등록 중에 Secure Hub 는 STA 티켓을 얻기 위해 Endpoint Management 로 요청을 보냅니다. Endpoint Management 는 STA 티켓을 장치로 보내며, 이 티켓은 장치에 저장되고 Endpoint Management STA 티켓 목록에 추가됩니다.

Endpoint Management 가 사용자에게 STA 티켓을 발급했는지 여부를 확인하려면 지원 번들에 포함된 UserAuditLog-File.log 를 살펴보세요. 이 로그에는 각 티켓에 대해 발급 시간, 사용자 이름, 사용자 장치 및 결과가 나열되어 있습니다. 예:

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’

Citrix Gateway 에서 메일 서버로의 통신을 확인하려면 DNS 및 네트워킹이 올바르게 구성되었는지 확인합니다. 확인하려면 Secure Web 을 사용해 OWA(Outlook Web Access) 에 액세스합니다. Secure Mail 과 마찬가지로 Secure Web 은 Micro VPN 터널을 사용하여 Citrix Gateway 로의 연결을 설정할 수 있습니다. Secure Web 은 앱이 액세스하는 내부 또는 외부 리소스에 대한 프록시 역할을 합니다. 일반적으로 그리고 특히 Exchange 환경에서 OWA 는 메일 서버에서 호스팅됩니다.

구성을 테스트하려면 Secure Web 을 열고 OWA 페이지의 FQDN 을 입력합니다. 이 요청은 Citrix Gateway 와 메일 서버 간의 통신과 동일한 라우팅 및 DNS 확인을 거치게 됩니다. OWA 페이지가 열리면 Citrix Gateway 가 메일 서버와 통신 중인 것입니다.

위에서 설명한 확인 절차를 통해 통신이 성공적인 것으로 나타나면 Citrix 설정에 문제가 있는 것이 아니라, Exchange 또는 Traveler 서버에 문제가 있는 것입니다.

이 경우 Exchange 또는 Traveler 서버 관리자를 위해 정보를 수집할 수 있습니다. 먼저 Secure Mail 진단 로그에서 Error 단어를 검색하여 Exchange 또는 Traveler 서버에서 HTTP 문제가 있는지 확인합니다. 오류에 HTTP 코드가 포함되어 있고 Exchange 또는 Traveler 서버가 여러 개인 경우, 각 서버를 조사합니다. Exchange 및 Traveler에는 클라이언트 장치로부터의 HTTP 요청 및 응답을 보여 주는 HTTP 로그가 있습니다. Exchange의 로그는 C:\inetpub\LogFiles\W3SVC1\U_EX.log입니다. Traveler의 로그는 IBM_TECHNICAL_SUPPORT > HTTPR.log입니다.

장치에서 **iOS** 용 **Secure Mail**에 대한 크래시 로그를 가져오려면

1. iOS 장치에서 설정 > 개인 정보 및 보안 > 분석 > 분석 데이터로 이동합니다.
2. 데이터 목록에서 앱 이름과 관련 타임스탬프를 클릭합니다. 로그가 나타납니다.

전자 메일, 연락처 또는 일정 관련 문제 해결

전자 메일이 임시 보관함에 갇힘, 연락처 누락 또는 일정 항목이 동기화되지 않는 등의 Secure Mail 문제를 해결할 수 있습니다. 이러한 문제를 해결하려면 Exchange ActiveSync 사서함 로그를 사용합니다. 이 로그는 장치에서 보낸 들어오는 요청 및 메일 서버로부터 나가는 응답을 보여 줍니다.

무제한 동기화 모범 사례

사용자가 메일 동기화 기간을 모두로 설정한 경우 무제한으로 동기화됩니다. 무제한 동기화에서는 사용자가 자신의 사서함 크기(받은 편지함 및 동기화되는 모든 하위 폴더)를 관리하는 것으로 가정합니다. 최상의 성능을 얻으려면 다음과 같은 몇 가지 사항에 유의해야 합니다.

1. 사서함 크기가 메시지 18,000 개 또는 총 크기 600MB를 초과하면 전자 메일 동기화가 느려질 수 있습니다.
2. 무제한 동기화를 사용하는 경우 **WiFi**에서 첨부 파일 로드를 사용 설정하지 않는 것이 좋습니다. 이 옵션을 설정하면 장치에서 메일 크기가 빠르게 증가할 수 있습니다.
3. 무제한 동기화가 사용자에게 옵션으로 표시되지 않도록 하려면 최대 동기화 간격 앱 정책을 모두 이외의 값으로 설정합니다.
4. 사용자의 기본 동기화 간격으로 모두를 설정하지 않는 것이 좋습니다.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).