

セキュアメール

Contents

Secure Mail の概要	30
Secure Mail の新機能	33
現在のバージョンの新機能	33
iOS 用 セキュアメール 26.8.0	33
iOS/iPadOS 27 のサポート	33
Secure Mail をデフォルトのメールアプリとして設定するサポート	33
以前のバージョンの新機能	34
Android版セキュアメール 26.5.0	34
Android 17のサポート	34
iOS版セキュアメール 26.5.0	34
iOS版セキュアメール 26.1.0	34
モバイルレスポンシブなメール書式設定のサポート	34
Android版セキュアメール 25.12.0	34
16KBメモリページサイズのサポート	34
iOS版 セキュアメール 25.9.0	35
連絡先の双方向同期のサポート	35
iOS 15の非推奨化	35
Android版 セキュアメール 25.8.0	35
Android APIレベル35のサポート	35
Android版 セキュアメール 25.6.0	35
レガシーMDXの非推奨化	35
iOS版 セキュアメール 25.5.0	36
iOS 26のサポート	36
TLS 1.3プロトコルのサポート	36
Domino 14 FP1のサポート	36
レガシーMDXの非推奨化	36

Android版セキュアメール 25.3.0	37
Android 16のサポート	37
大容量添付ファイルのダウンロードのサポート	37
Android版セキュアメール 25.1.0	37
TLS 1.3プロトコルのサポート	37
iOS版セキュアメール 25.1.0	37
大容量添付ファイルのダウンロードのサポート	37
Android版セキュアメール 24.11.0	38
ウォーターマークなしでメールの添付ファイルを表示	38
iOS版セキュアメール 24.11.0	38
iOS版セキュアメール 24.9.0	38
iOS 18のサポート	38
Android版セキュアメール 24.9.1	38
Android 15のサポート	38
Android版セキュアメール 24.9.0	39
APIレベル34のサポート	39
Android版セキュアメール 24.7.0	39
iOS版セキュアメール 24.3.0	39
iOS版セキュアメール 24.2.0	39
Android版セキュアメール 24.1.0	39
カレンダーイベントのズームイン機能に対応	39
iOS版セキュアメール 23.9.0	40
iOS 17に対応	40
HCL Domino 12に対応	40
Android版セキュアメール 23.8.2	41
透かしなしでメールの添付ファイルを表示	41
Android向け セキュアメール 23.8.1	41
透かしなしでメール添付ファイルを表示	41

HCL Domino 12のサポート	41
Android版 セキュアメール 23.8.0	42
Android 14のサポート	42
Android版 セキュアメール 23.7.0	42
Microsoft Exchange累積更新プログラム13のサポート	42
オンプレミスExchangeでのハイブリッドモダン認証のサポート	42
iOS 用 セキュアメール 23.7.0	42
オンプレミスExchangeでのハイブリッドモダン認証のサポート	42
ダークモード	42
Android 用 セキュアメール 23.6.0	42
ダークモード	42
iOS 用 セキュアメール 23.5.0	43
分割表示モードとスライドオーバーモードでのマルチタスク	43
セキュアメール 23.3.5	43
アンドロイド版 セキュアメール	43
Secure Mail バージョン 23.2.0	43
Android 用 セキュアメール	43
iOS 用 セキュアメール	43
セキュアメール 22.11.0	43
Android 用セキュアメール	43
セキュアメール 22.9.0	44
iOS 用 セキュアメール	44
アンドロイド版 Secure Mail	44
セキュアメール 22.6.2	44
iOS用 セキュアメール	44
セキュアメール 22.6.0	44
iOS用 セキュアメール	44
Android用 セキュアメール	44

セキュアメール 22.3.0	44
iOS用 セキュアメール	44
Android用 セキュアメール	44
セキュアメール 22.2.0	45
iOS版セキュアメール	45
Android版セキュアメール	45
Secure Mail バージョン 21.12.0	45
iOS 向け セキュアメール	45
Android 向け セキュアメール	46
セキュアメール 21.11.0	46
Android 用セキュアメール	46
セキュアメール 21.10.5	49
iOS 用セキュアメール	49
Android 用セキュアメール	49
セキュアメール 21.10.0	50
Android 用セキュアメール	50
セキュアメール 21.9.1	50
Android 用セキュアメール	50
セキュアメール 21.9.0	50
iOS用セキュアメール	50
Android用セキュアメール	50
セキュアメール 21.8.5	50
Android用セキュアメール	50
セキュアメール 21.8.0	51
iOS用セキュアメール	51
ハイブリッド環境におけるExchange Serverのメールベースの自動検出	51
Microsoft Office 365 で最新認証を実行するセットアップでのリッチプッシュ通知	51
前提条件	52

制限事項	53
Android用 セキュアメール	54
セキュアメール 21.7.0	54
アイオーエス用 セキュアメール	54
Android用 セキュアメール	54
セキュアメール 21.6.0	54
アイオーエス用 セキュアメール	54
Android版Secure Mail	55
セキュアメール 21.5.0	55
iOS向けセキュアメール	56
Android向けセキュアメール	56
セキュアメール 21.4.5	57
Android 版 セキュアメール	57
セキュアメール 21.4.0	57
iOS 版 セキュアメール	57
セキュアメール 21.3.5	57
Android 版 セキュアメール	57
セキュアメール 21.3.0	57
iOS版セキュアメール	57
Android版セキュアメール	57
セキュアメール 21.2.0	58
iOS版セキュアメール	58
Android版セキュアメール	58
セキュアメール 21.1.5	58
セキュアメール iOS版	58
セキュアメール 21.1.0	58
セキュアメール 20.12.0	58
セキュアメール iOS版	58

セキュアメール 20.11.0	58
セキュアメール 20.10.5	59
セキュアメール iOS版	59
セキュアメール Android版	59
セキュアメール 20.10.0	59
iOS版セキュアメール	59
Android版セキュアメール	59
セキュアメール 20.9.5	60
Android版セキュアメール	60
セキュアメール 20.9.0	60
前提条件	60
アップグレード後	61
セキュアメール 20.8.5	61
Android版セキュアメール	61
セキュアメール 20.8.0	62
Android向けセキュアメール	62
iOS向けセキュアメール	64
セキュアメール 20.7.5	64
セキュアメール 20.7.0	64
セキュアメール 20.6.5	65
セキュアメール 20.6.0	65
セキュアメール 20.5.0	65
セキュアメール 20.4.5	65
Android版 セキュアメール	65
セキュアメール 20.4.0	65
セキュアメール 20.3.0	65
Android版 セキュアメール	65
iOS版 セキュアメール	66

セキュアメール 20.2.0	66
Android版 セキュアメール	66
下書きを最小化	66
セキュアメール 20.1.5	66
iOS版セキュアメール	66
Android版セキュアメール	67
セキュアメール 20.1.0	67
セキュアメール 19.12.5	67
iOS版セキュアメール	67
Android版セキュアメール	67
セキュアメール 19.11.5	67
セキュアメール for iOS	67
セキュアメール for Android	67
セキュアメール for iOS 19.10.6	68
セキュアメール 19.10.5	68
セキュアメール for iOS	68
セキュアメール for Android	68
セキュアメール 19.10.0	68
iOSを実行しているデバイス	69
Androidを実行しているデバイス	69
セキュアメール 19.9.5	70
iOS版セキュアメール	70
Android版セキュアメール	70
セキュアメール 19.9.0	70
iOS向けセキュアメール	70
Android向けセキュアメール	71
Android向けセキュアメール 19.8.5	71
セキュアメール 19.8.0	71

iOS用セキュアメール	71
Android用セキュアメール	71
セキュアメール 19.7.5	72
iOS用セキュアメール	72
Android用セキュアメール	72
セキュアメール 19.6.5	73
iOS版セキュアメール	73
Android版セキュアメール	73
セキュアメール 19.5.5	74
Android版セキュアメール	74
iOS向けセキュアメール	74
セキュアメール 19.5.0	75
アンドロイド向けセキュアメール	75
Android版Secure Mail 19.4.6、19.4.5、および 19.3.5	76
セキュアメール 19.3.0	77
iOSデバイス用Secure Mail	77
iOSおよびAndroid版Secure Mail	79
セキュアメール 19.2.0	80
iOS用セキュアメール	80
Android用セキュアメール	80
iOSデバイス用Secure Mail 19.1.6	81
セキュアメール 19.1.5	81
セキュアメール 19.1.0	82
iOS向けセキュアメール	82
アンドロイド版Secure Mail	83
セキュアメール 18.12.0	83
セキュアメール 18.11.5	84
アンドロイド向けセキュアメール	84

セキュアメール 18.11.1	85
セキュアメール 18.11.0	86
Android 版 セキュアメール	86
iOS 版 セキュアメール	86
セキュアメール 18.10.5	87
セキュアメール 18.10.0	87
セキュアメール 18.9.0	88
セキュアメール 10.8.65	88
セキュアメール 10.8.60	89
セキュアメール 10.8.55	89
セキュアメール 10.8.50	89
セキュアメール 10.8.45	91
セキュアメール 10.8.40	93
セキュアメール 10.8.35	93
セキュアメール 10.8.25	95
カレンダーの変更	98
連絡先の変更	99
添付ファイルの変更	100
セキュアメール 10.8.20	100
セキュアメール 10.8.15	100
セキュアメール 10.8.10	101
既知の問題と修正された問題	102
iOS向け セキュアメール 26.8.0	102
修正された問題	102
既知の問題	102
Android向け セキュアメール 26.5.0	102
修正された問題	102
既知の問題	102

iOS用セキュアメール 26.5.0	103
修正された問題	103
既知の問題	103
iOS用セキュアメール 26.1.0	103
修正された問題	103
既知の問題	103
アンドロイド版セキュアメール 25.12.0	104
修正された問題	104
既知の問題	104
iOS 用 セキュアメール 25.9.0	104
修正された問題	104
既知の問題	104
Android 用 セキュアメール 25.8.0	105
修正された問題	105
既知の問題	105
Android版 セキュアメール 25.6.0	105
修正された問題	105
既知の問題	105
iOS版 セキュアメール 25.5.0	105
修正された問題	105
既知の問題	106
セキュアメール for Android 25.3.0	106
修正された問題	106
既知の問題	106
セキュアメール for Android 25.1.0	106
修正された問題	106
既知の問題	106
iOS 用 セキュアメール 25.1.0	106

修正された問題	106
既知の問題	107
iOS 用 セキュアメール 24.11.0	107
修正された問題	107
既知の問題	107
アンドロイド版 セキュアメール 24.11.0	107
修正された問題	107
既知の問題	107
Android版 セキュアメール 24.9.1	107
修正された問題	107
既知の問題	107
Android版 セキュアメール 24.9.0	108
修正された問題	108
既知の問題	108
iOS版 セキュアメール 24.9.0	108
修正された問題	108
既知の問題	108
Android版 セキュアメール 24.7.0	108
修正された問題	108
既知の問題	108
iOS版 セキュアメール 24.3.0	109
修正された問題	109
既知の問題	109
iOS版 セキュアメール 24.2.0	109
修正された問題	109
既知の問題	109
アンドロイド版 セキュアメール 24.1.0	110
修正された問題	110

既知の問題	110
Android版 セキュアメール 23.10.0	110
修正された問題	110
既知の問題	110
Android版 セキュアメール 23.8.2	110
修正された問題	110
既知の問題	111
AndroidおよびiOS版 Secure Mail 23.7.0	111
修正された問題	111
既知の問題	111
Android版 セキュアメール 23.8.1	111
修正された問題	111
既知の問題	111
iOS版 セキュアメール 23.9.0	111
修正された問題	111
既知の問題	111
Android版 セキュアメール 23.8.0	112
修正された問題	112
既知の問題	112
Android版 セキュアメール 23.7.0	112
修正された問題	112
既知の問題	112
Android版セキュアメール 23.6.0	112
修正された問題	112
既知の問題	112
iOS版セキュアメール 23.5.0	112
修正された問題	112
既知の問題	113

以前のバージョンにおける既知の問題と修正された問題	113
Secure Mail の既知の修正済み問題の履歴	114
セキュアメール 23.3.5	114
Android 版 Secure Mail の既知の問題	114
Android 版 Secure Mail の修正済み問題	114
セキュアメール 23.2.0	114
iOS および Android 版 Secure Mail の既知の問題	114
Android 版 Secure Mail の修正済み問題	114
iOS版Secure Mailの修正済み問題	115
セキュアメール 22.11.0	115
Android版Secure Mailの既知の問題	115
Android版Secure Mailの修正済み問題	115
セキュアメール 22.9.0	115
iOSおよびAndroid版Secure Mailの既知の問題	115
iOSおよびAndroid版Secure Mailの修正された問題	115
セキュアメール 22.6.2	116
iOS版Secure Mailの既知の問題	116
iOS版Secure Mailの修正された問題	116
セキュアメール 22.6.0	116
iOS版Secure Mailの既知の問題	116
iOS版Secure Mailの修正された問題	116
セキュアメール 22.3.0	116
Secure Mail 22.3.0 の既知の問題	116
Secure Mail 22.3.0 で修正された問題	116
セキュアメール 22.2.0	117
Secure Mail 22.2.0 の既知の問題	117
Secure Mail 22.2.0 で修正された問題	117
セキュアメール 21.12.0	117

修正された問題	117
セキュアメール 21.11.0	117
セキュアメール 21.10.5	117
Android版Secure Mailで修正された問題	117
Android版Secure Mailの既知の問題	117
セキュアメール 21.10.0	118
Android版Secure Mailの既知の問題	118
Android版Secure Mailで修正された問題	118
セキュアメール 21.9.1	118
Android版Secure Mailの既知の問題	118
Android版Secure Mailの修正された問題	118
セキュアメール 21.9.0	118
セキュアメール 21.8.5	119
既知の問題	119
修正された問題	119
セキュアメール 21.8.0	119
既知の問題	119
修正された問題	119
セキュアメール 21.7.0	119
既知の問題	119
修正された問題	119
セキュアメール 21.6.0	120
セキュアメール 21.5.0	120
セキュアメール 21.4.5	120
セキュアメール 21.4.0	120
セキュアメール 21.3.5	120
セキュアメール 21.3.0	120
セキュアメール 21.2.0	120

既知の問題	120
修正された問題	120
セキュアメール 21.1.5	120
iOS版セキュアメール	120
セキュアメール 21.1.0	121
既知の問題	121
修正された問題	121
セキュアメール 20.12.0	121
iOS版セキュアメール	121
セキュアメール 20.11.0	121
セキュアメール 20.10.5	121
既知の問題	121
修正された問題	121
セキュアメール 20.10.0	121
既知の問題	121
修正された問題	121
セキュアメール 20.9.5	122
Android版 セキュアメール	122
セキュアメール 20.9.0	122
既知の問題	122
修正された問題	122
セキュアメール 20.8.5	122
Android版セキュアメール	122
既知の問題	122
修正された問題	122
セキュアメール 20.8.0	122
セキュアメール 20.7.5	122
セキュアメール 20.7.0	123

セキュアメール 20.6.5	123
既知の問題	123
修正された問題	123
セキュアメール 20.6.0	123
既知の問題	123
修正された問題	123
セキュアメール 20.5.0	123
iOS用セキュアメール	123
既知の問題	123
修正された問題	123
セキュアメール 20.4.5	124
既知の問題	124
修正された問題	124
セキュアメール 20.4.0	124
既知の問題	124
修正された問題	124
セキュアメール 20.3.0	124
セキュアメール 20.2.0	124
セキュアメール 20.1.5	125
既知の問題	125
修正された問題	125
セキュアメール 20.1.0	125
既知の問題	125
修正された問題	125
セキュアメール 19.12.5	125
既知の問題	125
修正された問題	126
セキュアメール 19.11.5	126

iOS版セキュアメール 19.10.6	126
iOS版Secure Mailの既知の問題	126
iOS版Secure Mailの修正された問題	126
セキュアメール 19.10.5	126
既知の問題	126
修正された問題	126
セキュアメール 19.10.0	126
セキュアメール 19.9.5	127
既知の問題	127
修正された問題	127
セキュアメール 19.9.0	127
既知の問題	127
修正された問題	127
セキュアメール 19.8.5	127
Android版Secure Mailの既知の問題	127
Android版Secure Mailで修正された問題	128
セキュアメール 19.8.0	128
既知の問題	128
修正された問題	128
セキュアメール 19.7.5	128
既知の問題	128
修正された問題	128
セキュアメール 19.6.5	128
既知の問題	128
修正された問題	129
セキュアメール 19.5.5	129
既知の問題	129
修正された問題	129

セキュアメール 19.5.0	129
既知の問題	129
修正された問題	129
Android版 セキュアメール 19.4.6	130
Secure Mail for Android の既知の問題と修正された問題	130
セキュアメール 19.4.5	130
既知の問題	130
修正された問題	130
セキュアメール 19.3.5	130
既知の問題	130
修正された問題	130
セキュアメール 19.3.0	131
既知の問題	131
修正された問題	131
セキュアメール 19.2.0	131
既知の問題	131
修正された問題	131
iOS 用セキュアメール 19.1.6	132
iOS版Secure Mailの既知の問題と修正された問題	132
セキュアメール 19.1.5	132
既知の問題	132
修正された問題	132
セキュアメール 19.1.0	132
既知の問題	132
修正された問題	132
セキュアメール 18.12.0	133
修正された問題	133
セキュアメール 18.11.1	133

修正された問題	133
既知の問題	133
セキュアメール 18.10.5	134
修正された問題	134
セキュアメール 18.10.0	134
修正された問題	134
セキュアメール 18.9.0	134
修正された問題	134
セキュアメール 10.8.65	135
修正された問題	135
セキュアメール 10.8.60	135
修正された問題	135
セキュアメール 10.8.55	136
修正された問題	136
バージョン 10.8.55 でのMDX関連の修正済み問題	136
セキュアメール 10.8.50	136
修正された問題	136
セキュアメール 10.8.45	136
修正された問題	136
セキュアメール 10.8.40	136
修正された問題	136
セキュアメール 10.8.35	136
修正された問題	136
セキュアメール 10.8.25	137
修正された問題	137
セキュアメール 10.8.20	137
修正された問題	137
セキュアメール 10.8.10	138

修正された問題	138
AndroidおよびiOS版Secure Mail - プレビュー	139
機能フラグ管理	140
Secure Mailの展開	141
Secure Mail の構成	143
Microsoft Office 365でのモダン認証	143
Citrix Endpoint Management™ ポリシーの前提条件	144
Exchange Server の構成オプション	145
outlook.office365.com を使用した構成	146
Microsoft 統合ドメイン outlook.cloud.microsoft を使用した構成	146
制限事項	146
Secure Mailポリシー	146
OAuthサポートマトリックスを備えたSecure Mail	147
iOSおよびAndroid向けオンプレミスExchangeサポートによるハイブリッド最新認証	148
MDXポリシーで必要な変更	148
制限事項	150
Secure Mailのバックグラウンドサービス	150
Secure Mailのバックグラウンドサービスを構成するには	150
バックグラウンドサービス構成用のMDXアプリポリシー	150
メールサーバーへの直接接続	152
STA経由でのメールサーバーへの接続	153
Exchange Server または IBM Notes Traveler Server の統合	153
Secure Mail 用の IBM Notes Traveler サーバーの構成	154
システム要件	155
インフラストラクチャサーバーの要件	155
認証プロトコル	155
ポート要件	155

SSL/TLSセキュリティレベルの構成	156
ノート トラベラー サーバーの構成	157
セキュアメール用 S/MIME	157
デジタルIDプロバイダーとの統合	159
前提条件	160
統合の構成	160
派生資格情報の使用	160
メールによる証明書の配布	161
前提条件	161
Microsoft Certificate Services の Web 登録を有効にする	162
IIS で認証設定を確認する	162
新しい証明書テンプレートを作成する	163
ユーザー証明書の要求	166
発行済み証明書の検証	168
ユーザー証明書のエクスポート	169
メールで証明書を送信する	169
iOSおよびAndroid版Secure MailでS/MIMEを有効にする	170
個別の署名証明書と暗号化証明書でS/MIMEを有効にするには	170
単一の署名および暗号化証明書でS/MIMEを有効にするには	171
iOSおよびAndroidでのS/MIMEのテスト	172
公開証明書ソースの構成	172
セキュアメール向けシングルサインオン	173
Secure Mail での自動登録を有効にするには	173
Secure Mailアプリポリシーを構成するには	174
自動プロビジョニングによるエンドツーエンドのSecure Mail SSOユーザーエクスペリエンス	174
問題のトラブルシューティング	175
セキュリティに関する考慮事項	176

Microsoft IRM および AIP メール権限保護のサポート	176
Secure Mail で情報権限管理を有効にするには	176
権限保護されたメールを受信した場合	177
権限保護されたメールを作成する場合	178
メールセキュリティ分類	179
iOS データ保護	182
iOS データ保護を有効にするポリシーを変更するには	182
オーストラリア信号局のデータ保護	182
画面コンテンツの隠蔽	183
iOS の機能	187
Secure Mail をデフォルトのメールアプリとして設定するサポート	187
Secure MailカレンダーイベントでMicrosoft Teams会議を作成する	188
下書きを最小化する	189
MIMEヘッダーを使用したフィッシングメールの報告	189
WkWebViewのサポート	189
Slack EMMのサポート	190
グループ通知	190
通知応答オプション	190
リッチプッシュ通知の失敗メッセージの機能強化	191
Microsoftセットアップでのリッチプッシュ通知のサポート	191
派生資格情報に対するS/MIMEのサポート	191
リッチテキスト署名	192
リッチテキスト署名を追加するには	192
Secure Mail発信者ID	193
カレンダーの色を設定する	193
「ファイル」アプリからファイルを添付する	193
スペルチェック機能	193
メールボックス画面	195

個別アカウント	196
カレンダー	196
カレンダーイベントに色を設定するには	196
検索	197
iOSでメール、カレンダーイベント、またはインライン画像を印刷する	197
前提条件	197
メールを印刷するには	197
カレンダーイベントを印刷するには	202
複数の会議コード（会議へのダイヤルイン）	203
会議にダイヤルインするには	203
メール添付ファイルの印刷サポート	203
Android の機能	204
Secure Mail のカレンダーイベントで Microsoft Teams 会議を作成する	204
双方向連絡先同期	206
送信済みメールの取り消し	206
下書きフォルダーでの添付ファイルの同期	206
PDFファイルのアプリ内表示	206
Microsoft Office 365でモダン認証を実行するセットアップのトンネリングポリシーにWeb SSO を使用する	206
カレンダーイベントのドラッグアンドドロップ	206
Google Play向け64ビットアプリのサポート	207
Android版Secure MailのプルツリーフレッシュUIの改善	207
カレンダーアジェンダのウィジェット	207
ネットワークアクセスポリシー	207
フィードカードの機能強化	208
添付ファイルの表示	208
メールとカレンダーイベントの印刷	208
前提条件	208

メールを印刷するには	209
インライン画像を印刷するには	211
カレンダーイベントを印刷するには	211
ActiveSyncヘッダー付きでフィッシングメールを報告する	212
サブフォルダー通知	212
サブフォルダーの通知を有効にするには	213
通知チャンネル	213
メール内の会議応答ボタン	214
添付ファイルの機能強化	214
戻るボタンの機能強化	215
Androidでギャラリーからファイルを添付できるようにするための管理者向け手順	215
サポートされているファイル形式	216
カレンダー	219
カレンダーイベントに色を設定するには	219
検索	220
バックグラウンドサービスの更新	220
セキュアメールにおけるアンドロイドエンタープライズ	220
前提条件	221
Android Enterpriseと互換性のある機能	221
制限事項	223
Secure Mail の iOS および Android 機能	224
アジュール ガバメント クラウド コンピューティング のサポート	224
前提条件	224
アップグレード後	225
ICSファイルのサポート	225
Secure Mailの連絡先写真	225
フィードの管理	226
Office 365 Exchange Serverポリシーを使用してOffice 365サーバーアドレスを定義する	226

暗号化管理のサポート	226
iOSを実行しているデバイス	227
Androidを実行しているデバイス	227
レスポンスメールのサポート	228
カレンダーイベントのドラッグアンドドロップ	228
フィードの管理	228
自動送り	228
下書きフォルダーの自動同期	228
MDM + MAM モードで Microsoft Intune を使用する場合のシングルサインオンのサポート	229
連絡先の機能強化	229
前提条件	229
会議の時間と場所をネイティブカレンダーにエクスポートする	230
複数のExchangeアカウント	230
連絡先	230
カレンダーで色を設定する	231
内部ドメイン	231
人間工学に基づいた改善	237
Secure MailとSlackの統合（プレビュー）	238
フィッシングメールを報告する（転送として）	238
フィッシングメールを報告する	239
Secure Mailの予定をエクスポートする	239
iOSの場合	240
Androidの場合	240
フィードフォルダー	241
フィードカードを表示するには	241
フィードフォルダーの機能強化	243
マネージャーからのフィード	244
カレンダーから会議に参加する	245

サポートされている会議の種類	245
Microsoft Teamsアプリ	246
Zoomアプリ	246
Webex (ラップされていないアプリ)	246
Skype for Business (スカイプ フォー ビジネス)	246
Skype (スカイプ)	247
ダイヤルインの仕様	247
スカイプ フォー ビジネス	248
一般的な音声会議情報	248
個人カレンダーのオーバーレイ	252
インライン画像を挿入する	252
スワイプアクション	252
iOSおよびAndroidでSkype for Business会議に参加する	252
Skype for Business会議に参加するには	252
添付ファイルのアプリ内プレビューとその他の機能強化	253
ファイルを添付するメッセージを選択するには	253
オフラインアクセス用に添付ファイルを保存するには	254
オフラインファイルから添付ファイルを削除するには	255
別のアプリケーションを使用して添付ファイルを開くには	255
添付ファイルの元のメールまたはカレンダーイベントを表示するには	257
ユーザー名をメールアドレス (UPN) に移行する	257
前提条件	258
UPNベースの認証に移行するには	258
移行を確認するには	258
個人配布リスト	258
前提条件	258
個人の配布リストを表示するには	259
連絡先グループにメールを作成するには	259

連絡先グループにカレンダー招待を送信するには	259
フォルダーの同期	260
フォルダーを同期するには	260
写真添付機能の改善	260
メールに写真を添付するには	260
Secure Mailはメール表示中に埋め込みリソースをレンダリングします	261
最新の認証のサポート	261
Secure MailのSecure WebドメインMDXポリシーを許可する	261
Secure Webドメインポリシーの構成例	262
Android版Secure Mailの場合	262
iOS版Secure Mailの場合	262
Secure Mail と Slack の統合	263
前提条件	263
デバイスでこの機能を有効にするには	263
この機能を使用するには	269
通知と同期	275
iOS の Secure Mail のバックグラウンドアプリ更新	275
セキュアメールとアクティブシンク	275
iOS	275
アンドロイド	276
Secure Mailでの連絡先のエクスポート	276
Secure Mailの通知	277
Secure Mail のプッシュ通知	277
プッシュ通知の仕組み	278
プッシュ通知のシステム要件	278
プッシュ通知のためのSecure Mailの構成	279
Exchange Serverの構成	279
Citrix Gateway の構成	281

トラブルシューティング	281
Secure Mail プッシュ通知に関する FAQ	281
Android は Secure Mail に通知をいつ配信しますか?	281
FCM は、ロック画面に表示されるメール通知にどのように影響しますか?	281
APNs は、ロック画面に表示されるメール通知にどのように影響しますか?	282
バックグラウンドアプリの更新は Secure Mail と APNs にどのように影響しますか?	282
低電力モードは Secure Mail と APNs にどのように影響しますか?	282
FCM 主導の同期がバックグラウンドで失敗する原因となるその他の問題は何ですか?	282
APNs 主導の同期がバックグラウンドで失敗する原因となるその他の問題は何ですか?	283
通知が配信されない場合や APNs が使用されていない場合、Secure Mail は他にどのようにロック画面通知を生成しますか?	283
Secure Mail は、ロック画面にコンテンツを表示する他のアプリとどう異なりますか?	284
Secure Mail for iOS のリッチプッシュ通知	285
Secure Mail iOS でプッシュ通知が機能する方法	286
リッチプッシュ通知サポートなしでのプッシュ通知の動作	287
Secure Mail iOS プッシュ通知に関する FAQ	287
iOS デバイスに「新着メールがあります」通知が表示される理由	287
Secure Mail for iOS におけるプッシュ通知の失敗メッセージ	288
Secure Mail と他のモバイル生産性アプリおよび Citrix Files との連携	289
Secure Mail のテストとトラブルシューティング	289
ActiveSync 接続、ユーザー認証、および APNs 構成のテスト	290
テストの前提条件	290
Secure Mail ログを使用した接続問題のトラブルシューティング	290
iOS 版 Secure Mail のデバイスからクラッシュログを取得するには	293
メール、連絡先、またはカレンダーに関する問題のトラブルシューティング	293
無制限同期のベストプラクティス	293

Secure Mail の概要

Citrix Secure Mail™ を使用すると、ユーザーはモバイルフォンやタブレットでメール、カレンダー、連絡先を管理できます。Microsoft Outlook または IBM Notes アカウントとの継続性を維持するために、Secure Mail は Microsoft Exchange Server および IBM Notes Traveler Server と同期します。

Citrix アプリスイートの一部として、Secure Mail は Citrix Secure Hub とのシングルサインオン (SSO) 互換性によるメリットがあります。ユーザーが Secure Hub にサインオンすると、ユーザー名とパスワードを再入力することなく、Secure Mail にシームレスに移行できます。Secure Mail は、デバイスが Secure Hub に登録されたときに自動的にユーザーのデバイスにプッシュされるように構成することも、ユーザーがストアからアプリを追加することもできます。

注:

- Exchange Server 2010 のサポートは October 13, 2020 に終了しました。
- Exchange Server 2013 のサポートは April 11, 2023 に終了しました。

Secure Mail は以下と互換性があります。

- エクスチェンジ サーバー SE RTM
- Exchange Server 2019 累積更新プログラム 15
- Exchange Server 2019 累積更新プログラム 14
- Exchange Server 2019 累積更新プログラム 13
- Exchange Server 2019 累積更新プログラム 12
- Exchange Server 2019 累積更新プログラム 11
- Exchange Server 2019 累積更新プログラム 10
- Exchange Server 2019 累積更新プログラム 9
- Exchange Server 2019 累積更新プログラム 8
- Exchange Server 2019 累積更新プログラム 7
- Exchange Server 2019 累積更新プログラム 6

- Exchange Server 2016 累積更新プログラム 23
- Exchange Server 2016 累積更新プログラム 22
- Exchange Server 2016 累積更新プログラム 21
- Exchange Server 2016 累積更新プログラム 20
- Exchange Server 2016 累積更新プログラム 19
- Exchange Server 2016 累積更新プログラム 18
- Exchange Server 2016 累積更新プログラム 17
- HCL Domino バージョン 14.0 FP1
- HCL Domino バージョン 12.0.2 FP2
- HCL Traveler バージョン 12.0.2.1 ビルド 202302010413_30
- HCL Domino 11 (以前の名称: Lotus Notes)
- HCL Domino 10.0.1 (以前の名称: Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197 (旧 ロータス ノーツ)
- HCL Domino 10.0.1.0 build 201811191126_20 (旧 ロータス ノーツ)
- HCL Domino 9.0.1.21 (旧 ロータス ノーツ)
- Microsoft Office 365 (エクスチェンジ オンライン)

まず、[Citrix Endpoint Management Downloads](#)からSecure Mail およびその他の Endpoint Management コンポーネントをダウンロードしてください。

Secure Mail およびその他のモビリティアプリのシステム要件については、[システム要件](#)を参照してください。

iOS および Android 版 Secure Mail での通知（アプリがバックグラウンドで実行されている場合、または閉じられている場合）に関する情報については、[Secure Mail のプッシュ通知](#)を参照してください。

Secure Mail でサポートされている iOS の機能については、[Secure Mail の iOS 機能](#)を参照してください。

Secure Mail でサポートされている Android の機能については、[Secure Mail の Android 機能](#)を参照してください。

Secure Mail でサポートされている iOS および Android の機能については、[Secure Mail の iOS および Android 機能](#)を参照してください。

ユーザーヘルプドキュメントについては、Citrix ユーザーヘルプセンターの[Citrix Secure Mail](#)ページを参照してください。

Secure Mail の新機能

以下のセクションでは、Secure Mail の現在および以前のリリースにおける新機能について説明します。

ユーザーヘルプドキュメントについては、Citrix User Help Center の [Citrix Secure Mail](#) ページを参照してください。

注:

- Secure Mail は、2023年9月現在、Android 7.x および iOS 12.x をサポートしていません。
- Secure Mail は、Android バージョン 25.6.0 および iOS バージョン 25.5.0 の時点では Intune をサポートしていません。

現在のバージョンの新機能

iOS 用 セキュアメール 26.8.0

iOS/iPadOS 27 のサポート

iOS 用 Secure Mail 26.8.0 のリリース以降、このアプリは iOS/iPadOS 27 と互換性があります。デバイスを iOS/iPadOS 27 にアップグレードして、Secure Mail の最新バージョンを引き続き使用できます。

Secure Mail をデフォルトのメールアプリとして設定するサポート

iOS 用 Secure Mail 26.8.0 のリリース以降、Secure Mail をデバイスのデフォルトのメールアプリとして設定できます。デフォルトとして設定すると、連絡先、Safari、またはその他のアプリで `mailto:` リンクをタップすると、ネイティブのメールアプリではなく Secure Mail で新しい下書きが開きます。その結果、ビジネスメールは管理対象コンテナ内に留まります。

Secure Mail をデフォルトのメールアプリとして設定するには、[Secure Mail をデフォルトのメールアプリとして設定するサポート](#) を参照してください。

バグ修正の詳細については、[既知の問題と修正された問題](#) を参照してください。

以前のバージョンの新機能

Android版セキュアメール 26.5.0

Android 17のサポート

Android版Secure Mail 26.5.0のリリース以降、アプリはAndroid 17と互換性があります。デバイスをAndroid 17にアップグレードし、Secure Mailの最新バージョンを引き続き使用できます。

バグ修正の詳細については、[既知の問題と修正済みの問題](#)を参照してください。

iOS版セキュアメール 26.5.0

このリリースでは、全体的なパフォーマンスと安定性の向上に役立ついくつかの問題に対処しています。

バグ修正の詳細については、[既知の問題と修正済みの問題](#)を参照してください。

iOS版セキュアメール 26.1.0

モバイルレスポンシブなメール書式設定のサポート

iOS版Secure Mail 26.1.0のリリース以降、アプリはメールメッセージのモバイルレスポンシブな書式設定の改善をサポートします。

バグ修正の詳細については、[既知の問題と修正済みの問題](#)を参照してください。

Android版セキュアメール 25.12.0

16KBメモリページサイズのサポート

Android版Secure Mail 25.12.0のリリース以降、アプリはパフォーマンスを最適化し、Google Playの要件に準拠するために16KBのメモリページサイズをサポートします。

バグ修正の詳細については、[既知の問題と修正済みの問題](#)を参照してください。

iOS版 セキュアメール 25.9.0

連絡先の双方向同期のサポート

iOS版Secure Mail 25.9.0のリリース以降、このアプリはSecure Mail iOSアプリとデバイスの連絡先システム間で双方向に同期する連絡先をサポートします。Secure Mailバージョン25.9.0にアップグレードすると、既存のAndroid実装と一致する連絡先同期の継続的なサポートと互換性が保証されます。

注：

- この機能はデフォルトで無効になっており、管理者はこの機能を有効にするためにCitrixカスタマーサポートに連絡する必要があります。
- この機能はiCloud連絡先同期の影響を受け、データ競合を引き起こす可能性があります。問題が発生した場合は、iCloud連絡先同期を無効にしてください。

iOS 15の非推奨化

iOS版Secure Mail 25.9.0のリリース以降、iOS 15のサポートは非推奨となり、アプリはiOS 15を実行しているデバイスをサポートしません。代替策として、利用可能な最新バージョンのiOSにアップグレードできます。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

Android版 セキュアメール 25.8.0

Android APIレベル35のサポート

Android版Secure Mail 25.8.0のリリース以降、Google Playアプリの更新要件に準拠するため、アプリはAndroid APIレベル35をサポートします。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

Android版 セキュアメール 25.6.0

レガシーMDXの非推奨化

Android版Secure Mail 25.6.0のリリース以降、アプリは常にMAM SDKポリシーコンテナモードを使用し、Intuneとの統合はサポートしていません。制限事項の詳細については、「[制限事項](#)」を参照してください。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

iOS版 セキュアメール 25.5.0

iOS 26のサポート

iOS版Secure Mail 25.5.0のリリース以降、アプリはiOS 26で動作するデバイスをサポートします。Secure Mailバージョン25.5.0にアップグレードすることで、iOS 26にアップデートされたデバイスに対する継続的なサポートと互換性が保証されます。

TLS 1.3プロトコルのサポート

iOS版Secure Mail 25.5.0のリリース以降、アプリはiOSデバイスでTLS 1.3プロトコルをサポートします。TLS 1.3はTLSプロトコルの最新バージョンであり、TLS 1.2と比較して、より高速なパフォーマンス、強化されたセキュリティ、およびサイバー攻撃に対する優れた回復力を提供します。TLS 1.3はネットワーク遅延も削減し、HTTPS接続の高速化とユーザーエクスペリエンスの向上をもたらします。

TLS 1.3の詳細については、「[The Transport Layer Security \(TLS\) Protocol Version 1.3](#)」を参照してください。

注：

この機能はデフォルトで無効になっており、管理者はこの機能を有効にするためにCitrixカスタマーサポートに連絡する必要があります。

Domino 14 FP1のサポート

iOS版Secure Mail 25.5.0のリリース以降、アプリはHCL Dominoバージョン14.0 FP1をサポートします。

レガシーMDXの非推奨化

iOS版Secure Mail 25.5.0のリリース以降、アプリは常にMAM SDKポリシーコンテナモードを使用し、Intuneとの統合はサポートしていません。制限事項の詳細については、「[制限事項](#)」を参照してください。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

Android版セキュアメール 25.3.0

Android 16のサポート

Android版Secure Mail 25.3.0のリリース以降、このアプリはAndroid 16と互換性があります。デバイスをAndroid 16にアップグレードして、Secure Mailの最新バージョンを引き続き使用できます。

大容量添付ファイルのダウンロードのサポート

Android版Secure Mail 25.3.0のリリース以降、このアプリは10MBを超える添付ファイルのダウンロードをサポートしています。

注:

この機能はデフォルトで無効になっており、管理者はこの機能を有効にするためにCitrixカスタマーサポートに連絡する必要があります。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

Android版セキュアメール 25.1.0

TLS 1.3プロトコルのサポート

Android版Secure Mail 25.1.0のリリース以降、このアプリはAndroidデバイスでTLS 1.3プロトコルをサポートしています。TLS 1.3はTLSプロトコルの最新バージョンであり、TLS 1.2と比較して、より高速なパフォーマンス、強化されたセキュリティ、およびサイバー攻撃に対する優れた回復力を提供します。TLS 1.3はネットワーク遅延も削減し、より高速なHTTPS接続とより良いユーザーエクスペリエンスをもたらします。

TLS 1.3の詳細については、「[The Transport Layer Security \(TLS\) Protocol Version 1.3](#)」を参照してください。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

iOS版セキュアメール 25.1.0

大容量添付ファイルのダウンロードのサポート

iOS版Secure Mail 25.1.0のリリース以降、アプリは10MBを超える添付ファイルのダウンロードをサポートします。

注:

この機能はデフォルトで無効になっており、管理者はこの機能を有効にするためにCitrixカスタマーサポートに連絡する必要があります。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

Android版セキュアメール 24.11.0

ウォーターマークなしでメールの添付ファイルを表示

Android版Secure Mailバージョン24.9.1以前を使用している場合、メールの添付ファイルを表示する際にウォーターマークが表示されることがあります。ウォーターマークなしでメールの添付ファイルを表示するには、Android版Secure Mailバージョン24.11.0以降にアップグレードしてください。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

iOS版セキュアメール 24.11.0

このリリースでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

iOS版セキュアメール 24.9.0

iOS 18のサポート

iOS版Secure Mailバージョン24.9.0のリリース以降、Secure MailはiOS 18以降で動作するデバイスをサポートします。Secure Mailバージョン24.9.0にアップグレードすることで、iOS 18にアップデートされたデバイスに対する継続的なサポートと互換性が保証されます。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」を参照してください。

Android版セキュアメール 24.9.1

Android 15のサポート

Secure Mailのバージョンを24.9.1にアップグレードすると、Android 15にアップデートされたデバイスに対する継続的なサポートが保証されます。

バグ修正の詳細については、「[既知の問題と修正された問題](#)」([/ja-jp/citrix-secure-mail/known-fixed-issues.html](#))を参照してください。

Android版セキュアメール 24.9.0

APIレベル34のサポート

Secure Mailは、Google Playの現在のターゲットAPI要件であるAPIレベル34をサポートしています。

バグ修正の詳細については、「既知の問題と修正された問題」([/ja-jp/citrix-secure-mail/known-fixed-issues.html](https://citrix.com/ja-jp/citrix-secure-mail/known-fixed-issues.html))を参照してください。

Android版セキュアメール 24.7.0

このリリースでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

iOS版セキュアメール 24.3.0

このリリースでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

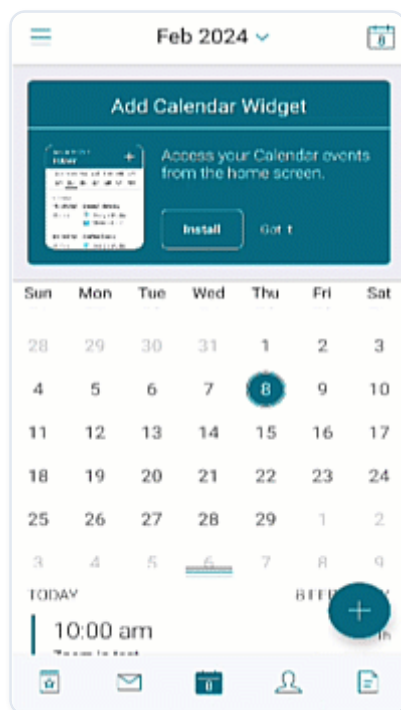
iOS版セキュアメール 24.2.0

このリリースでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

Android版セキュアメール 24.1.0

カレンダーイベントのズームイン機能に対応

リリース24.1.0以降、Android版Secure Mailはカレンダーイベントのズームイン機能に対応しています。この機能はデフォルトで有効になっています。現在、ズームイン機能はメッセージとカレンダーイベントの両方に適用されます。強化されたズームイン機能は、より良いユーザーエクスペリエンスを提供します。



iOS版セキュアメール 23.9.0

iOS 17に対応

本リリース以降、Secure MailはiOS 17を実行しているデバイスでサポートされます。Secure Mailバージョン23.9.0にアップグレードすることで、iOS 17にアップデートされたデバイスへの継続的なサポートが保証されます。

HCL Domino 12に対応

本リリース以降、Android版およびiOS版Secure Mailは、HCL Dominoバージョン12.0.2 FP2およびHCL Travelerバージョン12.0.2.1 Build 202302010413_30に対応しています。

注:

HCL Domino 11からHCL Domino 12にアップグレードする場合は、Dominoサーバーの **notes.ini** ファイルで以下のユーザーエージェントを更新してください。これにより、下書き同期やカレンダー添付ファイルなど、Secure MailのすべてのActiveSync 16.1機能が引き続き正常に機能することが保証されます。詳細については、「[HCL Traveler Exchange ActiveSync 16.1サポート向けCitrix Secure Mailクライアントを有効にする方法](#)」を参照してください。

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

Android版セキュアメール 23.8.2

透かしなしでメールの添付ファイルを表示

Android版Secure Mailバージョン23.8.1以前を使用している場合、メールの添付ファイルを表示すると透かしが表示されます。透かしなしでメールの添付ファイルを表示するには、Android版Secure Mailバージョン23.8.2以降にアップグレードしてください。

注:

October 31, 2023以降、バージョン23.8.1へのアップグレードでは、メール添付ファイルの透かしの問題は解決されません。したがって、バージョン23.8.2に更新することをお勧めします。

Android向け セキュアメール 23.8.1

透かしなしでメール添付ファイルを表示

Android版Secure Mailバージョン23.8.0以前を使用している場合、メール添付ファイルを表示する際に透かしが表示されることがあります。透かしなしでメール添付ファイルを表示するには、Android版Secure Mailバージョン23.8.1以降にアップグレードしてください。

HCL Domino 12のサポート

このリリース以降、AndroidおよびiOS版Secure Mailは、HCL Dominoバージョン12.0.2 FP2およびHCL Travelerバージョン12.0.2.1 Build 202302010413_30をサポートします。

注:

HCL Domino 11からHCL Domino 12にアップグレードする場合は、Dominoサーバーの **notes.ini** ファイルで以下のユーザーエージェントを更新してください。これにより、下書き同期やカレンダー添付ファイルなど、Secure MailのすべてのActiveSync 16.1機能が引き続き正常に機能するようになります。詳細については、「[HCL Traveler Exchange ActiveSync 16.1サポート向けCitrix Secure Mailクライアントを有効にする方法](#)」を参照してください。

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

Android版 セキュアメール 23.8.0

Android 14のサポート

このリリース以降、Secure MailはAndroid 14を実行しているデバイスでサポートされます。
Secure Mailバージョン23.8.0にアップグレードすることで、Android 14に更新されたデバイスに対する継続的なサポートが保証されます。

Android版 セキュアメール 23.7.0

Microsoft Exchange累積更新プログラム13のサポート

23.7.0リリース以降、Secure MailはMicrosoft Exchange Server 2019累積更新プログラム13をサポートします。

オンプレミスExchangeでのハイブリッドモダン認証のサポート

Secure Mailは、Exchange Server 2016の累積更新プログラム8およびExchange Server 2013の累積更新プログラム19で、ハイブリッドモダン認証 (HMA) をサポートするようになりました。

iOS 用 セキュアメール 23.7.0

オンプレミスExchangeでのハイブリッドモダン認証のサポート

Secure Mailは、Exchange Server 2016の累積更新プログラム8およびExchange Server 2013の累積更新プログラム19で、ハイブリッドモダン認証 (HMA) をサポートするようになりました。

ダークモード

23.7.0リリース以降、Secure Mailはダークモードをサポートしています。ダークモードでメールを表示するには、アプリの > > の順に選択し、 を選択します。

Android 用 セキュアメール 23.6.0

ダークモード

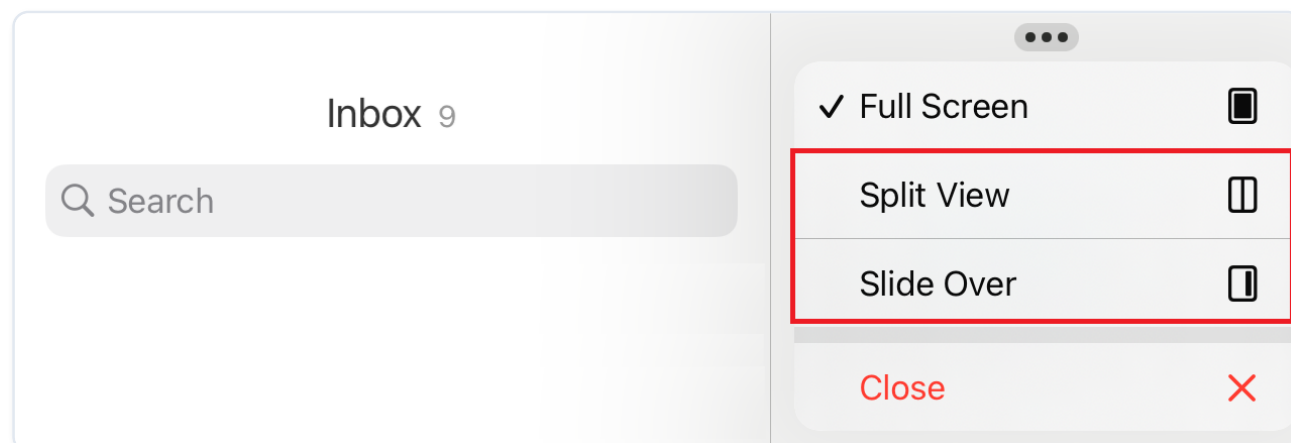
23.6.0リリース以降、Secure Mailはダークモードをサポートしています。ダークモードでメールを表示するには、アプリの > > の順に選択し、 を選択します。

iOS 用 セキュアメール 23.5.0

分割表示モードとスライドオーバーモードでのマルチタスク

23.5.0リリース以降、Secure MailはiPadデバイスでのマルチタスクをサポートしています。

Secure Mailを開き、省略記号 (...) をタップして、または オプションのいずれかを選択してマルチタスクを実行します。この機能は、ユーザーの生産性向上に役立ちます。



では、2番目のアプリが現在のアプリの隣に表示されます。レイアウトでは、2番目のアプリが全画面モードで開き、現在のアプリは画面の右または左に移動できる小さなウィンドウに縮小されます。

セキュアメール 23.3.5

アンドロイド版 セキュアメール

このリリースにはバグ修正が含まれています。

Secure Mail バージョン 23.2.0

Android 用 セキュアメール

このリリースにはバグ修正が含まれています。

iOS 用 セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 22.11.0

Android 用セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 22.9.0

iOS 用 セキュアメール

Secure Mail は iOS 16 をサポートするようになりました。

アンドロイド版 Secure Mail

Secure Mail は Android 13 をサポートするようになりました。

セキュアメール 22.6.2

iOS用 セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 22.6.0

このリリース以降、Secure Mail は Exchange Server 2016 Cumulative Update 23 をサポートします。

iOS用 セキュアメール

このリリースにはバグ修正が含まれています。

Android用 セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 22.3.0

iOS用 セキュアメール

HCL Domino 11 のサポート。 このリリース以降、iOS 用 Secure Mail は HCL Domino 11 (旧 Lotus Notes) をサポートします。

Google Analytics。 Citrix Secure Mail は、製品品質を向上させるために、アプリの統計情報と使用状況分析データを収集するために Google Analytics を使用します。Citrix は、その他の個人ユーザー情報を収集または保存しません。Secure Mail の Google Analytics を無効にする方法の詳細については、「[Google Analytics を無効にする](#)」を参照してください。

Android用 セキュアメール

HCL Domino 11のサポート。 このリリース以降、Android版Secure MailはHCL Domino 11（旧 Lotus Notes）をサポートします。

Google Analytics。 Citrix Secure Mailは、製品品質を向上させるために、アプリの統計情報と利用状況分析データを収集するためにGoogle Analyticsを使用します。Citrixは、その他の個人ユーザー情報を収集または保存しません。Secure MailのGoogle Analyticsを無効にする方法の詳細については、「[Google Analyticsを無効にする](#)」を参照してください。

セキュアメール 22.2.0

iOS版セキュアメール

フィードを管理するオプションは、バージョン21.5.0で非推奨になりました。このリリースでは、iOS版Secure Mailに以下のデフォルトフィードカードのみが表示されます。

- 未読
- 会議の招待
- 今後の会議
- マネージャーから

現在この機能が有効になっていて構成されている場合、設定はデフォルトのカードで上書きされます。

Android版セキュアメール

フィードを管理するオプションは、バージョン21.5.0で非推奨になりました。このリリースでは、iOS版Secure Mailに以下のデフォルトフィードカードのみが表示されます。

- 未読
- 会議の招待
- 今後の会議
- マネージャーから

この機能が現在有効になっていて構成されている場合、設定はデフォルトのカードで上書きされます。

Secure Mail バージョン 21.12.0

iOS 向け セキュアメール

カスタムユーザーエージェントのサポート。このリリースから、Active Directory フェデレーションサービス (AD FS) または ID プロバイダー (IdP) 用の Microsoft Office 365 での認証にカスタムユーザーエージェントを使用できます。この機能を使用するには、Citrix Endpoint Management™

コンソールで **モダン認証用のカスタムユーザーエージェント ポリシー**を有効にして構成する必要があります。

Android 向け セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 21.11.0

Android 用セキュアメール

自己診断ツール

Secure Mail for Android で発生する可能性のある問題をトラブルシューティングできるようになりました。アプリ設定の **サポート** メニューオプションの下にある **トラブルシューティング** ボタンを使用します。問題を解決するには、Secure Mail を開き、**設定** > **トラブルシューティング** に移動します。



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

トラブルシューティングのために、次のメニュー項目が表示されます。

- デフォルトのアプリ設定をクリア
- デフォルトのリマインダー時間
- バッテリー最適化を無視
- カレンダー通知を管理
- メール通知を管理
- 画像を表示
- カレンダーを同期
- 連絡先を同期
- メールを同期
- 受信トレイの同期頻度
- メールの同期期間

これらの設定がすべてデフォルトに戻されてもSecure Mailで問題が発生する場合は、管理者に連絡してください。

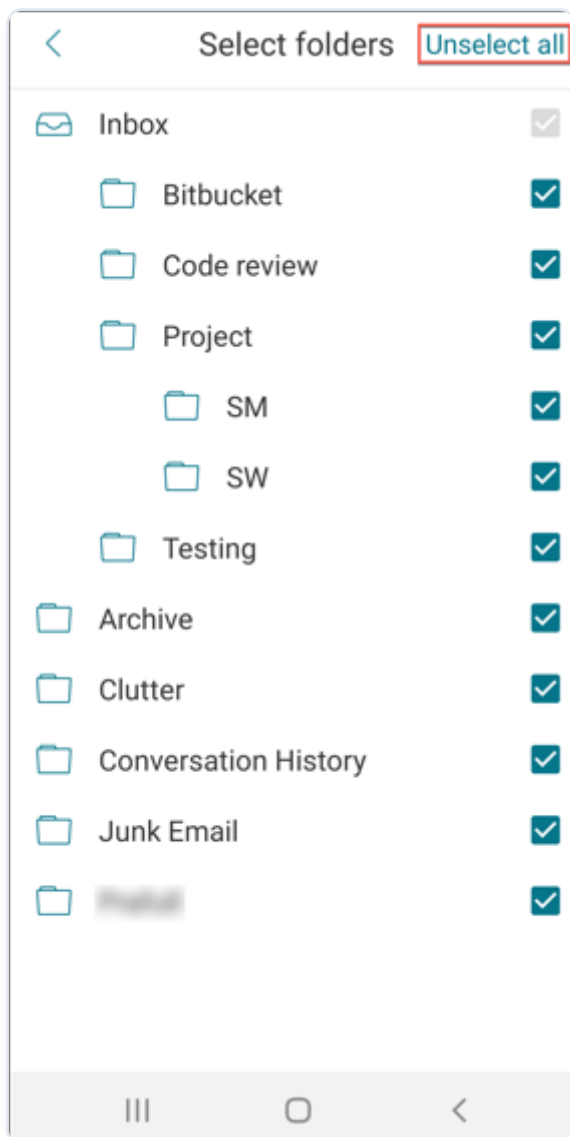
管理者に連絡(/en-us/mobile-productivity-apps/media/troubleshoot-nothing-to-fix.png)

サブフォルダー通知の機能強化

設定 > 通知 > メールフォルダーに移動し、**フォルダーの選択画面**で**すべて選択**オプションをクリックすると、すべてのサブフォルダーの通知を受信できるようになりました。

すべて選択(/en-us/mobile-productivity-apps/media/select-all.png)

すべて選択解除をクリックすると、すべてのサブフォルダーの通知の受信を停止できます。



セキュアメール 21.10.5

このリリース以降、Secure Mail は Exchange Server 2019 Cumulative Update 11 および Exchange Server 2016 Cumulative Update 22 をサポートします。

iOS 用セキュアメール

このリリースにはバグ修正が含まれています。

Android 用セキュアメール

このリリースにはバグ修正が含まれています。

注記:

Secure Mail の Android 7 のサポートは、2021年10月をもって終了します。

セキュアメール 21.10.0

Android 用セキュアメール

- **Android 12 のサポート。**このリリース以降、Secure Mail は Android 12 を実行しているデバイスでサポートされます。
- Secure Mail は、Android 11 の Google Play の現在のターゲット API 要件 (API レベル 30) を満たしています。

セキュアメール 21.9.1

Android 用セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 21.9.0

iOS用セキュアメール

このリリースにはバグ修正が含まれています。

Android用セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 21.8.5

Android用セキュアメール

登録済みデバイスでのAndroid 12 Beta 4のサポート。 Secure MailはAndroid 12 Beta 4をサポートするようになりました。Android 12 Beta 4へのアップグレードを検討している場合は、まず Secure Hubをバージョン21.7.1にアップデートしてください。Secure Hub 21.7.1は、Android 12 Beta 4にアップグレードするために必要な最小バージョンです。このリリースにより、すでに登録されているユーザーはAndroid 11からAndroid 12 Beta 4へシームレスにアップグレードできます。

注:

CitrixはAndroid 12のDay 1サポートを提供することにコミットしています。Secure Mailの以降のバージョンでは、Android 12を完全にサポートするためのさらなるアップデートが提供されます。

セキュアメール 21.8.0

iOS用セキュアメール

ハイブリッド環境におけるExchange Serverのメールベースの自動検出

iOS版Secure Mailでは、メールアドレスを使用してMicrosoft 365 Exchangeアカウントを設定でき、ハイブリッドExchangeサーバーでのスムーズなログインエクスペリエンスを保証します。この機能は、オンプレミスExchangeサーバーでも利用できます。

注:

Exchange Server の自動検出機能を有効にしてください。

Microsoft Office 365 で最新認証を実行するセットアップでのリッチプッシュ通知

このリリースでは、ネットワークアクセスポリシーが **Tunneled - Web SSO** に設定され、Exchange Web Services (EWS) ホスト名が **Exclusion List** に含まれている場合、Secure Mail はプッシュ通知をサポートします。EWS と ActiveSync ホストが同じである場合は、ActiveSync ホストが **Exclusion List** ポリシーに含まれていることを確認してください。

Secure Mail のデュアルモード

モバイルアプリケーション管理 (MAM) SDK は、iOS プラットフォームでカバーされていない MDX 機能の領域を置き換えるために利用できます。MDX ラッピングテクノロジーは、2023 年 7 月にサポート終了 (EOL) を迎える予定です。

Citrix Secure Mail™ は、2023 年 7 月に予定されている MDX EOL に備えて、MDX と MAM SDK の両方のフレームワークでリリースされています。エンタープライズアプリケーションの管理を継続するには、MAM SDK を組み込む必要があります。Citrix は **MAM SDK** への切り替えを推奨しています。デュアルモード機能は、Secure Mail アプリを新しい MAM SDK モデルに移行する方法を提供することを目的としています。

デュアルモード機能を使用すると、MDX (現在は **Legacy MDX**) を使用してアプリの管理を継続するか、新しい **MAM SDK** に切り替えることができます。**MDX or MAM SDK policy container** のポリシー設定には、次のオプションがあります。

- **MAM SDK**
- **レガシー MDX**

The screenshot shows the Citrix Cloud Endpoint Management console. The left sidebar has a menu with 'MDX' and a list of app types: '1 App Information', '2 Platform' (with a 'Select All' link), '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. Under '2 Platform', 'iOS' is selected. The main area shows the configuration for an app named 'Secure Mail'. Fields include 'File name', 'App Description', 'App version', 'Minimum OS version', 'Maximum OS version', and 'Excluded devices'. There are several toggle switches: 'Remove app if MDM profile is removed' (ON), 'Prevent app data backup' (ON), 'Force app to be managed' (ON), and 'App deployed via Volume purchase' (OFF). At the bottom, there is a section for 'MDX or MAM SDK policy container' with two radio buttons: 'MAM SDK' and 'Legacy MDX'. The 'Legacy MDX' option is selected and highlighted with a red box. Below this is a section for 'MDX Policies' with a sub-section for 'Authentication'.

MDX or MAM SDK policy container ポリシーで、オプションを **Legacy MDX** から **MAM SDK** に変更できます。**MAM SDK** から **Legacy MDX** への切り替えは、アプリの再インストールが必要になるため、推奨されません。デフォルト値は **Legacy MDX** です。Secure Mail と Secure Web の両方で、デバイス上で同じポリシーモードが実行されていることを確認してください。同じデバイスで2つの異なるモードを実行することはできません。

MAM SDK モードを選択すると、アプリは自動的に MAM SDK フレームワークに切り替わり、管理者が追加の操作を行うことなくデバイスポリシーが更新されます。

注:

Legacy MDX から **MAM SDK** フレームワークに切り替える場合、**Network access** ポリシーは **Tunneled – Web SSO** または **Unrestricted** のいずれかに変更する必要があります。

前提条件

デュアルモード機能の展開を成功させるには、以下の要件が満たされていることを確認してください。

- Citrix Endpoint Managementをバージョン10.12 RP2以降、または10.11 RP5以降にアップデートしてください。
- モバイルアプリをバージョン21.8.0以降にアップデートしてください。

- 組織がサードパーティ製アプリを使用している場合は、MAM SDKフレームワークに切り替える前に、サードパーティ製アプリにMAM SDKを組み込むようにしてください。管理対象アプリはすべて、一度にMAM SDKに移行する必要があります。

制限事項

- MAM SDKはプラットフォームベースの暗号化のみをサポートしており、MDX暗号化はサポートしていません。
- Citrix Endpoint Managementをバージョン10.12 RP2以降、または10.11 RP5以降にアップデートしない場合、重複するポリシーエントリが表示されます。ポリシーファイルがバージョン21.8.0以降で実行されている場合、重複エントリが作成されます。
- アプリ管理のMAM SDKモードに切り替えると、一部の機能はサポートされなかったり、利用できなくなったりします。また、Open-inやコピー/貼り付けなどのアクションでは、異なるモードのアプリ間の相互運用はサポートされません。たとえば、**Legacy MDX**モードで管理されているアプリから**MAM SDK**モードで管理されているアプリにコンテンツをコピーしたり、その逆を行ったりすることはできません。MAM SDKモードで利用できない機能については、以下の表を参照してください。

機能	レガシーMDX	MAM SDK
共有デバイス	はい	いいえ
イントラネット	はい	いいえ
SMIME共有証明書保管庫	はい	いいえ
派生資格情報	はい	いいえ
UIWebViewトンネリング	はい	いいえ
フルVPN	はい	いいえ

- 以下のポリシーは非推奨であり、MAM SDKモードでは利用できません。
 - 許可されたSecure Webドメイン
 - 許可されたWi-Fiネットワーク
 - 代替シトリックス ゲートウェイ
 - 証明書ラベル
 - Citrixレポート

- 明示的なログオフ通知
- micro VPNセッションが必要
- micro VPNセッションの猶予期間（分）
- レポートファイルキャッシュの最大値
- Wi-Fiを必須にする
- レポートはWi-Fi経由でのみ送信
- アップロードトークン

注：

内部サーバーへの認証にクライアント証明書を使用している場合、そのクライアント証明書は Access Gatewayで使用されているものと同じである必要があります。

MAM SDK の詳細については、以下の記事を参照してください。

- [MAM SDK の概要](#)
- [MAM SDK の最新リリース](#)
- [Citrix Developer ドキュメント: モバイルアプリケーション統合](#)
- [Citrix ブログ投稿](#)

Android用 セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 21.7.0

アイオーエス用 セキュアメール

このリリースにはバグ修正が含まれています。

Android用 セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 21.6.0

アイオーエス用 セキュアメール

このリリース以降、以下の ネットワークアクセス ポリシーオプションはサポートされなくなりました。

- 以前の設定を使用
- トンネル化 - フルVPN
- トンネル化 - フルVPNおよびWeb SSO

「Tunneled - Full VPN」または「Tunneled - Full VPN and Web SSO」ポリシーを使用している場合は、「Tunneled - Web SSO」ポリシーに切り替える必要があります。廃止されたポリシーを使い続けると、メールが同期されなくなります。

注:

Secure Ticket Authority (STA) を使用するには、ネットワークアクセスポリシーを「Tunneled - Web SSO」に設定する必要があります。

アンドロイド版Secure Mail

トラブルシューティングオプションを使用した自己診断のサポート。この機能を使用すると、アプリが正しく機能するために不可欠な基本設定がデフォルトに設定されているかどうかを確認できます。特定のSecure Mail設定に関してエラーが発生している場合は、この機能を使用してアプリのトラブルシューティングを行ってください。

この機能にアクセスするには、アプリの設定を開き、**サポート**の下にある**トラブルシューティング**をタップします。確認および編集できる以下のメニューオプションが表示されます。

- メール同期期間
- 受信トレイ同期頻度
- メールを同期
- 画像を表示
- デフォルトのリマインダー時間
- カレンダーを同期
- 連絡先を同期

設定を既定値に戻すには、**APPLY CHANGE** をタップします。すべての設定を既定値に戻すには、**APPLY CHANGES TO ALL** をタップします。

セキュアメール 21.5.0

このリリース以降、Secure Mail は Exchange Server 2019 Cumulative Update 9 および Exchange Server 2016 Cumulative Update 20 をサポートします。

iOS向けセキュアメール

- **Secure Mail のカレンダーイベントで Microsoft Teams 会議を作成する。** iOS 用 Secure Mail では、カレンダーイベントの作成中に Microsoft Teams 会議の招待を作成できます。Microsoft Teams 会議を作成するには、**Microsoft Teams Meeting** トグルをオンにします。会議の招待リンクと詳細は、イベントの詳細とともに自動的に送信されます。詳細については、「[Secure Mail のカレンダーイベントで Microsoft Teams 会議を作成する](#)」を参照してください。
- このリリース以降、以下の **ネットワークアクセス** ポリシーオプションは非推奨となり、バージョン 21.6.0 以降ではサポートされません。
 - 以前の設定を使用
 - トンネル化 - フル VPN
 - トンネル化 - フル VPN および Web SSO

トンネル化 - フル VPN または トンネル化 - フル VPN および Web SSO ポリシーを使用している場合は、トンネル化 - Web SSO ポリシーに切り替える必要があります。非推奨のポリシーを使い続けると、メールの同期に失敗します。

注:

トンネル化 - フル VPN を使用しており、Secure Ticket Authority (STA) が構成されている場合、最新の認証画面の読み込みに失敗します。

Android向けセキュアメール

- このリリースでは、**必須アップグレードの無効化** のその他のポリシーは Citrix Endpoint Management コンソールで利用できなくなりました。アプリは Play ストアで利用可能な最新バージョンに自動的にアップグレードされます。
- Secure Mail for Androidでは、**フィードの管理** オプションは本リリースで非推奨になりました。この機能を現在有効にして構成している場合、フィードウィンドウで設定した好みに基づいてフィードが引き続き表示されます。新規ユーザーの場合、または以前にすべてのフィードカードを削除している場合は、以下のデフォルトのフィードカードが利用可能です。
 - 未読
 - 会議の招待
 - 今後の会議
 - マネージャーから

セキュアメール 21.4.5

Android 版 セキュアメール

メールベースの自動検出サポート。Secure Mail for Androidでは、メールアドレスを使用してMicrosoft O365 Exchangeアカウントを構成でき、スムーズなログインエクスペリエンスが保証されます。この機能は、ハイブリッド環境で自動検出が有効になっている場合、オンプレミスユーザーも利用できます。

注：

この機能は、Exchange Server 2016 Cumulative Update 3以降でのみサポートされています。

セキュアメール 21.4.0

iOS 版 セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 21.3.5

Android 版 セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 21.3.0

iOS版セキュアメール

Secure Mail iOSの展開ターゲットがiOS 12.2に変更されました。iOS版Microsoft Intune App SDKバージョン14.1.3では、ターゲットアプリの最小iOS展開バージョンがiOS 12.2である必要があります。この要件に準拠するため、Secure Mailの展開ターゲットはiOS 12.2に更新されました。

Android版セキュアメール

Secure MailカレンダーイベントでMicrosoft Teams会議を作成する。Android版Secure Mailでは、カレンダーイベントの作成中にMicrosoft Teams会議の招待を作成できます。Microsoft Teams会議を作成するには、**Microsoft Teams会議**トグルをオンにします。会議の招待リンクと詳細は、イベントの詳細とともに自動的に送信されます。詳細については、「[Secure MailカレンダーイベントでMicrosoft Teams会議を作成する](#)」を参照してください。

セキュアメール 21.2.0

このリリース以降、Secure MailはExchange Server 2019累積更新プログラム8およびExchange Server 2016累積更新プログラム19をサポートします。

iOS版セキュアメール

- **Secure Mailのカラー刷新。** Secure MailはCitrixブランドのカラーアップデートに準拠しています。

Android版セキュアメール

- **Secure Mailのカラー刷新。** Secure MailはCitrixブランドのカラーアップデートに準拠しています。
- **Microsoft Intuneのサポート。** Android版Secure Mailは、Microsoft Intune 7.2.2の最新バージョンをサポートしています。
- **折りたたみ式デバイスでの安定した動作。** Android版Secure Mailには、折りたたみ式デバイスでの安定した動作のための修正が含まれています。

セキュアメール 21.1.5

セキュアメール iOS版

このリリースにはバグ修正が含まれています。

セキュアメール 21.1.0

このリリースにはバグ修正が含まれています。

セキュアメール 20.12.0

セキュアメール iOS版

このリリースにはバグ修正が含まれています。

セキュアメール 20.11.0

注：

Exchange Server 2010のサポートは October 13, 2020 に終了しました。

セキュアメール 20.10.5

セキュアメール iOS版

このリリースにはバグ修正が含まれています。

セキュアメール Android版

AndroidXライブラリのサポート。 Googleの推奨に従い、Secure Mailは**android.support**パッケージライブラリの代替である**AndroidX**ライブラリをサポートしています。

セキュアメール 20.10.0

このリリース以降、Secure Mail は Exchange Server 2019 累積更新プログラム 7 および Exchange Server 2016 累積更新プログラム 18 をサポートします。

iOS版セキュアメール

Secure Mail から Microsoft Teams 会議に参加する。 Secure Mail for iOS では、カレンダーの招待から直接 Microsoft Teams 会議に参加できます。Microsoft Teams アプリがインストールされている場合、アプリが開き、会議に参加できます。アプリがインストールされていない場合、App Store に移動して Microsoft Teams をインストールするオプションが表示されます。 <https://teams.microsoft.com/l/meetup-join/meetinglink> 形式の会議の場合、アプリが開き、直接会議に参加できます。

注:

管理者が許可された URL ポリシーに `+\\^msteams:` を含めるようにしてください。詳細については、「[アプリの操作 \(送信 URL\)](#)」を参照してください。

Android版セキュアメール

- **Secure Mail から Microsoft Teams 会議に参加する。** Secure Mail for Android では、カレンダーの招待から直接 Microsoft Teams 会議に参加できます。Microsoft Teams アプリがインストールされている場合、アプリが開き、会議に参加できます。アプリがインストールされていない場合、Google Play に移動して Microsoft Teams をインストールするオプションが表示されます。 <https://teams.microsoft.com/l/meetup-join/>meetinglink> 形式の会議の場合、アプリが開き、直接会議に参加できます。

注:

管理者が制限付き「Open-In」例外リストポリシーに

```
{action=android.intent.action.VIEW scheme=msteams
```

```
package=com.microsoft.teams}
```

を含めるようにしてください。詳細については、「[アプリの操作](#)」を参照してください。

- Secure Mail は、Android 10 向けの Google Play の現在のターゲット API 要件をサポートしています。

セキュアメール 20.9.5

Android版セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 20.9.0

Azure Government Cloud Computingのサポート。 iOSおよびAndroid版Secure Mailは、Azure Active Directoryテナントでの最新認証（OAuth）向けにGovernment Cloud Computing（GCC）Highをサポートしています。Secure Mailは、すべてのGCC Highサービスに対するMicrosoftの必須要件を満たすため、GCC Highのエンドポイントとして登録されています。詳細については、「[Microsoft 365 GovernmentにおけるAzure Active Directoryの新機能](#)」を参照してください。

この変更により、認証のためにAzure Active Directoryテナント上のGCC Highにルーティングされます。また、管理者はAzure Active DirectoryテナントでSecure Mailのアクセス許可を付与する必要があります。

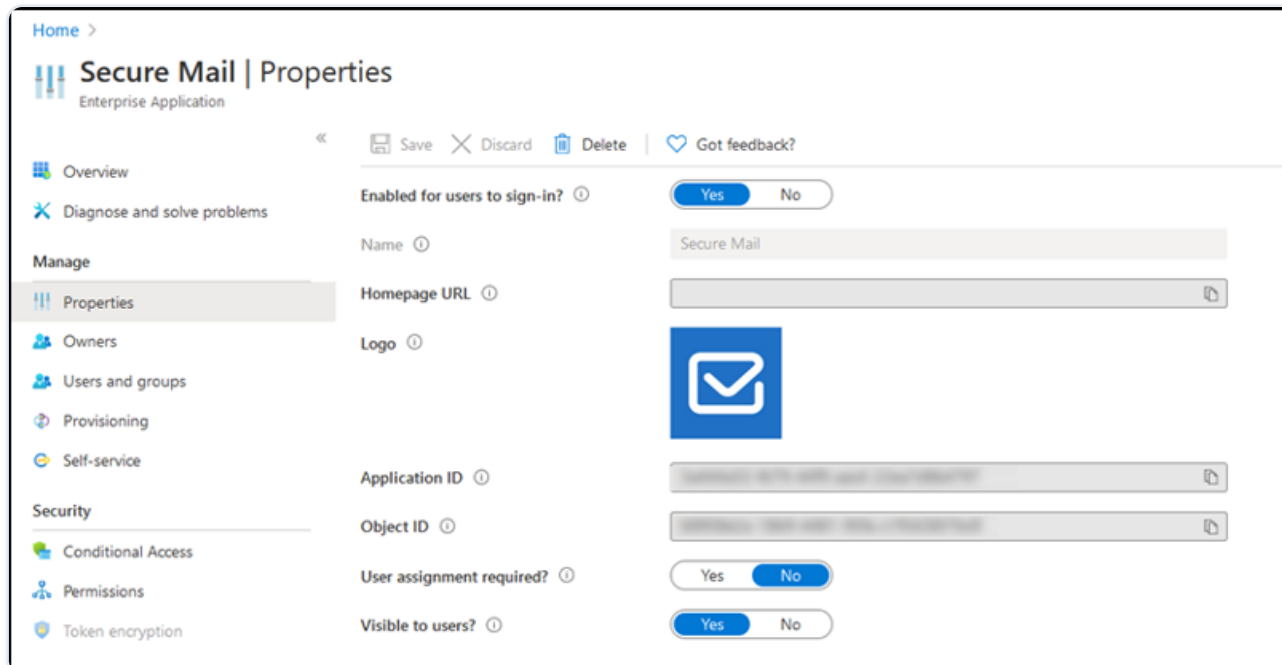
前提条件

Azure Active Directoryのグローバル管理者が以下を実行していることを確認してください。

- デバイスにSecure Mailの最新バージョンをダウンロードします。
- Secure MailアプリでExchangeアカウントを構成し、すべてのユーザーがサインインできるようにAzure Active Directoryでアプリのアクセス許可を付与します。次の画面を参照してください。

注：

これらの手順は、グローバル管理者のみに適用される1回限りの要件です。アプリへのアクセスが許可されれば、App Storeから簡単にアップグレードできます。



アップグレード後

アップグレード後、更新トークンの有効期限が切れると再認証プロンプトが表示され、Azure Active Directory上のGCC Highにリダイレクトされます。認証要求がAzure Active Directory上のGCC Highに送信されていることを確認するために、前述のワークフローを検証してください。

ワークフローは、次のいずれかの方法で検証できます。

- アプリ名が**Secure Mail-GCC High**のSecure Mailが、Azure Active Directoryテナントのサインインページに表示されます。
- Secure Mailログをチェックして、再認証後にリダイレクトが `<https://login.microsoftonline.us>` 経由で発生するかどうかを確認します。

セキュアメール 20.8.5

Android版セキュアメール

Android版Secure MailはAndroid 11をサポートしています。

セキュアメール 20.8.0

このリリース以降、Secure MailはExchange Server 2019累積更新プログラム6およびExchange Server 2016累積更新プログラム17をサポートします。

Android向けセキュアメール

Secure Mailのデュアルモード。 iOSおよびAndroidプラットフォームでカバーされていないMDX機能の領域を置き換えるために、モバイルアプリケーション管理（MAM）SDKが利用可能です。MDXラッピングテクノロジーは、2022年3月にサポート終了（EOL）を迎える予定です。エンタープライズアプリケーションの管理を継続するには、MAM SDKを組み込む必要があります。

バージョン20.8.0以降、Androidアプリは、前述のMDX EOL戦略に備えて、MDXおよびMAM SDKとともにリリースされます。MDXデュアルモードは、従来のMDX Toolkitから新しいMAM SDKへの移行方法を提供することを目的としています。デュアルモードを使用すると、MDX Toolkit（現在はLegacy MDX）を使用してアプリの管理を継続するか、アプリ管理のために新しいMAM SDKに切り替えることができます。

アプリ管理のためにMAM SDKに切り替えると、Citrixはさらなる変更を実装し、管理者からのアクションは不要になります。

MAM SDK（プレビュー）の詳細については、以下の記事を参照してください。

- [MAM SDKの概要](#)
- [MAM SDKの最新リリース](#)
- [Citrix Developerのデバイス管理セクション](#)
- [Citrixブログ投稿](#)

前提条件

デュアルモード機能の展開を成功させるには、以下を確認してください。

- Citrix Endpoint Management をバージョン 10.12 RP2 以降、または 10.11 RP5 以降に更新してください。
- モバイルアプリをバージョン 20.8.0 以降に更新してください。
- ポリシーファイルをバージョン 20.8.0 以降に更新してください。
- 組織がサードパーティ製アプリを使用している場合は、Citrix モバイル生産性向上アプリで MAM SDK に切り替える前に、MAM SDK をサードパーティ製アプリに組み込むようにしてください。管理対象アプリはすべて、一度に MAM SDK に移行する必要があります。

注:

MAM SDK は、すべてのクラウドベースのお客様でサポートされています。

制限事項

- MAM SDK は、Citrix Endpoint Management 展開の Android Enterprise プラットフォームで公開されているアプリのみをサポートします。新しく公開されたアプリの場合、デフォルトの暗号化はプラットフォームベースの暗号化です。
- MAM SDK はプラットフォームベースの暗号化のみをサポートし、MDX 暗号化はサポートしません。
- Citrix Endpoint Management を更新せず、モバイルアプリのポリシーファイルがバージョン 20.8.0 以降で実行されている場合、Secure Mail に重複するネットワークポリシーエントリが表示されます。

Citrix Endpoint Management で Secure Mail を構成すると、デュアルモード機能により、MDX Toolkit (現在は **Legacy MDX**) を使用してアプリの管理を継続するか、新しい **MAM SDK** に切り替えてアプリを管理することができます。MAM SDK はよりモジュール化されており、組織が使用する MDX 機能のサブセットのみを使用できるようにすることを目的としているため、Citrix は **MAM SDK** への切り替えを推奨します。

MDX または MAM SDK ポリシーコンテナのポリシー設定には、次のオプションがあります。

- **MAM SDK**
- **レガシー MDX**

The screenshot displays the Citrix Cloud Endpoint Management interface for configuring an application. The left sidebar shows the 'MDX' section selected under 'Apps'. The main configuration area includes the following fields and settings:

- File name ***: Secure Mail
- App Description ***: Managed Enterprise Application
- App version**: 20.4.5
- Minimum OS version**: 11.0
- Maximum OS version**: (empty)
- Excluded devices**: example: manufacturer or model, ...
- Remove app if MDM profile is removed**: ON
- Prevent app data backup**: ON
- Force app to be managed**: ON
- App deployed via Volume purchase**: OFF
- MDX or MAM SDK policy container**: Legacy MDX (selected), MAM SDK (unselected)

The 'MDX Policies' section is expanded, showing 'Authentication'.

MDXまたはMAM SDKポリシーコンテナポリシーでは、オプションをLegacy MDXからMAM SDKに変更することのみ可能です。MAM SDKからLegacy MDXへの切り替えは許可されておらず、アプリを再公開する必要があります。デフォルト値はLegacy MDXです。Secure MailとSecure Webの両方が同じデバイスで実行されている場合、同じポリシーモードを設定していることを確認してください。同じデバイスで2つの異なるモードを実行することはできません。

iOS向けセキュアメール

メールボックスの同期の最適化。iOS版Secure Mailでは、ユーザーエクスペリエンスを向上させるためにメールボックスの同期が改善されました。カレンダーと連絡先の同期がより高速になりました。同期時間を短縮するため、3週間以上前のメールは切り詰められます。メールを開くと完全なメールを表示できます。

セキュアメール 20.7.5

注：

Android 6.xのサポートは June 30, 2020 に終了しました。

モバイル生産性アプリに関する最新情報については、記事「[最近の発表](#)」を参照してください。

セキュアメール 20.7.0

このリリースにはバグ修正が含まれています。

セキュアメール 20.6.5

このリリースにはバグ修正が含まれています。

セキュアメール 20.6.0

このリリースにはバグ修正が含まれています。

セキュアメール 20.5.0

このリリースにはバグ修正が含まれています。

セキュアメール 20.4.5

Android版 セキュアメール

このリリース以降、Secure MailはExchange Server 2019累積更新プログラム5およびExchange Server 2016累積更新プログラム16をサポートします。

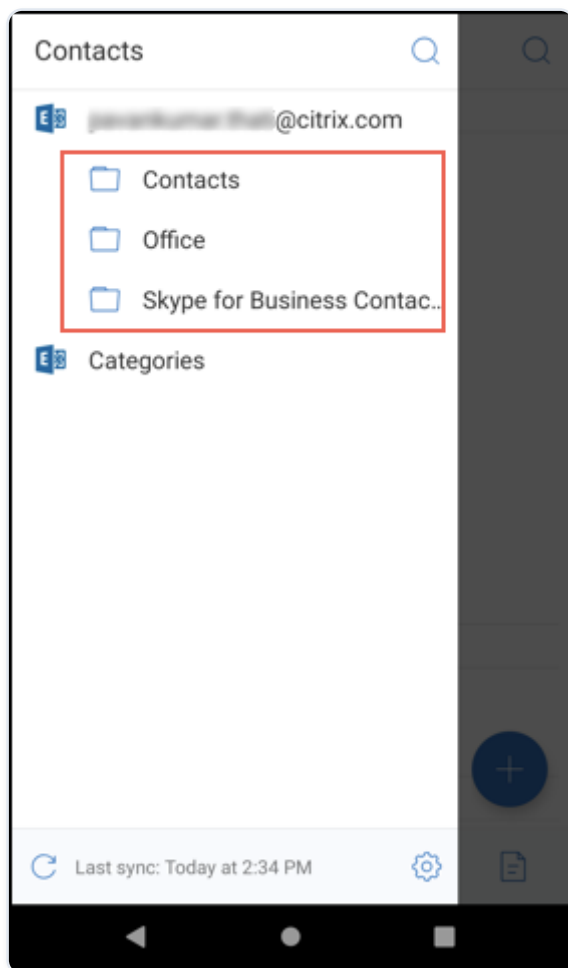
セキュアメール 20.4.0

このリリース以降、Secure MailはExchange Server 2016累積更新プログラム15およびExchange Server 2013累積更新プログラム23をサポートします。

セキュアメール 20.3.0

Android版 セキュアメール

連絡先にフォルダーを作成する。Android版Secure Mailでは、メールアカウントの連絡先セクションでフォルダーを追加、編集、削除できます。



iOS版 セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 20.2.0

Android版 セキュアメール

下書きを最小化

Android版Secure Mailでは、メール作成中に下書きを最小化して、アプリ内を移動できます。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[下書きメールを最小化する](#)」を参照してください。

セキュアメール 20.1.5

iOS版セキュアメール

本リリース以降、Secure MailはExchange Server 2019 Cumulative Update 4をサポートします。

Android版セキュアメール

- **双方向連絡先同期。** Android版Secure Mailでは、ローカルの連絡先リストからSecure Mailの連絡先を作成、編集、削除できます。
- **ICSファイルのサポート。** Android版Secure Mailでは、添付ファイルとして受信したICSファイルをプレビューし、イベントとしてカレンダーにインポートできます。
- 本リリース以降、Secure MailはExchange Server 2019 Cumulative Update 4をサポートします。

セキュアメール 20.1.0

本リリース以降、Secure MailはExchange Server 2016 Cumulative Update 14をサポートします。

セキュアメール 19.12.5

iOS版セキュアメール

本リリースにはバグ修正が含まれています。

Android版セキュアメール

送信済みメールの取り消し。 Android版Secure Mailでは、送信済みメールを取り消すことができます。送信ボタンをタップすると、送信アクションを取り消すことができるトーストメッセージが表示されます。**Undo**をタップすると、送信アクションが元に戻り、メールの編集、メール受信者の変更、添付ファイルの追加または削除、またはメールの破棄ができます。

下書きフォルダーでの添付ファイルの同期。 Android版Secure Mailでは、下書きフォルダーが同期されると、添付ファイルも同期され、すべてのデバイスで利用可能になります。この機能は、Exchange ActiveSyncバージョン16以降を実行しているデバイスで利用できます。

セキュアメール 19.11.5

セキュアメール for iOS

Secure Mailでの連絡先画像。 Secure Mail for iOSでは、メールや会議の招待状に受信者を追加する際に、連絡先の画像を表示できます。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[連絡先の画像を表示する](#)」を参照してください。

セキュアメール for Android

PDFファイルのアプリ内表示。 Secure Mail for Androidでは、ブックマークや注釈とともに、アプリ内でPDFファイルを表示できます。また、他のMicrosoft Office添付ファイルの拡張表示も利用できます。

セキュアメール for iOS 19.10.6

このリリースにはバグ修正が含まれています。

セキュアメール 19.10.5

セキュアメール for iOS

下書きの最小化。 Secure Mail for iOSでは、メール作成中に下書きを最小化し、アプリ内を移動できます。この機能は、iOS 13以降を実行しているデバイスで利用できます。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[下書きメールを最小化する](#)」を参照してください。

セキュアメール for Android

このリリースにはバグ修正が含まれています。

セキュアメール 19.10.0

Office 365 Exchange Serverポリシーを使用してOffice 365サーバーアドレスを定義します。

Secure Mail iOSおよびAndroidでは、**OAuth Support for Office 365**セクションに**Office 365 Exchange Server**という新しいポリシーが追加されました。このポリシーを使用すると、クラウド上にあるOffice 365メールボックスのホスト名を定義できます。このポリシーは、政府機関向けのOffice 365のサポートも有効にします。ホスト名は、*outlook.office365.com*のような単一の値です。デフォルト値は*outlook.office365.com*です。

Secure Mail iOSおよびAndroidは暗号化管理をサポートします。 暗号化管理により、最新のデバイスプラットフォームセキュリティを使用しながら、デバイスがプラットフォームセキュリティを効果的に使用できる十分な状態を維持できます。暗号化管理を使用することで、ファイルシステム暗号化はiOSまたはAndroidプラットフォームによって提供されるため、ローカルデータ暗号化の冗長性を排除できます。この機能を有効にするには、管理者はCitrix Endpoint Managementコンソールで**Encryption type** MDXポリシーを**Platform encryption with compliance enforcement**に構成する必要があります。

暗号化管理機能を使用するには、Citrix Endpoint Managementコンソールで、**Encryption type**ポリシーを**Platform encryption with compliance enforcement**に設定します。これにより、暗号化管理が有効になり、ユーザーのデバイス上の既存の暗号化されたアプリデータはすべて、デバイスによって暗号化され、MDXによって暗号化されない状態にシームレスに移行します。この移行中、アプリは1回限りのデータ移行のために一時停止されます。移行が成功すると、ローカルに保存されたデータの暗号化の責任はMDXからデバイスプラットフォームに移管されます。MDXは、

アプリを起動するたびにデバイスのコンプライアンスチェックを続行します。この機能は、MDM + MAM環境とMAM-only環境の両方で機能します。

Encryption typeポリシーを**Platform encryption with compliance enforcement**に設定すると、新しいポリシーが既存のMDX Encryptionに優先します。

Secure Mailの暗号化管理MDXポリシーの詳細については、次の**Encryption**セクションを参照してください。

- Android向けモバイル生産性アプリのMDXポリシー(/ja-jp/mobile-productivity-apps/administrator-tasks/policies-android.html#encryption)
- iOS向けモバイル生産性アプリのMDXポリシー(/ja-jp/mobile-productivity-apps/administrator-tasks/policies-ios.html)

デバイスが最小コンプライアンス要件を下回った場合、**Non-compliant device behavior**ポリシーにより、実行されるアクションを選択できます。

- **Allow app** – アプリを通常どおり実行することを許可します。
- **Allow app after warning** – アプリが最小コンプライアンス要件を満たしていないことをユーザーに警告し、アプリの実行を許可します。これがデフォルト値です。
- **Block app** – アプリの実行をブロックします。

iOSを実行しているデバイス

次の基準により、デバイスがiOSを実行しているデバイスの最小コンプライアンス要件を満たしているかどうか判断されます。

- iOS 10 - アプリが指定されたバージョン以上のオペレーティングシステムバージョンで実行されていること。
- デバッガーアクセス - アプリでデバッグが有効になっていないこと。
- ジェイルブレイクされたデバイス - アプリがジェイルブレイクされたデバイスで実行されていないこと。
- デバイスのパスコード - デバイスのパスコードが**ON**であること。
- データ共有 - アプリではデータ共有が有効になっていません。

Androidを実行しているデバイス

以下の基準により、デバイスがAndroidを実行しているデバイスの最小コンプライアンス要件を満たしているかどうか判断されます。

- Android SDK 24 (Android 7 Nougat) - アプリが指定されたバージョン以上のオペレーティングシステムバージョンで実行されていること。
- デバッガーアクセス - アプリでデバッグが有効になっていないこと。
- ルート化されたデバイス - アプリがルート化されたデバイスで実行されていないこと。
- デバイスロック - デバイスのパスコードが**ON**であること。
- デバイスの暗号化 - アプリが暗号化されたデバイスで実行されていること。

セキュアメール 19.9.5

iOS版セキュアメール

ICSファイルのサポート。iOS版Secure Mailでは、添付ファイルとして受信したICSファイルをカレンダーにイベントとしてインポートできます。

Android版セキュアメール

このリリースにはバグ修正が含まれています。

セキュアメール 19.9.0

このリリース以降、Secure Mailは以下のサーバーをサポートします。

- Exchange Server 2016 累積更新プログラム 13
- IBM Lotus Notes Traveler バージョン 10.0.1.0 ビルド 201811191126_20
- IBM Domino Mail Server バージョン 10.0.1

iOS向けセキュアメール

- iOS版Secure MailはiOS 13をサポートしています。
- **MIMEヘッダー付きのフィッシングメールの報告**。iOS版Secure Mailでは、ユーザーがフィッシングメールを報告すると、そのメールに対応するEMLファイルが添付ファイルとして生成されます。管理者はこのメールを受信し、報告されたメールに関連付けられたMIMEヘッダーを表示できます。この機能を有効にするには、管理者がフィッシングメールアドレスの報告ポリシーを構成し、Citrix Endpoint Managementコンソールでフィッシング報告メカニズムを「添付ファイルとして報告」に設定する必要があります。詳しくは、「[フィッシングメールを添付ファイルとして報告](#)」を参照してください。
- **レスポンスメールのサポート**。iOS版Secure Mailは、レスポンスメールを配信するように最適化されました。以前は、大きなテーブルや画像を含むメールコンテンツが正しくレンダ

リングされませんでした。この機能により、メールの形式やサイズに関わらず、サポートされているすべてのデバイスでメールコンテンツがより読みやすく表示されます。

- **カレンダーイベントのドラッグアンドドロップ。** iOS版Secure Mailでは、既存のカレンダーイベントをドラッグアンドドロップして時刻を変更できます。イベントをドラッグして、同じ日の希望する時間枠にドロップするか、複数日にわたってドロップして更新します。
- **自動送り。** iOS版Secure Mailでは、**会話**でメッセージを削除するときに、どのメッセージに戻るかを選択できます。この機能を使用するには、** [設定] > [自動送り] **に移動します。次に、利用可能な選択肢から設定を選択します。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[会話でメールを削除して自動的に次に進む](#)」を参照してください。
- **WkWebViewのサポート。** iOS版Secure MailはWkWebViewをサポートしています。この機能により、Secure Mailのメールとカレンダーイベントがデバイスでレンダリングされる方法が改善されます。

Android向けセキュアメール

このリリース以降、Android版Secure MailはAndroid 6以降を実行しているデバイスでのみサポートされます。

Android向けセキュアメール 19.8.5

このリリースにはバグ修正が含まれています。

セキュアメール 19.8.0

iOS用セキュアメール

このリリースには、パフォーマンスの強化とバグ修正が含まれています。

Android用セキュアメール

- Android Qのサポート。
- **Google Play向け64ビットアプリのサポート。** Android版Secure Mailは64ビットアーキテクチャをサポートしています。
- **Android版Secure MailのプルツリーフレッシュUIの改善。** Material Designガイドラインに沿って、プルツリーフレッシュ機能に軽微な改善を加えました。ハンバーガーアイコンをタップすると、同期タイムスタンプが画面の下部に表示されます。

セキュアメール 19.7.5

iOS用セキュアメール

- **下書きフォルダーの自動同期。** iOS版Secure Mailでは、下書きフォルダーが自動的に同期され、すべてのデバイスで下書きを利用できます。この機能は、Exchange ActiveSync v16以降を実行しているセットアップで利用できます。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[下書きフォルダーの自動同期](#)」を参照してください。
- **MDM + MAMモードでMicrosoft Intuneを使用している場合、iOS版Secure Mailはシングルサインオンをサポートします。** この機能を使用するには、Microsoft Authenticatorアプリがデバイスにインストールされていることを確認してください。Microsoft Authenticatorアプリのインストールに関する詳細については、[Docs.microsoft.com](https://docs.microsoft.com)の「**Microsoft Authenticatorアプリのダウンロードとインストール**」を参照してください。

Android用セキュアメール

注:

Citrixでは、OSをAndroid Qにアップグレードする前に、Secure Mailバージョン19.7.5にアップグレードすることをお勧めします。

- **Microsoft Office 365で最新の認証を実行しているセットアップ向けのWeb SSO for tunnelingポリシーの使用。** Android版Secure Mailに、**Web SSO for tunneling**という新しいポリシーが追加されました。このポリシーを使用すると、OAuthトラフィックをトンネル化してTunneled – Web SSO経由で送信できます。これを行うには：
 - **Web SSO for tunneling**ポリシーをオンに設定します。
 - 「ネットワークアクセス」ポリシーで「トンネル化 - Web SSO」オプションを選択します。
 - 「バックグラウンドサービス」ポリシーから、OAuthに関連するホスト名を除外します。
- **Android版Secure Mailは、MDM + MAMモードでMicrosoft Intuneを使用している場合のシングルサインオンをサポートします。** この機能を使用するには、Intune Company Portalアプリがデバイスにインストールされていることを確認してください。Intune Company Portalアプリにログインすると、Secure Mailで資格情報を使用して再認証することなく、MDM + MAMモードでSSOを使用できます。

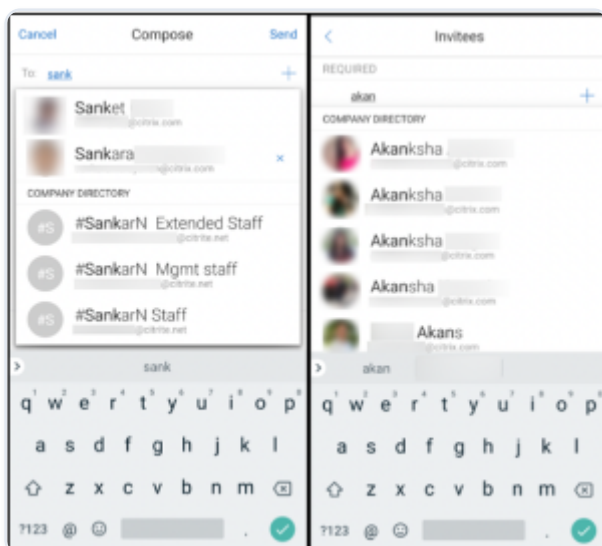
セキュアメール 19.6.5

iOS版セキュアメール

iOS版Secure Mailバージョン19.6.5には、パフォーマンスの強化とバグ修正が含まれています。修正済みおよび既知の問題のリストについては、「[既知の問題と修正済みの問題](#)」を参照してください。

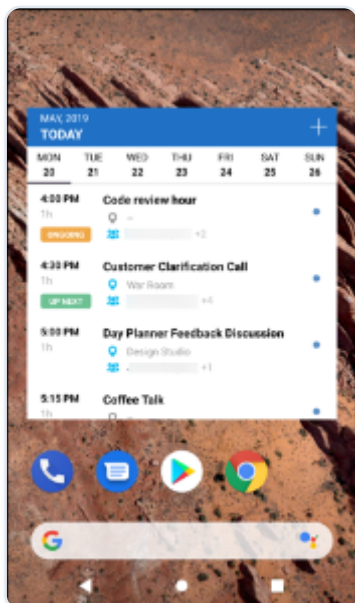
Android版セキュアメール

- **カレンダーイベントのドラッグアンドドロップ。** Android版Secure Mailでは、既存のカレンダーイベントをドラッグアンドドロップして時間を変更できます。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[カレンダーイベントの時間を変更する](#)」を参照してください。
- **レスポンスメールのサポート。** Android版Secure Mailは、レスポンスメールを配信するように最適化されています。以前は、大きなテーブルや画像を含むメールコンテンツが正しくレンダリングされませんでした。この機能により、メールの形式やサイズに関係なく、サポートされているすべてのデバイスでメールコンテンツがより読みやすくなります。
- **Secure Mailの連絡先画像。** Android版Secure Mailでは、メールや会議の招待状に受信者を追加する際に、連絡先の画像を表示できます。連絡先の画像は名前の横に表示されます。同じ名前の人が複数いる場合、メールや会議の招待状に受信者を追加する際に、画像は正しい受信者を特定するのに役立ちます。ローカルに保存されていない連絡先を検索するには、受信者の名前を4文字以上入力すると画像が表示されます。



- **カレンダーアジェンダのウィジェット。** Android版Secure Mailでは、「カレンダー」アジェンダがウィジェットとして利用できます。このウィジェットから、1週間分の「カレンダー」の今後のイベントを表示できます。この機能を使用すると、「カレンダー」イベントを作成したり、既存のイベントを表示したり、詳細を編集したりできます。「[画面キャプチャをブロック](#)

」ポリシーは、ホーム画面に配置されたウィジェットには適用されません。ただし、「**カレンダーアジェンダウィジェットを許可**」ポリシーを使用してウィジェットを無効にすることができます。



セキュアメール 19.5.5

Android版セキュアメール

Secure Mail for Android バージョン 19.5.5 には、パフォーマンスの強化とバグ修正が含まれています。修正済みおよび既知の問題のリストについては、「[既知の問題と修正済みの問題](#)」を参照してください。

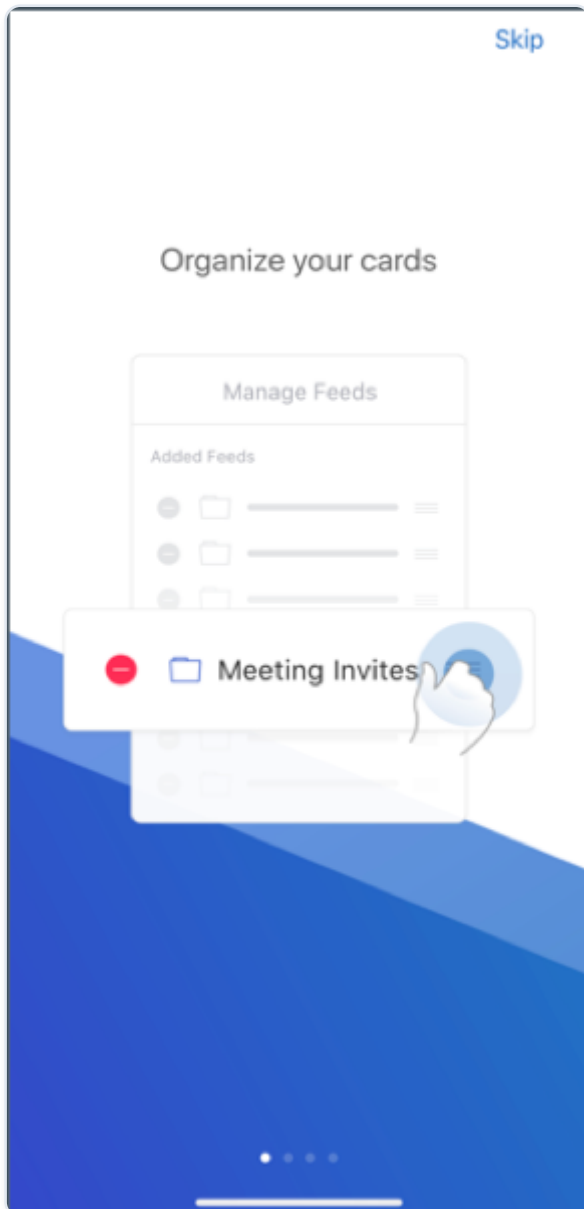
iOS向けセキュアメール

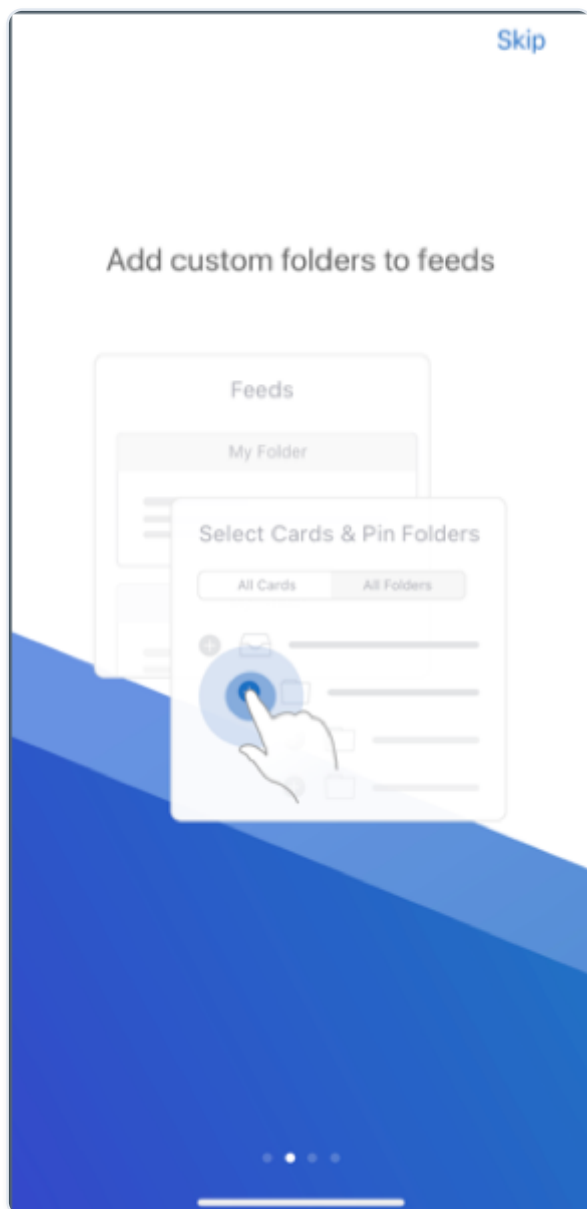
- Secure Mail for iOS は、MDM + MAM モードで Microsoft Intune を使用している場合にシングルサインオンをサポートします。この機能を使用するには、Microsoft Authenticator アプリがデバイスにインストールされていることを確認してください。Microsoft Authenticator アプリはアプリストアで入手できます。
- **Slack EMM のサポート:** Slack EMM は、Enterprise Mobility Management (EMM) が有効になっている Slack のお客様向けです。Secure Mail for iOS は、アプリケーション **Slack EMM** をサポートしており、管理者は Secure Mail を **Slack** アプリまたは **Slack EMM** アプリのいずれかと統合するかを選択できます。

セキュアメール 19.5.0

Android向けセキュアメール

フィードを管理する。Secure Mail for Android では、要件に基づいて フィード カードを整理できます。





フィードの管理の詳細については、「[フィードを管理する](#)」を参照してください。

下書きフォルダーの自動同期。 Secure Mail for Android では、下書きフォルダーが自動的に同期され、下書きはすべてのデバイスで利用できます。この機能に関するユーザーヘルプドキュメントについては、Citrix ユーザーヘルプセンターの記事「[下書きフォルダーの自動同期](#)」を参照してください。

Android版Secure Mail 19.4.6、19.4.5、および 19.3.5

これらのリリースには、パフォーマンスの強化とバグ修正が含まれています。

修正済みおよび既知の問題のリストについては、「[既知の問題と修正済みの問題](#)」を参照してください。

セキュアメール 19.3.0

このリリース以降、Secure Mail は以下のサーバーをサポートします。

- Exchange Server 2019 累積更新プログラム 1
- Exchange Server 2016 累積更新プログラム 12
- Exchange Server 2013 累積更新プログラム 22
- Exchange Server 2010 SP3 更新プログラムのロールアップ 26

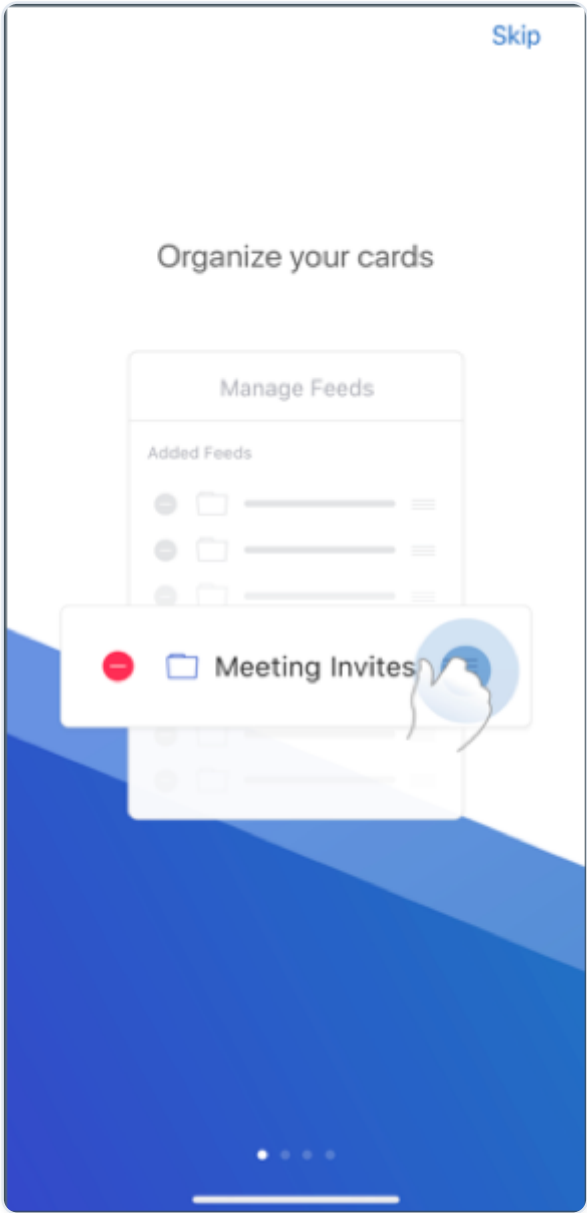
Secure Mail サーバーの互換性に関する完全なリストについては、「[Secure Mail の概要](#)」を参照してください。

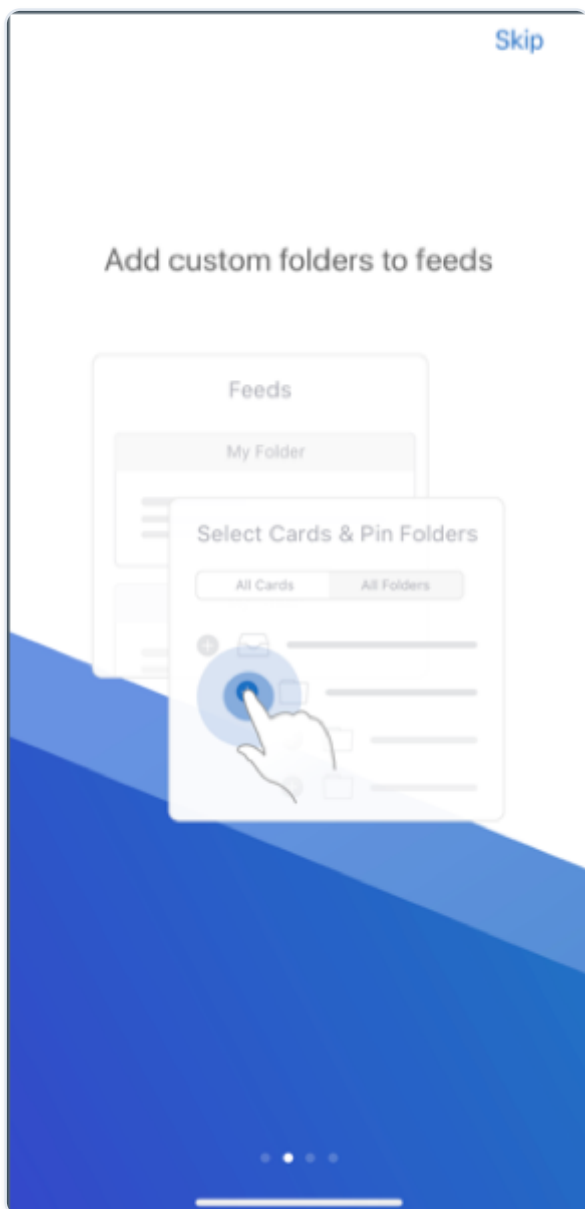
iOSデバイス用Secure Mail

フィードを管理する。Secure Mail for iOS では、要件に基づいてフィードカードを整理できるようになりました。

注：

この機能は iPad では利用できません。





フィードの管理について詳しくは、「[フィードを管理する](#)」を参照してください。

iOSおよびAndroid版Secure Mail

内部ドメイン。 外部組織に属するメール受信者を識別して編集できます。この機能を使用するには、Citrix Endpoint Management で**内部ドメイン**ポリシーが有効になっていることを確認してください。

メールを作成、返信、または転送すると、メーリングリスト内の外部受信者が強調表示されます。画面の左下隅に警告として**連絡先**アイコンが表示されます。メーリングリストを変更するには、**連絡先**アイコンをタップします。

外部受信者(/en-us/mobile-productivity-apps/media/extrecipients-ios.png)

内部ドメインの詳細については、「**内部ドメイン**」を参照してください。

人間工学に基づいた改善。操作ボタンが画面の上部から下部に移動され、アクセスしやすくなりました。これらの変更は、受信トレイ、カレンダー、および連絡先画面に適用されます。

注:

Androidを実行しているデバイスの場合、変更は受信トレイおよびカレンダー画面に適用されます。

人間工学に基づいた改善(/en-us/mobile-productivity-apps/media/ergonomic-improvements-ios.png)

人間工学に基づいた改善の詳細については、「人間工学に基づいた改善」を参照してください。

セキュアメール 19.2.0

iOS用セキュアメール

このリリースには、パフォーマンスの強化とバグ修正が含まれています。

修正済みおよび既知の問題のリストについては、「既知の問題と修正済みの問題」を参照してください。

Android用セキュアメール

- **連絡先の機能強化。** Android版Secure Mailで、連絡先をタップして連絡先を選択すると、その連絡先の詳細が連絡先タブの下に表示されます。組織タブをタップすると、マネージャー、直属の部下、同僚などの組織階層の詳細が表示されます。画面右上のその他アイコンをタップすると、次のオプションが表示されます。

- メールに添付
- 共有
- 削除

「組織」タブで、MANAGER、DIRECT REPORTS、またはPEERSの右にあるその他アイコンをタップします。その後、メールまたはカレンダーの招待を作成します。メールまたはカレンダーイベントの宛先:フィールドには、MANAGER、DIRECT REPORTS、またはPEERSの詳細が自動的に入力されます。

前提条件:

Exchange Web Services (EWS) がExchange Serverで有効になっていることを確認してください。

連絡先の詳細は、Active Directoryから取得された組織の詳細に基づいて表示されます。連絡先に正しい詳細が表示されるように、管理者がActive Directoryで組織階層を構成していることを確認してください。

注:

この機能は、IBM Lotus Notesサーバーではサポートされていません。

- **ネットワークアクセスポリシー**。Android版Secure Mailでは、**トンネル化 - Web SSO**という新しいオプションがネットワークアクセスMDXポリシーに追加されました。このポリシーを構成すると、内部トラフィックをトンネル化 - Web SSOとSecure Ticket Authority (STA) を介して並行してトンネル化する柔軟性が得られます。また、NTLM、Okta、Kerberosなどの認証サービスに対して、トンネル化 - Web SSO接続を許可することもできます。STAを最初に構成するときは、個々のFQDNとサービスアドレスのポートをバックグラウンドネットワークサービスポリシーに追加する必要があります。ただし、**トンネル化 - Web SSO**オプションを構成する場合は、これらの構成を行う必要はありません。

Citrix Endpoint ManagementコンソールでSecure Mail for Androidのこのポリシーを有効にするには:

1. Android用の.mdxファイルをダウンロードして使用します。詳細については、「[MDXアプリの追加](#)」の手順を参照してください。
2. ネットワークアクセスポリシーで、**トンネル化 - Web SSO**オプションをクリックします。詳しくは、「[アプリのネットワークアクセス](#)」を参照してください。

iOSデバイス用Secure Mail 19.1.6

このリリースには、パフォーマンスの強化とバグ修正が含まれています。

セキュアメール 19.1.5

このリリース以降、Secure Mailは以下のサーバーをサポートします:

- Exchange Server 2016 累積更新プログラム 11
- Exchange Server 2010 SP3 更新プログラムのロールアップ 24

Secure Mailとサーバーの互換性の完全なリストの詳細については、[Secure Mailの概要](#)を参照してください。

セキュアメール 19.1.0

iOS向けセキュアメール

- **連絡先の機能強化。** Secure Mail for iOSで、**連絡先**をタップして連絡先を選択すると、その連絡先の詳細が**連絡先**タブに表示されます。**組織**タブをタップすると、**マネージャー**、**直属の部下**、**同僚**などの組織階層の詳細が表示されます。画面右上のその他アイコンをタップすると、以下のオプションが表示されます:

- 編集
- VIPに追加
- キャンセル

組織タブで、**マネージャー**、**直属の部下**、または**同僚**の右にあるその他アイコンをタップできます。この操作により、メールまたはカレンダーイベントを作成できます。メールまたはカレンダーイベントの宛先:フィールドには、**マネージャー**、**直属の部下**、または**同僚**の詳細が自動的に入力されます。メールを作成して送信できます。

前提条件:

Exchange ServerでExchange Web Services (EWS) が有効になっていることを確認してください。

連絡先の詳細は、Active Directoryから取得された組織の詳細 (Outlook連絡先) に基づいて表示されます。連絡先に正しい詳細が表示されるように、管理者がActive Directoryで組織階層を構成していることを確認してください。

注:

この機能はIBM Lotus Notesサーバーではサポートされていません。

- **会議の時間と場所をネイティブカレンダーにエクスポートする。** iOS版Secure Mailでは、**Export Calendar** MDXポリシーに新しい値**Meeting Time, Location**が追加されました。この機能強化により、Secure Mailカレンダーイベントの会議の時間と場所をネイティブカレンダーにエクスポートできます。
- iOS版Secure Mailは、最新の認証 (O365) を使用するMicrosoft Enterprise Mobility + Security (EMS)/Intuneを実行しているセットアップで、リッチプッシュ通知をサポートします。

リッチプッシュ通知機能を有効にするには、以下の前提条件が満たされていることを確認してください。

- Endpoint Managementコンソールで、**Push notifications**をONに設定します。
 - **Network access policy**が**Unrestricted**に設定されています。
 - **Control locked screen notifications**ポリシーが**Allow**または**Email sender or event title**に設定されています。
 - **Secure Mail > Settings > Notifications**に移動し、**Mail Notifications**を有効にします。
- Secure MailユーザーはZoomアプリを使用して会議に参加できます。Zoomアプリを使用するために必要なポリシーの構成については、「カレンダーから会議に参加する」を参照してください。
 - このリリースには、iPad Pro 11インチおよびiPad Pro 12.9インチのサポートが含まれています。

Android版Secure Mail

- **添付ファイルの機能強化。** Android版Secure Mailでは、添付ファイルの表示が簡素化されました。より良いエクスペリエンスのために、不要な手順が削除され、以前のリリースに存在した添付ファイルオプションは保持されています。

Secure Mailアプリ内で添付ファイルを表示できます。Secure Mailを使用して表示できる場合、添付ファイルは直接開きます。Secure Mailを使用して添付ファイルを表示できない場合は、アプリのリストが表示されます。必要なアプリを選択して添付ファイルを表示できます。詳細については、「[添付ファイルの表示](#)」を参照してください。

- Secure MailユーザーはZoomアプリを使用して会議に参加できます。Zoomアプリを使用するために必要なポリシーの構成については、「カレンダーから会議に参加する」を参照してください。
- **会議の時間と場所をネイティブカレンダーにエクスポートする。** Android版Secure Mailでは、**Export Calendar MDX**ポリシーに値**Meeting Time, Location**が追加されました。これにより、Secure Mailカレンダーイベントの会議の時間と場所をネイティブカレンダーにエクスポートできます。

注：

Android 5.x のサポートは December 31, 2018 に終了しました。

セキュアメール 18.12.0

このリリースには、パフォーマンスの強化とバグ修正が含まれています。

修正済みおよび既知の問題のリストについては、[既知の修正済み問題](#)を参照してください。

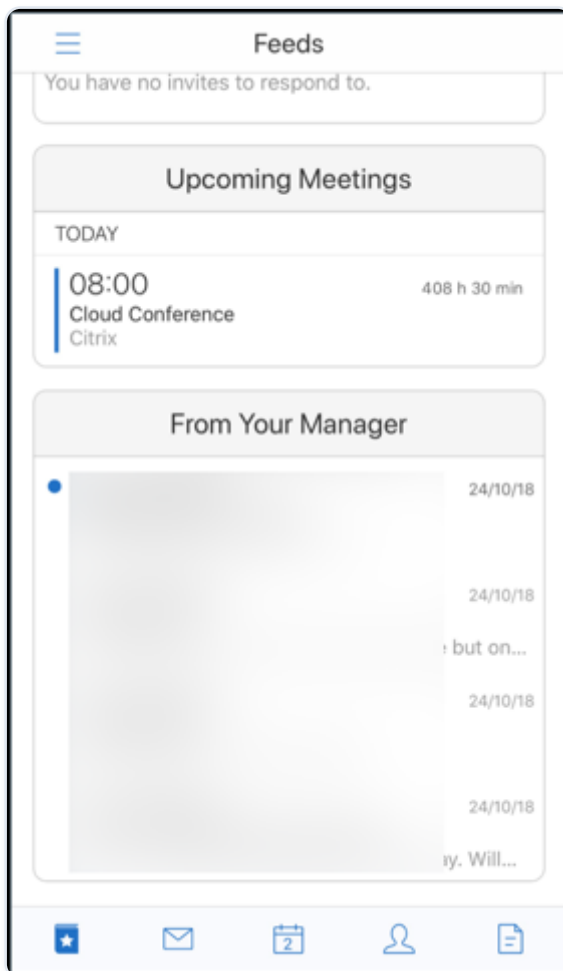
セキュアメール 18.11.5

アンドロイド向けセキュアメール

- **ActiveSyncヘッダー付きのフィッシングメールを報告する。** Android版Secure Mailでは、ユーザーがフィッシングメールを報告すると、そのメールに対応するEMLファイルが添付ファイルとして生成されます。管理者はこのメールを受信し、報告されたメールに関連付けられたActiveSyncヘッダーを表示できます。

この機能を有効にするには、管理者は**Report Phishing Email Address**ポリシーを構成し、**Report Phishing Mechanism**を**Report Via Attachment**に設定する必要があります。管理者はこれらの設定をCitrix Endpoint Managementコンソールで構成します。Secure MailのMDXポリシーの構成の詳細については、[モバイル生産性向上アプリのMDXポリシー](#)を参照してください。

- **メールとカレンダーイベントを印刷する。** Android版Secure Mailでは、Androidデバイスからメールとカレンダーイベントを印刷できます。この印刷機能はAndroid Printフレームワークを使用します。詳細については、[メールとカレンダーイベントの印刷](#)を参照してください。
- **マネージャーからのフィード。** Android版Secure Mailでは、フィード画面でマネージャーからのメールを表示できます。**メール同期期間**の設定に基づいて、最大5件のメールが**マネージャーからのフィード**の下に表示されます。マネージャーからのメールをさらに表示するには、**すべて表示**をタップします。

**前提条件：**

Exchange ServerでExchange Web Services (EWS) が有効になっていることを確認してください。

マネージャーカードは、Active Directoryから取得された組織の詳細（Outlook連絡先）に基づいて表示されます。マネージャーフィードに正しい詳細が表示されるように、管理者がActive Directoryで組織階層を構成していることを確認してください。

注記:

この機能はIBM Lotus Notesサーバーではサポートされていません。

セキュアメール 18.11.1

重要:

以下の問題はSecure Mail for Android 18.11.1で修正されました。

IBM Notes Traveler 9.0.1 SP 10に接続されたSecure Mail for Androidでは、添付ファイル付きのメールが送信トレイに残ります。

セキュアメール 18.11.0

Android 版 セキュアメール

- **サブフォルダー通知。** Secure Mail for Androidでは、メールアカウントのサブフォルダーからメール通知を受け取ることができます。詳細については、[サブフォルダー通知](#)を参照してください。
- **Secure Mail for Androidのバックグラウンドサービスへの更新。** Android 8.0 (APIレベル26)以降を実行しているデバイスでのGoogle Playのバックグラウンド実行制限要件を満たすため、Secure Mailのバックグラウンドサービスをアップグレードしました。デバイスでの中断のないメール同期と通知のために、Firebase Cloud Messaging (FCM)サービスプッシュ通知を有効にしてください。FCMベースのプッシュ通知の有効化に関する詳細については、[Secure Mailのプッシュ通知](#)を参照してください。

デバイスのSecure Mail設定で**メール通知**をオンにしてください。

制限事項:

- FCMベースのプッシュ通知を有効にしていない場合、バックグラウンド同期は15分に1回実行されます。この間隔は、アプリがバックグラウンドで実行されているかフォアグラウンドで実行されているかによって異なります。
- ユーザーがデバイス設定から時刻を手動で更新しても、カレンダーウィジェットの日付は自動的に更新されません。

iOS 版 セキュアメール

- **iOS 12.1のサポート。** Secure Mail for iOSはiOSバージョン12.1をサポートしています。
- **リッチプッシュ通知の失敗メッセージの機能強化。** Secure Mail for iOSでは、通知失敗の種類に応じて、適切なプッシュ通知失敗メッセージがデバイスの通知センターに表示されます。詳細については、「[Secure Mail for iOSでのプッシュ通知失敗メッセージ](#)」を参照してください。
- **マネージャーからのフィード。** Secure Mail for iOSでは、フィード画面でマネージャーからのメールを表示できます。メール同期期間の設定に基づいて、マネージャーからのフィードの下に最大5件のメールが表示されます。マネージャーからのメールをさらに表示するには、**すべて表示**をタップします。

Secure Mailマネージャーフィード(/en-us/mobile-productivity-apps/media/manager-feeds.png)

前提条件:

Exchange ServerでExchange Web Services (EWS) が有効になっていることを確認してください。

マネージャーカードは、Active Directoryから取得された組織の詳細 (Outlook連絡先) に基づいて表示されます。マネージャーフィードに正しい詳細が表示されるように、管理者がActive Directoryで組織階層を構成していることを確認してください。

注:

この機能はIBM Lotus Notesサーバーではサポートされていません。

セキュアメール 18.10.5

- **SlackとのSecure Mail統合 (プレビュー):** iOSまたはAndroidを実行しているデバイスで、メールの会話をSlackアプリに引き継ぐことができるようになりました。詳細については、「[SlackとのSecure Mail統合 \(プレビュー\)](#)」を参照してください。
- **フィードフォルダーの機能強化:** Secure Mail for iOSでは、既存のフィードフォルダーに次の機能強化が加えられています。
 - フィードカードで最大5件の今後の会議を表示します。
 - 今後24時間以内の会議はフィードカードに表示され、**今日**と**明日**のセクションに分類されます。

セキュアメール 18.10.0

- **メールおよびカレンダー通知用のSecure Mail通知チャネル:** Android O以降を実行しているデバイスでは、通知チャネル設定を使用して、メールおよびカレンダー通知の処理方法を管理できます。この機能を使用すると、通知をカスタマイズおよび管理できます。詳細については、「[通知チャネル](#)」を参照してください。
- **フィッシングメールの報告 (転送として):** iOS版Secure Mailでは、フィッシングの疑いがあるメールを (転送として) 報告するために、フィッシングとして報告機能を使用できます。疑わしいメッセージは、管理者がポリシーで構成したメールアドレスに転送できます。この機能を有効にするには、管理者が「フィッシングメールアドレスの報告」ポリシーを構成し、**「フィッシングメカニズムの報告」を「転送による報告」**に設定する必要があります。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[フィッシングメールの報告](#)」を参照してください。

セキュアメール 18.9.0

- 「yy.mm.version」形式の新しいバージョン番号付けスキーム。例：バージョン**18.9.0**
- **フィッシングメールの報告（転送として）**：Android版Secure Mailでは、フィッシングの疑いがあるメールを（転送として）報告するために、フィッシングとして報告機能を使用できます。疑わしいメッセージは、管理者が構成したメールアドレスに転送できます。この機能を有効にするには、管理者が「フィッシングメールアドレスの報告」ポリシーを構成し、「フィッシングメカニズムの報告」を**「転送による報告」**に設定する必要があります。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[フィッシングメールの報告](#)」を参照してください。
- **フィードカードの機能強化**：Android版Secure Mailの既存の**「フィード」**フォルダーに、以下の機能強化が加えられました。
 - 自動同期されたすべてのフォルダーからの会議出席依頼がフィードカードに表示されます。
 - フィードカードで最大5件の今後の会議を表示します。
 - 今後の会議は、現在の時刻から24時間に基づいて表示されるようになりました。これらの会議出席依頼は、**「今日」と「明日」**に分類されます。以前のリリースでは、その日の終わりまでの今後の会議がフィードに表示されていました。
- **Secure Mailカレンダーイベントのエクスポート**：AndroidおよびiOS版Secure Mailでは、Secure Mailカレンダーイベントをデバイスのネイティブカレンダーアプリにエクスポートできます。この機能を有効にするには、**「設定」**をタップし、「カレンダーイベントのエクスポート」のスライダーを右にドラッグします。詳細については、「[Secure Mailカレンダーイベントのエクスポート](#)」を参照してください。

セキュアメール 10.8.65

- **iOS 12で利用可能**：iOS版Secure Mailでは、グループ通知機能をサポートしています。この機能により、会話はメールスレッドからグループ化されます。デバイスのロック画面でグループ化された通知をすばやく確認できます。グループ通知設定は、デバイスでデフォルトで有効になっています。
- iOS版Secure Mailでは、**「下書きを保存」ボタンと「下書きを削除」**ボタンが大きくなりました。この機能強化により、お客様はオプションを区別しやすくなります。
- iOS版Secure Mailでは、デバイスの**「設定」**でSecure Mail発信者IDを有効にすることで、連絡先からの着信を識別できます。これらの設定を有効にすると、着信があったときに、デバイスは「Secure Mail発信者ID：Joe Jay」のように、発信者IDとともにアプリ名を表示します。詳細については、「Secure Mail発信者ID」を参照してください。

セキュアメール 10.8.60

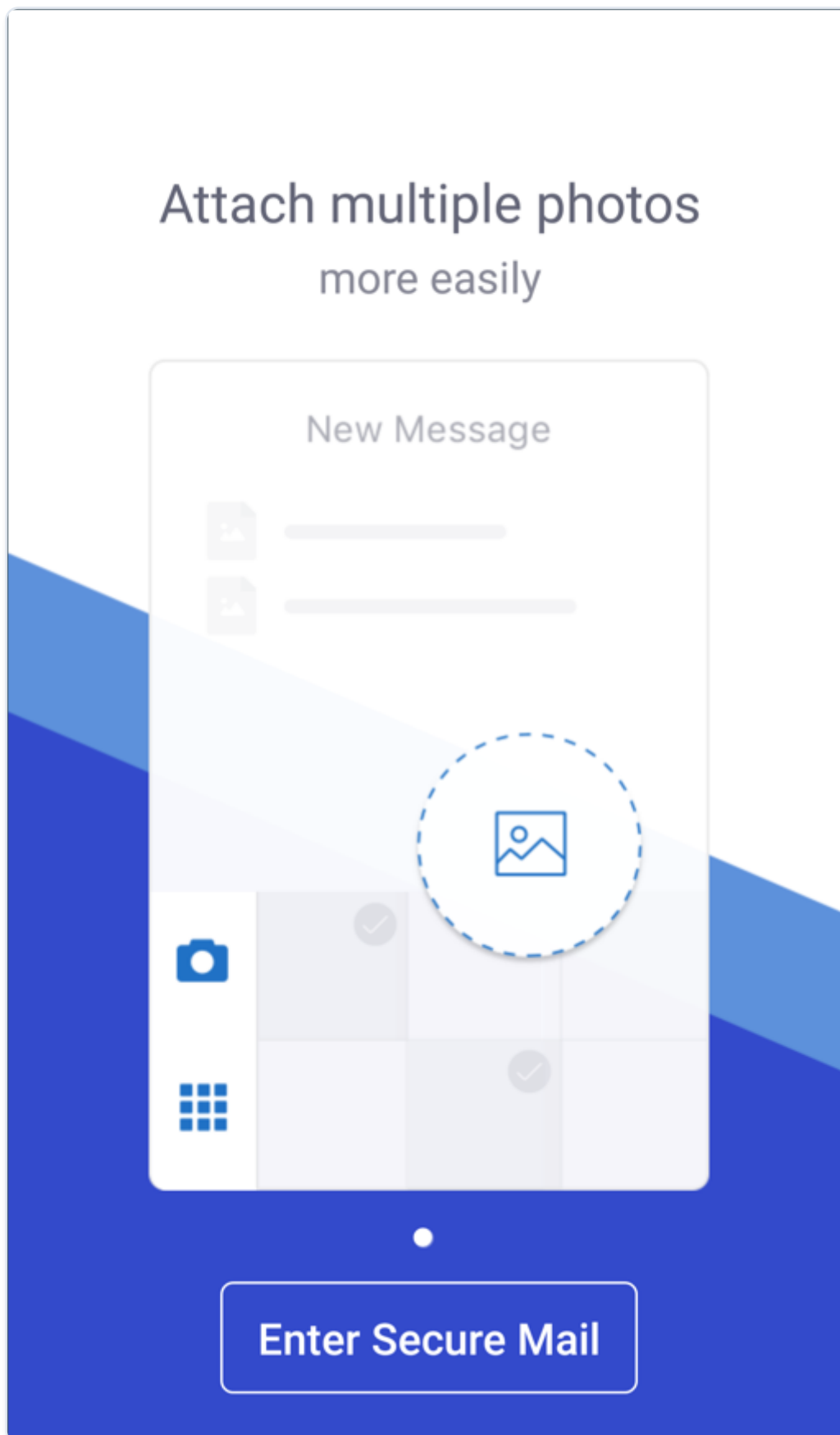
- Secure Mail は Android P をサポートしています。
- Secure Mail がポーランド語で利用可能になりました。
- iOS 版 Secure Mail では、iOS ネイティブのファイルアプリからメールにファイルを添付できます。詳細については、[iOS の機能](#)を参照してください。

セキュアメール 10.8.55

Secure Mail バージョン 10.8.55 に新機能はありません。修正された問題については、[既知の問題と修正された問題](#)を参照してください。

セキュアメール 10.8.50

写真添付機能の改善。 iOS 版 Secure Mail では、新しいギャラリーアイコンをタップすることで、写真を簡単に添付できます。ギャラリーアイコンをタップし、メールに添付したい写真を選択します。



Secure Mail フィード画面。 iOS および Android 版 Secure Mail では、未読メール、対応が必要な会議の招待、今後の会議がすべてフィード画面に表示されます。

セキュアメール 10.8.45

フォルダー同期。 iOS および Android 版 Secure Mail では、**同期**アイコンをタップしてすべての Secure Mail コンテンツを更新できます。**同期**アイコンは、メールボックス、カレンダー、連絡先、添付ファイルなどの Secure Mail のスライドアウトに表示されます。**同期**アイコンをタップすると、メールボックス、カレンダー、連絡先など、自動更新するように構成したフォルダーが更新されます。最終同期のタイムスタンプは**同期**アイコンの横に表示されます。

写真添付機能の改善。 Android 版 Secure Mail では、新しい**ギャラリー**アイコンをタップすることで、写真を簡単に添付できます。**ギャラリー**アイコンをタップし、メールに添付したい写真を選択します。

Attach multiple photos more easily

New Message







Enter Secure Mail

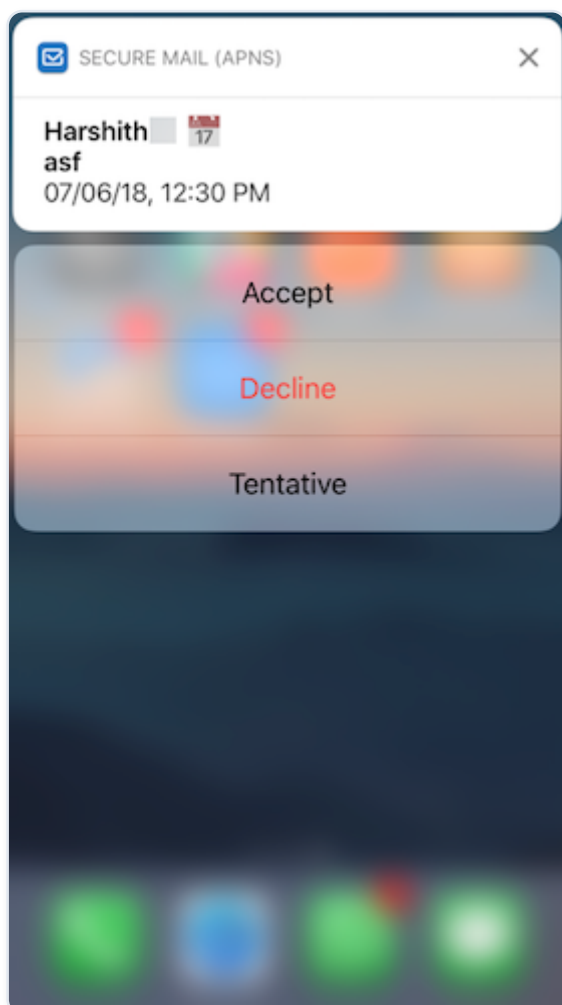
セキュアメール 10.8.40

カレンダー検索のサポート。iOS 版 Secure Mail では、カレンダーでイベント、出席者、またはその他のテキストを検索できます。

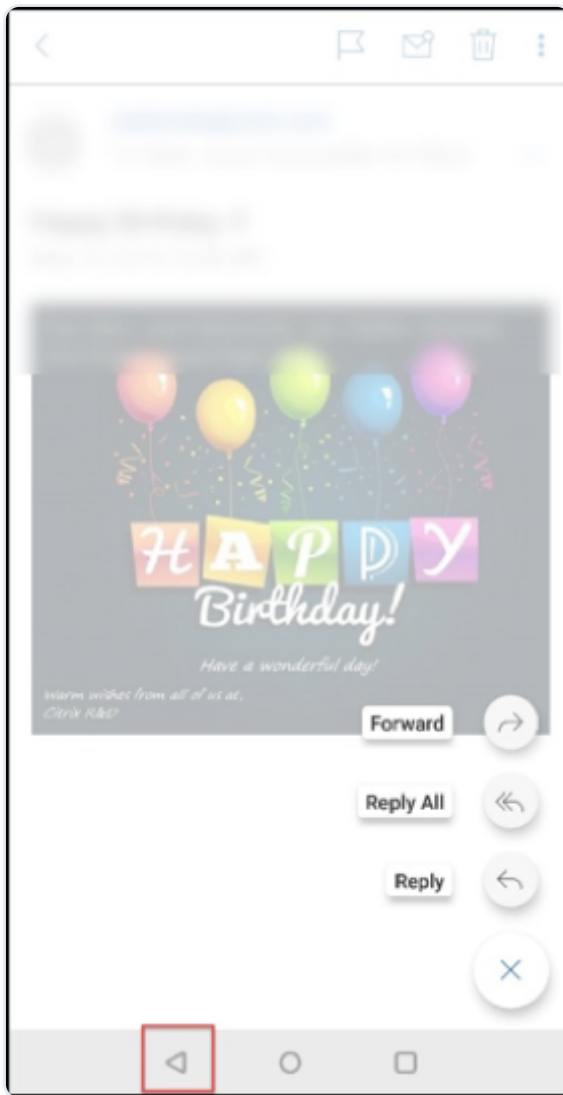
セキュアメール 10.8.35

Secure Mail for iOSのバージョンは10.8.36です。

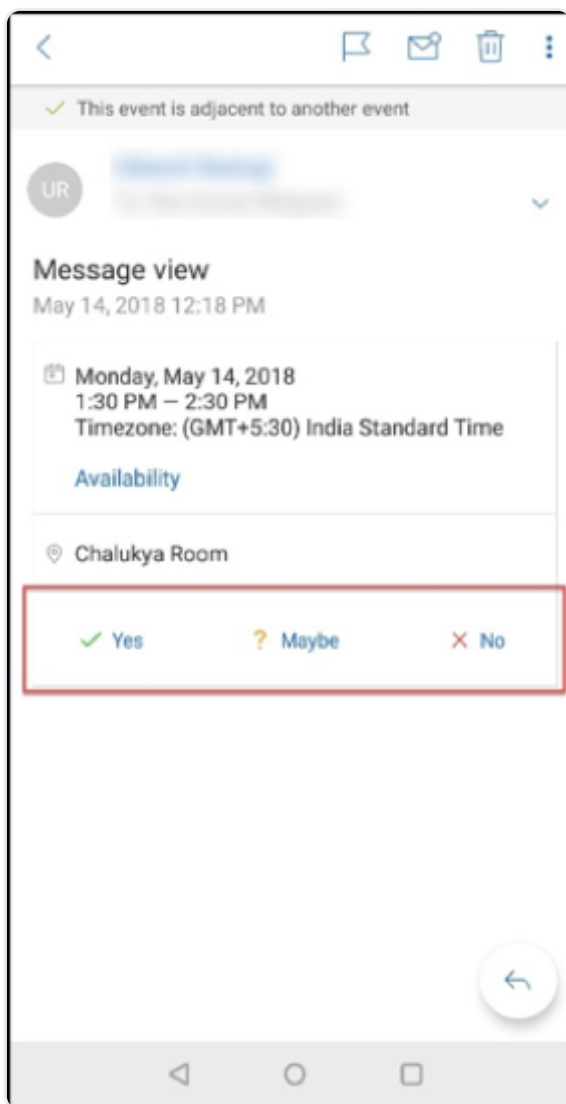
- **通知応答オプション。** Secure Mail for iOSでは、ユーザーは会議通知（承諾、辞退、仮承諾など）に応答できます。メッセージ通知には、返信と削除で応答できます。



- **Secure Mail for Androidの戻るボタンの機能強化。** Secure Mail for Androidでは、デバイスの戻るボタンをタップして、フローティングアクションボタンの展開されたオプションを閉じることができます。フローティングアクションボタンが展開状態の場合、デバイスの戻るボタンをタップすると、応答オプションが折りたたまれます。この操作により、メッセージまたはイベントの詳細表示に戻ります。



- **Secure Mail for Android**では、会議応答ボタンがメール内に表示されます。会議の招待に関するメール通知を受信すると、次のいずれかのオプションをタップして招待に応答できます。
 - はい
 - 未定
 - いいえ



セキュアメール 10.8.25

Secure Mail for iOSが派生資格情報用のS/MIMEをサポートするようになりました。この機能を使用するには、次の操作を行う必要があります。

- S/MIME証明書ソースとして「派生資格情報」を選択します。詳細については、「[iOS用派生資格情報](#)」を参照してください。
- Citrix Endpoint ManagementでLDAP属性クライアントプロパティを追加します。次の情報を使用してください。
 - キー: SEND_LDAP_ATTRIBUTES
 - 値: `userPrincipalName=${user.userprincipalname}, sAMAccountName=${user.samaccountname}, displayName=${user.displayName}, mail=${user.mail}`

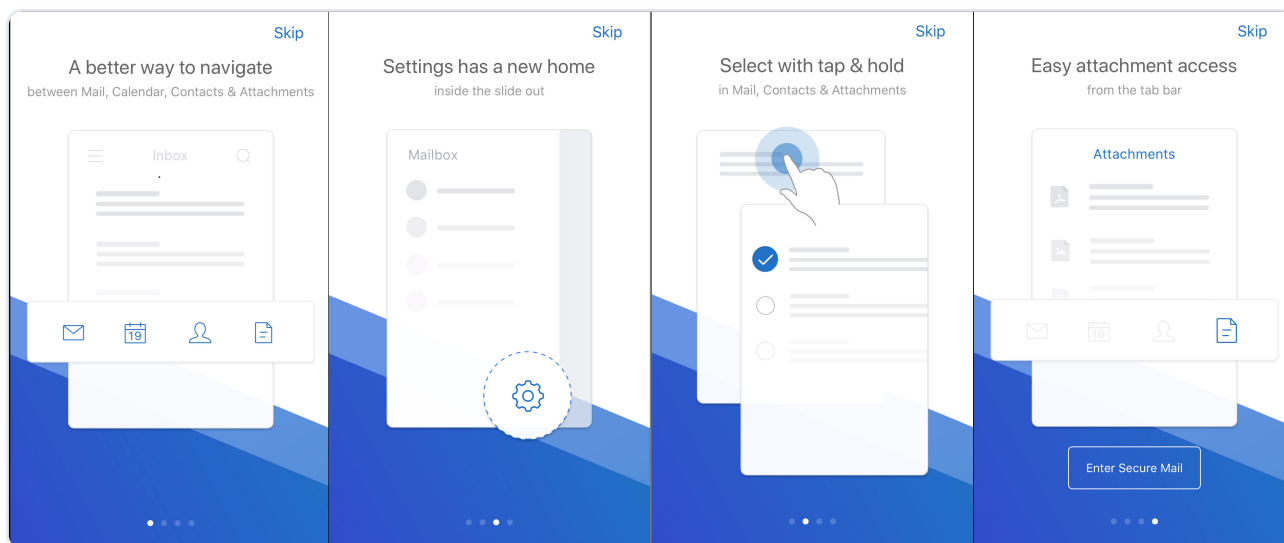
クライアントプロパティを追加する手順については、XenMobile Server の場合は、[クライアントプロパティ](#) を、Endpoint Management の場合は、[クライアントプロパティ](#) を参照してください。

派生資格情報を使用してデバイスを登録する方法の詳細については、[派生資格情報を使用してデバイスを登録する](#) を参照してください。

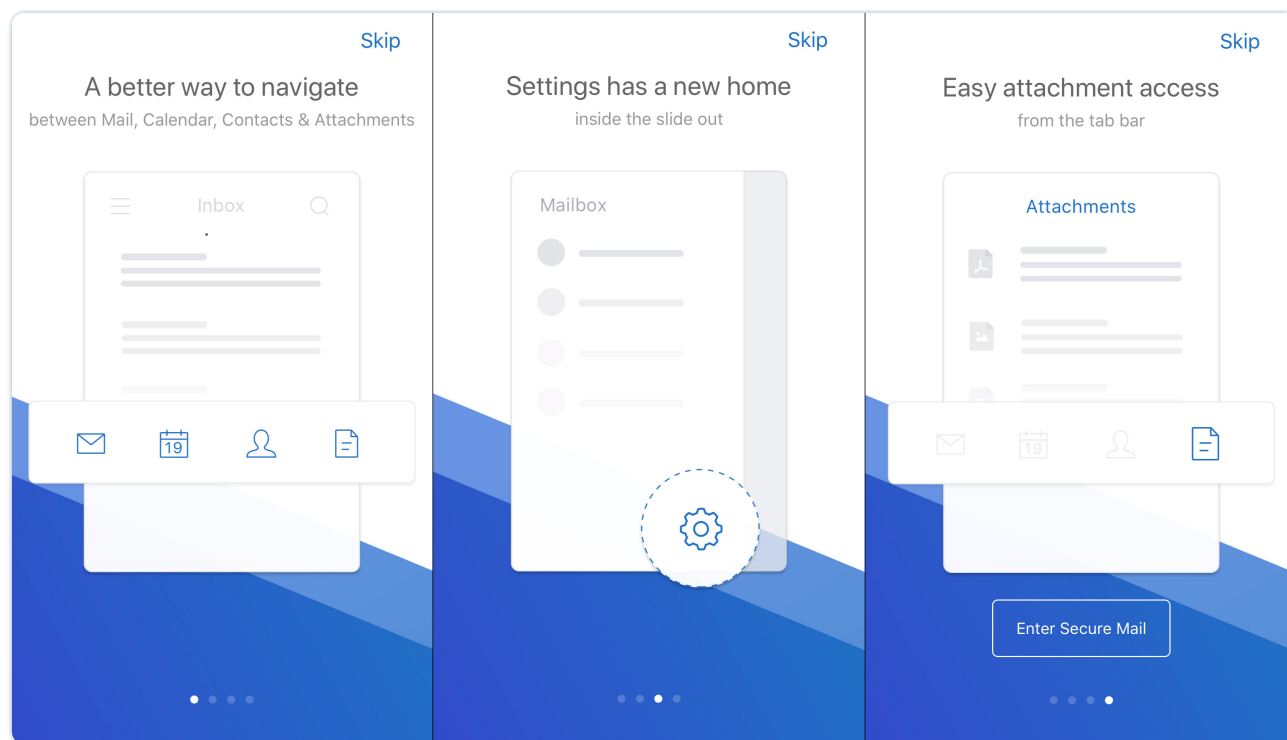
1. Endpoint Management コンソールで、> の順に移動します。
2. **Secure Mail** を選択し、 をクリックします。
3. iOS プラットフォームで、S/MIME 証明書ソースとして を選択します。

Secure Mail for iOS および Android の外観と操作性が一新されました: ユーザーナビゲーションをよりシンプルで効率的なものにしました。メニューとアクションボタンをナビゲーションバーの形式に再配置しました。

次の図は、iOS デバイスの新しいナビゲーションバーを示しています。



次の図は、Android デバイスの新しいナビゲーションバーを示しています。

**変更点:**

- グラバーアイコンは削除されました。メール、カレンダー、連絡先、添付ファイルなどの Secure Mailの機能は、フッタータブバーのボタンとして利用できるようになりました。次の図にこの変更を示します。

フッタータブバーの画像(/en-us/mobile-productivity-apps/media/mail-inbox.png)

注:

Androidデバイスでは、メールアイテムを開いた後、フッタータブバーは利用できません。たとえば、次の図に示すように、メールまたはカレンダーイベントを開くと、フッタータブバーは利用できません。

フッタータブバーのないAndroidデバイスの画像(/en-us/mobile-productivity-apps/media/android-footer-level1.png)

- **設定**メニューは、メール、カレンダー、連絡先、添付ファイルなど、すべてのメニュー内で利用できます。**設定**に移動するには、ハンバーガーアイコンをタップし、次に右下にある設定ボタンをタップします。次の図を参照してください。

Secure Mailの設定メニューの画像(/en-us/mobile-productivity-apps/media/settings-icon.png)

- **検索**アイコンが検索バーに代わり、受信トレイ、連絡先、添付ファイルの各ビューで利用できます。

検索アイコンの画像(/en-us/mobile-productivity-apps/media/find-searchicon-1.png)

- iOSデバイスでは、メールアイテムを長押ししてアイテムを選択できます。
- **作成フローティングアクションボタン**をタップして、新しいメールを作成できます。次の図を参照してください。

作成フローティングアクションボタンの画像(/en-us/mobile-productivity-apps/media/inbox-fab.png)

- 次のメニューオプションが画面の右上で利用可能になりました。
 - **同期オプション**: 右上のオーバーフローアイコンをタップし、**その他のオプション** > **同期オプション**に移動して、同期設定を変更します。

注:

このオプションはAndroidデバイスでのみ利用可能です。

- **検索アイコン**: タップしてメールを検索します。
- **トリアージビューアイコン**: タップすると、会話のトリアージビューが表示されます。
- **返信フローティングアクションボタン**: メールを表示中に、次の図に示すように、タップして転送、全員に返信、または返信します。

返信フローティングアクションボタンの画像(/en-us/mobile-productivity-apps/media/inbox-respond-fab-and-actions.png)

- メールを表示中に、画面の右上から次のメニューオプションを利用できます。
 - **フラグ**: タップしてメールにフラグを付けます。
 - **未読にする**: タップしてメールを未読にします。
 - **削除**: タップしてメールを削除します。
 - **その他のオプション**: オーバーフローアイコンをタップすると、移動などの他の利用可能なアクションが表示されます。

カレンダーの変更

- カレンダーから、次の図に示すように、イベントフローティングアクションボタンをタップしてイベントを作成できます。

カレンダーフローティングアクションボタンの画像(/en-us/mobile-productivity-apps/media/calendar-fab.png)

- 画面の右上から次のメニューオプションを利用できるようになりました。
 - **今日:** タップして今日のイベントを表示します。
 - **検索:** タップしてイベントを検索します。
 - **応答フローティングアクションボタン:** イベントを表示中に、転送、全員に返信、または返信をタップします。

カレンダー応答オプションの画像(/en-us/mobile-productivity-apps/media/calendar-response-options.png)

イベントを表示すると、はい、未定、いいえなどのイベント応答アクションが再配置され、イベント詳細の下に表示されます。

連絡先の変更

- 次の図に示すように、**新しい連絡先の作成**フローティングアクションボタンをタップできます。

新しい連絡先の作成画像の画像(/en-us/mobile-productivity-apps/media/contacts-fab.png)

- **検索**メニューオプションが画面の右上から利用できるようになりました。このオプションをタップして連絡先を検索できます。
- 連絡先を表示中に、画面の右上から次のメニューオプションが利用できます。

Androidデバイスの場合:

- **編集:** 連絡先を編集するにはタップします。
- **その他のオプション:** 編集アイコンをタップして、メールに添付、共有、削除などのその他の利用可能なアクションを表示します。

Androidのオーバーフローアイコンの画像(/en-us/mobile-productivity-apps/media/android-contacts-options.png)

iOSデバイスの場合:

- **編集:** 連絡先を編集するにはタップします。
- **共有:** 共有アイコンをタップして、連絡先の共有、メールに添付などのその他の利用可能なアクションを表示します。

iOSの共有アイコンの画像(/en-us/mobile-productivity-apps/media/ios-to-delete-contact.png)

注:

iOSデバイスで連絡先を削除するには、連絡先を選択し、**編集**をタップし、次の図に示すとおり、画面下部の**削除**をタップします。

iOSデバイスでの連絡先削除オプションの画像(/en-us/mobile-productivity-apps/media/ios-delete-contact-button.png)

添付ファイルの変更

添付ファイルに関する以下のメニューオプションが、画面の右上から利用できるようになりました。

- **並べ替え:** 並べ替えアイコンをタップし、適切なフィルターを選択して添付ファイルを並べ替えます。
- **検索:** タップして添付ファイルを検索します。

セキュアメール 10.8.20

- Secure Mail for iOSは、登録と認証に派生資格情報の使用をサポートするようになりました。派生資格情報の詳細については、「[iOS向け派生資格情報](#)」を参照してください。
- Secure Mail for iOSは、リッチプッシュ通知をサポートしています。リッチ通知により、Secure Mailがバックグラウンドで実行されていない場合でも、受信トレイのロック画面通知を受信できます。この機能は、パスワードベースの認証とクライアントベースの認証設定でサポートされています。詳細については、「[リッチプッシュ通知](#)」を参照してください。

注:

リッチプッシュ通知機能をサポートするためのアーキテクチャの変更により、**VIPのみ**のメール通知は利用できなくなりました。

- Secure Mail for iOSは、リッチテキスト署名をサポートするようになりました。メール署名に画像やリンクを使用できます。詳細については、「[リッチテキスト署名](#)」を参照してください。

セキュアメール 10.8.15

- **iOS版Secure Mail**がリッチテキスト署名をサポートするようになりました。メール署名に画像やリンクを使用できます。詳細については、「[リッチテキスト署名](#)」(/ja-jp/citrix-secure-mail/ios-features.html#rich-text-signatures)を参照してください。

- **Secure Mailは、以前はAndroid for Workとして知られていたAndroid Enterpriseをサポートしています。** Secure MailでAndroid Enterpriseアプリを使用することで、個別の仕事用プロフィールを作成できます。詳細については、「Secure MailでのAndroid Enterprise」([/ja-jp/citrix-secure-mail/android-features.html#android-enterprise-in-secure-mail](https://ja-jp/citrix-secure-mail/android-features.html#android-enterprise-in-secure-mail))を参照してください。
- **Secure Mailは、メールの表示中に埋め込みリソースをレンダリングします。** リソースが社内ネットワークに存在する場合（内部リンクである画像URLを含むメールなど）、Secure Mailは社内ネットワークに接続してコンテンツを取得し、レンダリングします。
- **Secure Mailは最新の認証をサポートしています。** 最新の認証は、ユーザー名とパスワードを使用したOAuthトークンベースの認証です。このサポートには、内部および外部のActive Directory Federation Services (AD FS) またはIDプロバイダー (IdP) 用のOffice 365のサポートが含まれます。
- **添付ファイルリポジトリのパフォーマンス強化。** 添付ファイルリポジトリをはるかに高速にスクロールできるようになりました。

セキュアメール 10.8.10

- **メール添付ファイルの印刷のサポート。** iOS版Secure Mailは、メール添付ファイルの印刷をサポートしています。
- **Microsoft Office 365での最新の認証。** iOS版Secure Mailは最新の認証をサポートしています。最新の認証は、ユーザー名とパスワードを使用したOAuthトークンベースの認証です。このサポートには、外部および内部のActive Directory Federation Services (AD FS) およびIDプロバイダー (IdP) 用のOffice 365のサポートが含まれます。詳細については、「Microsoft Office 365を使用した最新の認証」([/ja-jp/citrix-secure-mail/modern-authentication-office-365.html](https://ja-jp/citrix-secure-mail/modern-authentication-office-365.html))を参照してください。

注：

このリリースでは、Microsoft Intune/EMSとのEndpoint Management統合による最新の認証はサポートされていません。

このリリースには、AD FSが外部からアクセス可能なシナリオでの最新の認証が含まれています。

既知の問題と修正された問題

Citrix® は、モバイル生産性向上アプリの最新の2つのバージョンからのアップグレードをサポートしています。

iOS向け セキュアメール 26.8.0

修正された問題

- iPad で、メールの会話に最新のメッセージのみが表示され、スレッド内の以前のメッセージとその添付ファイルが欠落する場合があります。
- iPad で、週表示カレンダーからカレンダー項目を開くと、空白の画面が表示される場合があります。
- iOS 27 を実行しているデバイスで、Secure Mail が白い画面を表示する場合があります。
- 添付ファイルを別のアプリと共有したり、ファイルに保存したりすると、元のファイル名がランダムに生成された文字列に置き換えられる場合があります。

既知の問題

このリリースには既知の問題はありません。

Android向け セキュアメール 26.5.0

修正された問題

- メールサーバーでピングストームまたはダウンロードストームの状態が HTTP 503 エラーを引き起こす場合、メールの同期とコンテンツのダウンロードが失敗する可能性があります。
- Secure Mail for Android で、ゲートウェイ証明書の更新が失敗する場合があります。
- 互換性の問題により、Secure Mail が AMAPI モードで起動しない場合があります。

既知の問題

このリリースには既知の問題はありません。

iOS用セキュアメール 26.5.0

修正された問題

- iPadで、Secure Mailの添付ファイルオプションが表示されない場合があります。
- iPadで、Secure MailでHTMLカレンダー招待の本文がレンダリングされない場合があります。
- Secure Hubが再認証を要求しない場合、Secure Mailの画面が点滅することがあります。
- 初回起動時に、Secure Mailが白い画面を表示し、再起動後にのみ回復する場合があります。
- DEPデバイスでアプリのワイプを実行すると、MDMプロファイルが削除されない場合があります。

既知の問題

このリリースには既知の問題はありません。

iOS用セキュアメール 26.1.0

修正された問題

- XenMobileでテキストのコピーがブロックされている場合でも、ユーザーは翻訳オプションを使用してテキストをコピー＆ペーストできる場合があります。
- **Open in** オプションを使用してファイル添付を開こうとすると、空白のファイルが表示され、添付ファイルが開かない場合があります。
- iPhone版Secure Mailで小さな添付ファイル（1MB未満）を開こうとすると、アプリが「添付ファイルを開けません」というエラーメッセージを表示して開けない場合があります。
- ユーザー証明書の有効期限が切れると、ユーザーは重複した証明書更新プロンプトを受け取る場合があります。
- PINの最大再試行回数を超過した場合、Secure Mailが回復しない場合があります。
- Secure Mailで連絡先を編集すると、アプリが応答しなくなる場合があります。
- Secure Mailを使用していると、アプリが断続的に空白の画面を表示する場合があります。
- iPad版Secure Mailのカレンダー検索オーバーレイが、背景のボタンを適切に覆わない場合があります。

既知の問題

このリリースには既知の問題はありません。

Android版セキュアメール 25.12.0

修正された問題

- 登録済みのAndroidデバイスでSecure Mailを使用している場合、一部のユーザーがActive Directory (AD) アカウントのロックアウトを経験する場合があります。
- 登録済みのAndroidデバイスが、有効な証明書が既に存在する場合に重複したAccess Gateway (AG) クライアント証明書を受け取り、PKIサーバーへの負荷が増大する場合があります。
- Secure Mailのプッシュ通知がAndroidデバイスで機能しない場合があります。
- Android版Secure Mailで入力中にスクロールが機能しない場合があります。

既知の問題

このリリースには既知の問題はありません。

iOS 用 セキュアメール 25.9.0

修正された問題

- iPad で Secure Mail をバージョン 25.5.0 にアップデートすると、一部のページでスクーリングの問題が発生し、ディスプレイがサポートされない場合があります。
- Secure Mail で O365 メールアカウントを追加できない場合があります。
- 証明書の有効期限が切れると、証明書の同期と要求が失敗する場合があります。
- Secure Hub がデバイスから削除された後も、アプリが利用可能なままになる場合があります。
- AG セッションの有効期限が切れると、Secure Mail が機能しなくなる場合があります。
- Face ID または Touch ID が有効なデバイスのロックを解除すると、Secure Mail がコンテンツを表示できない場合があります。
- カレンダーイベントページにアクセスした後、Secure Mail がアプリモードをダークまたはライトに切り替えられない場合があります。
- iPad で **稼働週の開始日** 設定が更新された後、Secure Mail が設定ページを正しく表示できない場合があります。

既知の問題

このリリースには既知の問題はありません。

Android 用 セキュアメール 25.8.0

修正された問題

- AndroidデバイスのSecure Mailでメールリンクをクリックすると、リンクが期待どおりに機能しない場合があります。
- Android版Secure Mailでサイズの大きい添付ファイルを開こうとすると、「Not enough memory」というエラーメッセージが表示され、アプリが予期せず終了する場合があります。
- Access Gateway証明書の有効期限が切れると、Android版Secure Mailでメールの取得に失敗する場合があります。

既知の問題

このリリースには既知の問題はありません。

Android版 セキュアメール 25.6.0

修正された問題

- XiaomiデバイスをOperating System 14にアップグレードすると、Secure Mailがクラッシュし、プロセスがサポートされない場合があります。
- 証明書の強力なマッピングが有効になっているExchange環境を使用すると、Transport Layer Security (TLS) 接続が失敗する場合があります。
- 言語をオランダ語に設定すると、Secure Mailカレンダーのポップアップボタンが整列しない場合があります。

既知の問題

このリリースには既知の問題はありません。

iOS版 セキュアメール 25.5.0

修正された問題

- Secure MailでSkypeから送信された不在着信メールを開こうとすると、アプリが突然終了する場合があります。
- ドメインコントローラーにパッチ **KB5014754** を適用した後、Secure Mail が接続に失敗する可能性があります。

- Wi-Fi に再接続した場合、または証明書もしくは Secure Ticket Authority (STA) チケットのいずれかが期限切れになった場合、アプリが同期に失敗する可能性があります。
- Secure Mail で証明書の有効期限が切れている場合、アプリが証明書の更新に失敗する可能性があります。
- Secure Mail で GoToMeeting にログインしようとする、次のエラーメッセージが表示され、プロセスが失敗する可能性があります。「このエンドポイントは無効になりました」

既知の問題

このリリースには既知の問題はありません。

セキュアメール for Android 25.3.0

修正された問題

このバージョンでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

既知の問題

このリリースには既知の問題はありません。

セキュアメール for Android 25.1.0

修正された問題

このバージョンでは、全体的なパフォーマンスと安定性を向上させる領域に対処しています。

既知の問題

このリリースには既知の問題はありません。

iOS 用 セキュアメール 25.1.0

修正された問題

- Secure Mailで10 MBを超えるメール添付ファイルを開こうとすると、添付ファイルのダウンロードに失敗する場合があります。
- iOS 18を実行しているiPhoneのSecure Mailで複数のメールアカウントが構成されている場合、アプリが突然終了することがあります。

既知の問題

このリリースには既知の問題はありません。

iOS 用 セキュアメール 24.11.0

修正された問題

ネットワーク接続の問題により、Secure MailはiPhoneとiPadの両方のデバイスでメールを同期できません。

既知の問題

- Wi-Fiを切断して再接続すると、Secure Mailはサーバーと同期しません。回避策として、ユーザーはSecure Mailを再起動できます。
- ユーザーがSecure Mailに2つのアカウントを追加すると、Secure Mailが突然終了することがあります。回避策として、この問題を回避するためにSecure Mailを横向きモードで使用してください。

アンドロイド版 セキュアメール 24.11.0

修正された問題

このリリースには修正された問題はありません。

既知の問題

このリリースには既知の問題はありません。

Android版 セキュアメール 24.9.1

修正された問題

折りたたみ式AndroidスマートフォンまたはAndroidタブレットでSecure Mailを使用している場合、メールを作成しようとするアプリが自動的に終了することがあります。

既知の問題

このリリースには既知の問題はありません。

Android版 セキュアメール 24.9.0

修正された問題

MAMモードでSecure Mailを開くと、次のエラーメッセージが表示されることがあります。

「SDK管理ポリシーへのサポートされていない変更。」

既知の問題

このリリースには既知の問題はありません。

iOS版 セキュアメール 24.9.0

修正された問題

- Secure Mail for iOSで、次のエラーメッセージ「セッションの有効期限が切れたため、このメッセージを取得できません。」を含む誤ったプッシュ通知が表示される場合があります。
- Secure Mail for iOSで他のカレンダーアプリから受信した会議の招待状にある.icsファイルをクリックすると、アプリが誤って間違った時間に予定をスケジュールする場合があります。
- Secure Mail for iOSをダークモードで使用している場合、メールを転送しようとする、メール本文の内容が読みにくくなります。
- Secure Mail for iOSで、カレンダーの月表示から日表示に切り替えると、アプリが強制終了します。
- Secure Mail for iOSでは、カレンダーの招待ページがSecure Mailアプリのテーマ設定ではなく、デバイスの設定に基づいてダークまたはライトテーマで表示されます。

既知の問題

このリリースには既知の問題はありません。

Android版 セキュアメール 24.7.0

修正された問題

このリリースには修正された問題はありません。

既知の問題

このリリースには既知の問題はありません。

iOS版 セキュアメール 24.3.0

修正された問題

- Secure Mail のインストールと登録が正常に完了しても、エンドユーザーがアプリを設定する際に次のエラーメッセージが表示されることがあります。

「サーバーへの接続がタイムアウトしました。数分後にもう一度お試しください」

- Secure Mail for iOS バージョン 24.2.0 にアップグレードした後、既存のエンドユーザーが Secure Mail にアクセスできなくなり、次のエラーメッセージが表示されることがあります。

「Secure Mail がサーバーに接続できませんでした。サーバーアドレスをもう一度入力してください。それでも問題が解決しない場合は、IT 管理者にお問い合わせください」

- エンドユーザーが iPad デバイスでアプリを開こうとすると、Secure Mail が応答しなくなります。この問題は、iPad バージョン 17.3.1 以降を実行しているデバイスに固有のものです。

既知の問題

このリリースには既知の問題はありません。

iOS版 セキュアメール 24.2.0

修正された問題

- Secure Mail for iOS で、カレンダーページに「追加」ボタン (+) が表示されず、新しいカレンダーイベントを作成できない場合があります。
- ネットワーク接続の問題により、Secure Mail は iPhone と iPad の両方のデバイスでメールを同期できません。
- Secure Mail for iOS でダークモードを使用すると、メールメッセージを読めない場合があります。

既知の問題

このリリースには既知の問題はありません。

Android版 セキュアメール 24.1.0

修正された問題

- 10 MBを超えるメール添付ファイルを開こうとすると、Secure Mail for Androidが応答しなくなります。
- アラビア文字またはハイパーリンクを含む.docx形式のメール添付ファイルを開こうとすると、Secure Mail for Androidが応答しなくなります。この問題は、Polaris SDKが更新されていない場合に発生します。

既知の問題

このリリースには既知の問題はありません。

Android版 セキュアメール 23.10.0

修正された問題

- Secure Mailから添付ファイルを開くと、デバイスに**Citrix Files**アプリがインストールされていなくても、**その他 (:) >** で開くオプションの下に**Citrix Files**に**アップロード**オプションが表示されることがあります。
- Secure Mailで受信した会議の招待状に添付された.icsファイルをプレビューすると、.icsファイルのプレビューに表示される会議時刻が元の時刻より1時間遅れていることに気づく場合があります。この問題は、夏時間地域で発生します。
- Secure Mailをバージョン23.8.2にアップグレードしてダークモードを有効にすると、メール添付ファイルをプレビューする際に問題が発生する可能性があります。省略記号****(...)****ボタンをクリックしてもメニューリストが表示されない場合があります。

既知の問題

このリリースには既知の問題はありません。

Android版 セキュアメール 23.8.2

修正された問題

このリリースには、修正された問題はありません。

既知の問題

Secure Mail をバージョン 23.8.2 にアップグレードし、ダークモードを有効にすると、メールの添付ファイルをプレビューする際に問題が発生する可能性があります。省略記号 (...) ボタンをクリックしても、メニューリストが表示されない場合があります。回避策として、Secure Mail をライトモードに切り替えることができます。

AndroidおよびiOS版 Secure Mail 23.7.0

修正された問題

このリリースには、修正された問題はありません。

既知の問題

このリリースには、既知の問題はありません。

Android版 セキュアメール 23.8.1

修正された問題

このリリースには、修正された問題はありません。

既知の問題

このリリースには、既知の問題はありません。

iOS版 セキュアメール 23.9.0

修正された問題

- HCL Domino 11サーバーでSecure Mail for iOS 23.2.0バージョンを使用している場合、以前に保存した下書きメールを送信できないことがあります。Secure Mailではメールが正常に送信された则表示されますが、受信者には届きません。

既知の問題

このリリースには既知の問題はありません。

Android版 セキュアメール 23.8.0

修正された問題

このリリースには修正された問題はありません。

既知の問題

このリリースには既知の問題はありません。

Android版 セキュアメール 23.7.0

修正された問題

- カレンダーイベントのリマインダー通知が届かないことがあります。この問題は、Secure Mailのアラームとリマインダーの権限が取り消された場合に発生します。

既知の問題

このリリースには既知の問題はありません。

Android版セキュアメール 23.6.0

修正された問題

メール添付ファイルを表示すると、「License expired.」という透かしが表示されることがあります。この問題は、Android版Secure Mailバージョン23.3.5以前を使用している場合に発生します。透かしなしでメール添付ファイルを表示するには、Android版Secure Mailバージョン23.6.0以降にアップグレードしてください。

既知の問題

このリリースには既知の問題はありません。

iOS版セキュアメール 23.5.0

修正された問題

- デジタル署名されたメールを受信し、Secure Mailで開くと、メール添付ファイルが表示されない場合があります。

既知の問題

このリリースには既知の問題はありません。

以前のバージョンにおける既知の問題と修正された問題

Secure Mailの以前のバージョンにおける既知の問題と修正された問題については、を参照してください。 (</ja-jp/citrix-secure-mail/known-fixed-issues-history.html>).

Secure Mail の既知の修正済み問題の履歴

この記事では、最近サポートされているバージョンよりも前のバージョンの Secure Mail の修正済みおよび既知の問題を一覧表示します。最新のドキュメントについては、[Citrix Secure Mail](#)を参照してください。

セキュアメール 23.3.5

Android 版 Secure Mail の既知の問題

- カレンダーイベントのリマインダー通知が届かない場合があります。この問題は、Secure Mail のアラームとリマインダーのアクセス許可が取り消された場合に発生します。

回避策として、**設定 > アプリ > 特別なアクセス > アラームとリマインダー > Secure Mail** に移動し、タップして通知をオンにします。

Android 版 Secure Mail の修正済み問題

- Android 13 にアップグレードすると、Secure Mail が応答なくなります。

セキュアメール 23.2.0

iOS および Android 版 Secure Mail の既知の問題

このリリースには既知の問題はありません。

Android 版 Secure Mail の修正済み問題

- Secure Mail で添付ファイルを開くと、ドキュメントの一部を覆う灰色の透かしが表示されることがあります。この問題は、Polaris ライセンスの有効期限が切れた場合に発生します。

この問題は、プレビューされる添付ファイルが次の形式である場合に影響します。

- .ドックス
- エクセル
- パワーポイント
- テキスト

- Secure Mailで**Open with...**オプションを使用して**.docx**、**.pptx**、**.xlsx**ファイルを開こうとすると、対応するネイティブアプリでファイルを開けない場合があります。この問題は、Android 13を使用している場合に発生します。

iOS版Secure Mailの修正済み問題

- Microsoft Teamsから**Voice Mail**メールを開こうとすると、Secure Mailが応答しなくなります。
- Skypeから**Missed Call**メールを開こうとすると、Secure Mailが応答しなくなります。この問題は、グローバルExchangeアドレス帳に外部発信者の識別情報が含まれていない場合に発生します。

セキュアメール 22.11.0

Android版Secure Mailの既知の問題

このリリースには既知の問題はありません。

Android版Secure Mailの修正済み問題

- Android版Secure Mailで添付ファイル付きのメールを開くと、添付ファイルの内容のスクリーンショットを撮ることができません。この問題は、制限ポリシーが無効になっている場合でも発生する可能性があります。
- 添付ファイル付きのメールを転送すると、メールは送信トレイに残ります。メールを手動で送信（送受信操作を開始）した後、受信者は添付ファイルを開くことができません。この問題は断続的に発生します。
- Secure Mailカレンダーからアクセスした場合、Webex会議リンクがそれぞれのアプリで開きません。

セキュアメール 22.9.0

iOSおよびAndroid版Secure Mailの既知の問題

このリリースには既知の問題はありません。

iOSおよびAndroid版Secure Mailの修正された問題

このリリースには修正された問題はありません。

セキュアメール 22.6.2

iOS版Secure Mailの既知の問題

このリリースには既知の問題はありません。

iOS版Secure Mailの修正された問題

- Secure Webを使用してファイルをダウンロードし、Secure Mailを使用して受信者に送信しようとする、**新規メッセージオプション**が表示されません。

セキュアメール 22.6.0

iOS版Secure Mailの既知の問題

このリリースには既知の問題はありません。

iOS版Secure Mailの修正された問題

- iOS版Secure Mailでメールを作成中に連絡先を追加しようとする、誤った連絡先の詳細が表示されます。
- アプリを開くと、iOS版Secure MailおよびSecure Webが応答しなくなります。

セキュアメール 22.3.0

Secure Mail 22.3.0 の既知の問題

- カレンダーイベントを編集し、会議のリマインダー時間を更新すると、会議の主催者にリマインダーが表示されません。この問題は、組織が HCL Domino 11 サーバー (旧 Lotus Notes) を実行している場合に発生します。
- 定期的なイベントを日次イベントに更新し、そのうちの1つの発生を編集しようとする、編集オプションが表示されません。この問題は、組織が HCL Domino 11 サーバーを実行している場合に発生します。
- 定期的なイベントの単一インスタンスの日付または時刻を変更すると、その会議はランダムな日付に再スケジュールされます。この問題は、組織が HCL Domino 11 サーバーを実行している場合に発生します。

Secure Mail 22.3.0 で修正された問題

このリリースには修正された問題はありません。

セキュアメール 22.2.0

Secure Mail 22.2.0 の既知の問題

このリリースには既知の問題はありません。

Secure Mail 22.2.0 で修正された問題

- Samsung SM-A315 および SM-F926 デバイスで、Secure Mail がセットアップ中にクラッシュします。

セキュアメール 21.12.0

修正された問題

- 添付された Microsoft Office ファイルを開くと、Android 版 Secure Mail がクラッシュします。この問題は、デバイスの言語がトルコ語に設定されている場合に発生します。
- Android版Secure MailのActive Directoryでアカウントパスワードを変更した後、アプリにサインインできません。

セキュアメール 21.11.0

このリリースには、既知の問題も修正された問題もありません。

セキュアメール 21.10.5

Android版Secure Mailで修正された問題

Network AccessがTunneled-Web SSOモードに設定されているオンプレミスのCitrix Endpoint Management™ (CEM)を使用すると、Microsoft Teams会議の作成に失敗します。この問題は、Citrix Gatewayの既知の問題により、Application Delivery Controller (ADC)がベアラートークンを含む認証ヘッダーを削除するために発生します。

Android版Secure Mailの既知の問題

このリリースには既知の問題はありません。

セキュアメール 21.10.0

Android版Secure Mailの既知の問題

このリリースには既知の問題はありません。

Android版Secure Mailで修正された問題

- Android版Secure Mailで、Android 12 Beta 4を実行しているデバイスでインタラクティブなPDFファイルを開くと、ファイルがクラッシュします。
- Android版Secure Mailで、埋め込み画像を含むメールを開くと、空白の画面が表示されます。
- 携帯電話ネットワークからWi-Fiネットワークに切り替えてから再び戻ると、Android版Secure Hubへのサインインを求められます。認証のためにPINを入力すると、Secure Mailからアカウントの有効期限が切れているというプロンプトが表示され、サインインに失敗します。
- Android版Secure Mailバージョン21.7.0にアップグレードすると、メールの同期に失敗します。

セキュアメール 21.9.1

Android版Secure Mailの既知の問題

- Android 12 Beta 4を実行しているデバイスでインタラクティブなPDFファイルを開くと、ファイルがクラッシュします。
- ワークプロファイルに外部Webブラウザがすでにインストールされている場合、Secure Webがデフォルトのブラウザでないと、リンクは外部ブラウザアプリで開きます。

Android版Secure Mailの修正された問題

- ワークプロファイルモードに登録されているデバイスでSecure Mailバージョン21.8.0を起動できません。この問題は、Citrix Endpoint ManagementがMicrosoft Intune/EMSと統合された環境で実行されている場合に発生します。
- デバイスでダークモードを有効にしている場合、Android版Secure Mailの添付ファイルが暗く表示され、内容が判読できません。

セキュアメール 21.9.0

このリリースには、既知の問題も修正された問題もありません。

セキュアメール 21.8.5

既知の問題

- Android 12 Beta 4を実行しているデバイスでインタラクティブなPDFファイルを開くと、ファイルがクラッシュします。
- ワークプロファイルに外部Webブラウザがすでにインストールされている場合、Secure Webがデフォルトのブラウザでないと、リンクは外部ブラウザアプリで開きます。

修正された問題

このリリースには修正された問題はありません。

セキュアメール 21.8.0

既知の問題

このリリースには既知の問題はありません。

修正された問題

- Android版Secure Mailで、Zoom会議のリンクをタップするとMicrosoft Teamsアプリが開きます。この問題は、Microsoft TeamsとZoomの両方がデバイスにインストールされている場合に発生します。
- 日付形式をdd-mm-yyyyとしてExcelファイルを作成し、Android版Secure Mailでこのファイルを開くと、日付形式が「mm-dd-yyyy」に変更されます。
- Android版Secure MailでPDFファイルを開くと、検証用の署名が表示されません。

セキュアメール 21.7.0

既知の問題

このリリースには既知の問題はありません。

修正された問題

iOS版Secure Mailでは、英語以外の言語で個人の連絡先グループが同期されません。

セキュアメール 21.6.0

このリリースには既知の問題も修正された問題也没有ありません。

セキュアメール 21.5.0

このリリースには、既知の問題も修正された問題也没有ありません。

セキュアメール 21.4.5

このリリースには、既知の問題も修正された問題也没有ありません。

セキュアメール 21.4.0

このリリースには、既知の問題も修正された問題也没有ありません。

セキュアメール 21.3.5

このリリースには、既知の問題も修正された問題也没有ありません。

セキュアメール 21.3.0

このリリースには、既知の問題も修正された問題也没有ありません。

セキュアメール 21.2.0

既知の問題

作成中のメールに画像を添付するために写真アイコンをクリックすると、カメラアプリがクラッシュします。この問題は、デバイスがAndroid 11を実行しており、Secure Mailがワークプロファイルモードで構成されている場合に発生します。

修正された問題

このリリースには、修正された問題はありません。

セキュアメール 21.1.5

iOS版セキュアメール

このリリースには、既知の問題も修正された問題也没有ありません。

セキュアメール 21.1.0

既知の問題

このリリースには既知の問題はありません。

修正された問題

iOS版Secure Mailでは、山括弧で囲まれた会議リンクをタップしても会議が開始されません。空白の画面が表示されます。

セキュアメール 20.12.0

iOS版セキュアメール

このリリースには、既知の問題も修正された問題もありません。

セキュアメール 20.11.0

このリリースには、既知の問題も修正された問題もありません。

セキュアメール 20.10.5

既知の問題

iOS版Secure Mailでは、通知設定にサブフォルダー (メールフォルダー) オプションがありません。

修正された問題

このリリースには、修正された問題はありません。

セキュアメール 20.10.0

既知の問題

iOS版Secure Mailでは、通知設定にサブフォルダー (メールフォルダー) オプションがありません。

修正された問題

このリリースには、修正された問題はありません。

セキュアメール 20.9.5

Android版 セキュアメール

このリリースには、既知の問題も修正された問題もありません。

セキュアメール 20.9.0

既知の問題

iOS版Secure Mailでは、通知設定にサブフォルダー (メールフォルダー) オプションがありません。

修正された問題

タイムゾーンがアリゾナの場合、iOS版Secure Mailの会議の招待状に誤った時刻 (1時間のずれ) が表示されます。

セキュアメール 20.8.5

Android版セキュアメール

既知の問題

Android 11を実行している一部のデバイスでは、連絡先とカレンダーの会議の詳細が全画面で開かなくなります。

修正された問題

このリリースには修正された問題はありません。

セキュアメール 20.8.0

このリリースには既知の問題も修正された問題もありません。

セキュアメール 20.7.5

このリリースには既知の問題も修正された問題もありません。

セキュアメール 20.7.0

このリリースには既知の問題も修正された問題もありません。

セキュアメール 20.6.5

既知の問題

このリリースには既知の問題はありません。

修正された問題

- Secure Mail for iOSでは、フォントサイズを大きく設定しても、メッセージビューでテキストを大きく表示できません。
- Secure Mail for iOSでは、同じドメインで複数のアカウントを設定すると、通知を受信できません。

セキュアメール 20.6.0

既知の問題

このリリースには既知の問題はありません。

修正された問題

- iOSを実行しているデバイスでは、IBM Travelerサーバーで特定のHTTPヘッダーを変更した後、Secure Mailの同期が停止します。
- Secure Mail for iOSでは、メールを受信したときに通知をタップしてもメールを開けません。次のエラーが表示されます: **メールを取得できません。**

セキュアメール 20.5.0

iOS用セキュアメール

既知の問題

このリリースには既知の問題はありません。

修正された問題

- iOS 13.4 を実行している iPad では、Secure Mail でテキスト選択が機能しません。

- iOS 版 Secure Mail では、**VoiceOver** 機能でメールを読み取ることができません。

セキュアメール 20.4.5

既知の問題

このリリースには既知の問題はありません。

修正された問題

- iOS 版 Secure Mail では、iPhone のメール作成ウィンドウでアクセシビリティサイズが尊重されません。
- iOS 版 Secure Mail では、iPad で **Share In** オプションを使用しているときに添付ファイルを追加できません。

セキュアメール 20.4.0

既知の問題

このリリースには既知の問題はありません。

修正された問題

- iOS を実行しているデバイスで、メール作成中に Secure Mail からコピーした画像を貼り付けると、受信者はその画像を表示できません。
- iOS 版 Secure Mail では、Office 365 に移行した後、複数の認証プロンプトが表示されます。
- iOS 版 Secure Mail では、Outlook で作成されたカレンダー招待を編集すると、説明を表示できません。招待を変更すると、説明が削除されます。

セキュアメール 20.3.0

このリリースには、既知の問題も修正された問題もありません。

セキュアメール 20.2.0

このリリースには、既知の問題も修正された問題もありません。

セキュアメール 20.1.5

既知の問題

このリリースには既知の問題はありません。

修正された問題

- iOS版Secure Mailでは、T-Mobile LTEネットワークで動作しているデバイスでメール通知が失敗します。
- iOS版Secure Mailでは、デバイスを縦向きモードから横向きモードに切り替えても、メール内の画像がリサイズされません。

セキュアメール 20.1.0

既知の問題

- Android版Secure Mailでは、カレンダーイベントからGTMにログオンできません。
- Android版Secure Mailでは、[添付ファイル] タブからファイルを添付するとメールを送信できません。
- Android 7を実行しているデバイスでは、バージョン19.12.7からバージョン20.1.0にアップグレードすると、Secure Mailが断続的にクラッシュします。

修正された問題

- ホーム画面でSecure Mailアイコンを長押しし、iPadでカレンダーをタップすると、受信トレイが表示されます。
- Android版Secure Mailでは、デジタル著作権管理 (DRM) 添付ファイルを開くことができません。

セキュアメール 19.12.5

既知の問題

iOS 13を実行しているデバイスで特定のPDFファイルを表示しているときに、iOS版Secure Mailがクラッシュします。

修正された問題

- iOS 13を実行しているデバイスで、Secure Mailが繰り返しクラッシュします。このクラッシュは、iPhone XS、11 Pro、11 Pro Maxなどの最新のAppleデバイスで発生します。
- iOS版Secure Mailでは、iPhoneの音声ディクテーションやApple Smart Keyboardの矢印キーなどの機能がiOS 13で動作しません。

セキュアメール 19.11.5

このリリースには、既知の問題も修正された問題もありません。

iOS版セキュアメール 19.10.6

iOS版Secure Mailの既知の問題

このリリースには既知の問題はありません。

iOS版Secure Mailの修正された問題

iOS 13を実行しているデバイスで、Secure Mail for iOSを使用している場合、メール作成中に断続的にクラッシュします。

セキュアメール 19.10.5

既知の問題

このリリースには既知の問題はありません。

修正された問題

iOS 13を実行しているiPhoneで、ユーザーがMDXアプリからファイルをダウンロードした後、Secure Mailでファイルを開くことができません。

セキュアメール 19.10.0

このリリースには既知の問題も修正された問題もありません。

セキュアメール 19.9.5

既知の問題

このリリースには既知の問題はありません。

修正された問題

- Secure Mail for Androidでは、証明書ベースの認証を実行しているデバイスで、サイズの大きいメールを同期できません。
- Secure Mail for iOSでは、IBM Lotus Travelerでユーザーのインスタンスを再プロビジョニングすると、メールフォルダーが重複します。
- Secure Mail for Androidでは、通知を受信できません。

セキュアメール 19.9.0

既知の問題

Microsoft Intune/EMSを実行しているiOS版Secure Mailで、**Share > Copy to Word**をタップしてMS Wordアプリを使用してMS Wordドキュメントを開くとクラッシュします。

修正された問題

- Android版Secure Mailで、既読メールを削除すると、OutlookおよびSecure Mailの**削除済みアイテム**に未読メールとして表示されます。
- iOS版Secure Mailで、添付ファイル付きのデジタル署名されたメールが送信されると、メール受信者は添付ファイルを受信しません。
- Active Directory Federation Services (ADFS) および Outlook 365 に接続しようとする、Secure Mail iOSがクラッシュします。
- Androidを実行しているデバイスで、Secure Mailを認証できません。次のエラーが表示されます: 認証中にエラーが発生しました。

セキュアメール 19.8.5

Android版Secure Mailの既知の問題

このリリースには既知の問題はありません。

Android版Secure Mailで修正された問題

- カレンダーイベントのリマインダーが通知バーに表示されている場合、その後のカレンダーリマインダーの通知アラートは受信されません。多数のカレンダーリマインダーを作成し、デバイスがアイドル状態またはDozeモードの場合、Secure Mailのカレンダー通知は遅延します。
- Android版Secure Mailで、設定をクリックすると、Secure Mailまたはサードパーティアプリを使用してアクションを完了する選択肢が表示されたポップアップが表示されます。
- Android版Secure Mailでは、受信した特定のメールの日付が Jan 1, 1970 になっています。
- Secure Mail for Androidでは、500人を超えるメンバーを含む連絡先グループを同期できません。

セキュアメール 19.8.0

既知の問題

Secure Mail for iOSで、メール通知をタップしてTouch IDでログインすると、クラッシュします。この問題は、アプリがバックグラウンドで実行されていない場合に発生します。

修正された問題

このリリースには、修正された問題はありません。

セキュアメール 19.7.5

既知の問題

このリリースには、既知の問題はありません。

修正された問題

- Secure Mail for Androidで、すでに読んだメールに対して複数の通知を受け取ります。
- Secure Mail for iOSで、カレンダーが同期されず、次のエラーが表示されます: カレンダーを同期できませんでした。

セキュアメール 19.6.5

既知の問題

このリリースには、既知の問題はありません。

修正された問題

- Secure Mail for iOS で、メールに返信すると、送信トレイには返信のみが表示され、スレッド全体は表示されませんでした。
- Secure Mail for Android で、メールのコンテンツが正しくレンダリングされません。
- カレンダーイベントの時刻をドラッグアンドドロップで変更し、更新を送信しても、招待者の応答がリセットされません。
- Secure Mail for Android で、カレンダーイベントの時刻をドラッグアンドドロップで変更しているときに、断続的にクラッシュします。

セキュアメール 19.5.5

既知の問題

- Secure Mail for Android で、ネットワークアクセスポリシーがトンネル化 - **Web SSO**に設定されている場合、HttpURLConnection を確立できません。
- Secure Mail for iOS で、アプリがフォアグラウンドまたはバックグラウンドで実行されていない場合、通知応答オプションが機能しません。

修正された問題

Secure Mail for Android で、メールを送信すると、受信者がメールを複数回受信します。この問題は、Android 8 以降を実行しているデバイスで発生します。

セキュアメール 19.5.0

既知の問題

iOS を実行しているデバイスで、許可された **Wi-Fi ネットワーク MDX** ポリシーで定義されている許可された Wi-Fi ネットワークの外部の Wi-Fi ネットワークに接続できます。この問題により、MDX ポリシーにリストされていないネットワークを介して Secure Mail および Secure Web for iOS を開くことができます。

修正された問題

- Secure Mail for Android で、新規メール作成時に **宛先:** または **Cc/Bcc:** フィールドにメールアドレスを貼り付けることができません。ただし、メールに返信する際は、**宛先:** または **Cc/Bcc:** フィールドにメールアドレスを貼り付けることができます。

- Secure Mail for Android で、Android Enterprise デバイスを登録する際にアカウント構成設定を保存できません。
- Secure Mail for Android で、数日間使用すると受信トレイが空になります。

Android版 セキュアメール 19.4.6

Secure Mail for Android の既知の問題と修正された問題

このリリースには、既知の問題も修正された問題もありません。

セキュアメール 19.4.5

既知の問題

このリリースには既知の問題はありません。

修正された問題

- Secure Mail for iOS で、Outlook で会議出席依頼を送信し、Secure Mail で編集しても、Outlook で会議が更新されません。受信者も更新を受け取りません。この問題は、Secure Mail で会議出席依頼を作成し、Secure Mail で編集した場合にも発生します。
- Secure Mail for iOS で、カレンダーが同期されず、次のエラーが表示されます: **カレンダーを同期できませんでした。**
- Secure Mail for Android で、Outlook を使用して作成した会議出席依頼の一部が Secure Mail カレンダーに反映されません。
- Secure Mail for Android で、定期的な会議が遅延して表示され、会議への更新が正しく同期されません。

セキュアメール 19.3.5

既知の問題

このリリースには既知の問題はありません。

修正された問題

- iOS版Secure Webでは、ブラウザにBitlyのURLを貼り付けることができません。
- iOS版Secure Mailでは、受信するすべてのメールに対して「このメッセージを取得できません。Secure Mailを開いてください。」というエラーメッセージが表示されます。

- iOS版Secure Mailでは、ユーザーがアプリケーションを開いてPINを入力すると、「会社のネットワークが利用できません」というエラーメッセージが頻繁に表示されます。
- 多要素認証に切り替えた後、iOS版Secure Mailが同期に失敗します。

セキュアメール 19.3.0

既知の問題

このバージョンには既知の問題はありません。

修正された問題

- iOS版Secure Mailでは、無効なネットワークセッションが原因でリクエストがタイムアウトした場合、メールを受信すると「**Secure Mail**はリクエストのタイムアウトによりこのメッセージを取得できません」という通知バナーが断続的に表示されます。
- Android版Secure Mailでは、mozaiekwonen.xm.cloud.comからのFirebase Cloud Messaging (FCM) 通知を受信できません。
- Android版Secure Mailでは、カレンダーイベントを更新しても、変更がOutlook Office 365と同期されません。
- Android版Secure Mailでは、ネットワーク接続が不良またはない場合、添付ファイルを含むメールが送信されません。これらのメールは、ネットワーク接続が回復した後も送信トレイに残ります。

セキュアメール 19.2.0

既知の問題

証明書でOnline Certificate Status Protocol (OCSP) staplingによる透過性オプションが有効になっている場合、iOS 12.1.1以降でSecure Mailの構成が失敗します。

修正された問題

- iOS版Secure Mailでは、Secure Mailの件名フィールドからSecure Notesバージョン10.8.6.6にテキストをコピーできません。
- Android版Secure Mailで、Samsungデバイスで予測変換が有効になっている場合、テキストの最後の単語に下線が引かれます。スペースを空けずに署名に最後の単語を保存すると、下線が引かれた状態で保存され、受信者にもそれが表示されます。
- Android版Secure Mailで、メールダイジェストを受信しても画像が表示されません。

- Intune Company Portalバージョン5.0.4324.0がインストールされている場合、Android版 Secure Mailは起動時にクラッシュします。

iOS 用セキュアメール 19.1.6

iOS版Secure Mailの既知の問題と修正された問題

このリリースには既知の問題も修正された問題もありません。

セキュアメール 19.1.5

既知の問題

このリリースには既知の問題はありません。

修正された問題

- iOS版Secure Mailでは、受信するすべてのメールに対して次のエラーメッセージが表示されます: このメッセージを取得できません。 Secure Mailを開いてください
- iOS版Secure Mailでは、アプリケーションを開いてPINを入力すると、「会社のネットワークが利用できません」というエラーメッセージが頻繁に表示されます。
- ラップされたAndroidアプリケーションでは、UserAgent文字列が複数回追加され、ヘッダーサイズが増加します。この動作によりエラーが発生し、ページが読み込まれません。

セキュアメール 19.1.0

既知の問題

このリリースには既知の問題はありません。

修正された問題

- Secure MailがExchange Serverへの接続に失敗すると、メール通知バナーに次のメッセージが表示されます。

「セッションの有効期限が切れました。このメッセージを取得できません。セッションを更新するにはSecure Mailを開いてください。」

この問題は修正され、メッセージは次のように更新されました。

「Secure Mailは組織のネットワークに接続できません。管理者にお問い合わせください。」

- O365メールボックスを使用しているユーザーが、はい、いいえ、たぶん、または削除などの通知応答アクションを繰り返し実行すると、Office 365のスロットリングが発生し、次のエラーメッセージが表示されます。

「サーバーがビジー状態です。もう一度お試しください。」

- Android版Secure Mailでトルコ語を使用している場合、アドレスに文字「İ」が含まれる受信者にメールを送信できません。
- Android版Secure Mailでは、ユーザーはメールの件名を選択して強調表示できません。
- Secure Mail for Android で、パスワードに文字 € が含まれている場合、ログオンに失敗します。
- Secure Mail for Android で、ローカル連絡先と同期設定が有効になっている場合、すべての Secure Mail 連絡先がネイティブ連絡先にエクスポートされます。同期後、携帯電話、職場、自宅、職場FAX、自宅FAXなどの電話フィールドが正しい順序で表示されません。たとえば、ネイティブ連絡先では、FAX番号が携帯電話番号の上に表示されます。ユーザーはこの順序を変更できません。

セキュアメール 18.12.0

修正された問題

- Secure Mail for iOS で、リッチテキスト形式 (RTF) のメールを受信すると、特定の種類のインライン添付ファイルと添付ファイルの記号が表示されません。
- Secure Mail for iOS で、リッチプッシュ通知が有効になっていて、メール通知をオフにしてからオンにすると、メールの種類オプションが断続的に表示されます。
- 環境でクライアントベースの認証メカニズムを実行している場合、Secure Mail はメールを断続的に自動同期できません。手動同期を実行しても、一部のメールしか取得されません。

セキュアメール 18.11.1

修正された問題

- IBM Notes Traveler 9.0.1 SP 10 に接続している Secure Mail for Android では、添付ファイル付きのメールが送信トレイに残ります。

既知の問題

- Secure Mail for Android では、メール内の埋め込み画像を表示できません。

- Secure Mail for Android は、`file:///C:...\jpg.` のような埋め込み URL を含む署名を持つメールを開くとクラッシュします。

セキュアメール 18.10.5

修正された問題

- 「iOSデータ保護MDXポリシーを有効にする」が有効になっている場合、「新しいメールがあります」という通知が断続的に届きます。
- iPhone XSでは、添付ファイルをダウンロードまたは送信できず、ダウンロードした画像を表示できません。
- Exchange ActiveSyncバージョン16以降を実行しているアカウントで、ユーザーが定期的な会議を変更すると、会議がExchange Serverで更新されません。その結果、会議はSecure MailとOutlookの間で同期されません。

セキュアメール 18.10.0

修正された問題

- Android版Secure Mailでは、ユーザーはExchangeサーバー以外のサーバーを指すインライン画像を表示できません。
- Android版Secure Mailでは、Webex会議に参加する際に、PIN番号がダイヤルイン番号に追加されませんでした。PIN番号を手動で入力する必要があります。
- 個人用カレンダーが構成されていない場合、Secure Mail for AndroidはSecure Mailカレンダーのエクスポート中にクラッシュします。
- iPhone XSのiOS版Secure Mailでは、添付ファイルをダウンロードまたは送信できず、ダウンロードした画像を表示できません。

セキュアメール 18.9.0

修正された問題

- NT LAN Manager (NTLM) 認証要求ごとに、クライアントワークステーションがランダムに変更されます。
- Android PでのSecure Mailの同期は、デバイスがバッテリーセーバーモードの場合、断続的に動作を停止します。

- 個人用カレンダーが構成されていない場合、Secure MailはSecure Mailカレンダーのエクスポート中にクラッシュします。

セキュアメール 10.8.65

修正された問題

- FIPsが有効で、ユーザーがiOS 11.3デバイスでSecure Mail for iOSを実行している場合、カット、コピー、およびペーストのMDXポリシーが機能しません。
- 共有デバイスでSecure Mail for iOSを使用している場合、新しいユーザーは、以前のユーザーがサインインしていないにもかかわらず、そのユーザーのメールを表示できます。新しいユーザーがディスプレイを更新するためにフォルダーをタップすると、以前のユーザーのメールは表示されなくなります。

セキュアメール 10.8.60

修正された問題

注:

Secure Mailバージョン10.8.25から10.8.60には、既知の問題は含まれていません。

- IBM Lotus Dominoサーバーで実行されているSecure Mail for iOSでは、受信トレイの検索アイコンを使用できません。
- ユーザーがIntune会社ポータルを使用してSecure Mail for Androidを実行しているデバイスを登録すると、Secure Mailが動作を停止します。
- FTUフロー中にサーバーから多数のメールフォルダーを同期しているときに、Secure Mail for iOSがクラッシュします。
- Secure Mail for iOSでは、PDFの印刷プレビューが小さく表示されます。
- Secure Mail for Androidでは、メールに返信するときに、複数のメールIDが自動入力されません。

セキュアメール 10.8.55

修正された問題

- Secure Mail for iOSでは、横向きモードで表示した場合、カレンダーの週表示がiPad Proで正しく表示されません。

バージョン 10.8.55 でのMDX関連の修正済み問題

- Androidでは、ユーザーがSecure HubからサインアウトするとSecure Mailがクラッシュします。
- iOSデバイスでは、Secure WebとSecure Mail 10.8.45が起動時にクラッシュします。

セキュアメール 10.8.50

修正された問題

- iOS版Secure MailはビデオファイルをShareFileに保存できません。
- Android版Secure Mailでプッシュ通知を有効にしても、新しいメールの通知が届きません。この問題は断続的に発生します。

セキュアメール 10.8.45

修正された問題

Secure Mailバージョン10.8.45には、修正された問題は含まれていませんでした。

セキュアメール 10.8.40

修正された問題

iOS版Secure Mailでは、新しいメールを受信するたびに重複した通知が断続的に表示されます。

セキュアメール 10.8.35

修正された問題

- Android版Secure Mailでは、自動同期が断続的に停止します。Office 365サーバーからの新しいメッセージの一部をSecure Mailに表示するには、ユーザーが手動で同期する必要があります。

- Android版Secure Mailでは、メールとカレンダーイベントのメール通知を無効にしても、通知が表示され、音による通知が発生します。
- Android版Secure Mailを使用して終日イベントを作成すると、Outlookカレンダーに誤った日付が表示されます。
- Android版Secure Mailでは、Exchangeの個人連絡先グループがアプリに同期されません。
- SSOが構成されている場合、Android版Secure MailのExchangeへのSSOが失敗します。ユーザーはサインインのためにパスワードを求められます。

セキュアメール 10.8.25

修正された問題

- Android版Secure Mailでは、ユーザーがカレンダーの招待をOffice 365と同期する際に遅延が発生します。この問題は、カレンダーの招待を作成または更新する際に発生します。
- Android版Secure Mailで、ユーザーがcc:フィールドに1文字入力し、**送信**をタップすると、Secure Mailは頻繁に使用されるユーザーのリストの最初のユーザーにメッセージを送信します。代わりに、cc:フィールドのエントリが無効であることを示す通知が表示されるべきです。
- Android 7を実行しているZebra T51デバイスでは、ユーザーはCitrix Launcherアプリをインストールできません。
- NetScaler® Gatewayが証明書ベースの認証で構成されている場合、iOS版Secure Mailでは、新しいメッセージを受信するたびに「新しいメールがあります」というメッセージが表示されます。代わりに、通知には送信者名、件名、本文のプレビューが表示されるべきです。

セキュアメール 10.8.20

修正された問題

- MAM専用モードで登録されたAndroidデバイスにIntune Company Portalアプリがインストールされている場合、Endpoint Managementでは、Secure MailがMicrosoftログインページにリダイレクトしようとします。次のエラーメッセージが表示されます。「アプリの構成を受信しませんでした。アプリを構成するには、管理者にお問い合わせください。」
- Android版Secure Mailでは、ユーザー名またはパスワードにä、ö、ü、€などの特殊文字が含まれている場合、サインインに失敗します。
- Androidデバイスでは、再起動すると認証をバイパスしてSecure Mailにアクセスできます。

- Android版Secure Mailで、インライン画像がダウンロードされる前にメールに返信すると、メールが送信トレイにスタックします。この問題は、設定で**画像の表示**設定が有効になっている場合に発生します。
- iOS版Secure Mailで、IRMポリシーが**ON**でメール分類が**保護済み**に設定されている場合、メール全体をダウンロードしても添付ファイルを表示できません。

セキュアメール 10.8.10

修正された問題

- iOS版Secure Mail 10.7.25にアップデートした後、Message-IDヘッダーに括弧（<および>）がありません。
- iOS版Secure Mailで、ユーザーがOutlookからカレンダー招待を追加した後、アプリが断続的にクラッシュします。この問題は、カレンダー招待に絵文字が含まれている場合に発生します。
- iOSで、モバイル生産性アプリを10.7.30にアップグレードした後、ログレベルが11以上に設定されている場合、Secure Mailは動作が遅くなり、開いたままにするとクラッシュします。
- iOS版Secure Mailで、画面ロック通知の制御ポリシーが**カウントのみ**に設定されている場合、重複する通知が断続的に表示されます。
- Android版Secure Mailで、ユーザーが宛先:フィールドに4つ以上のメールアドレスをコピー & ペーストすると、アプリがクラッシュします。

AndroidおよびiOS版Secure Mail - プレビュー

今後のリリースで提供される新機能と解決済みの問題にご期待ください。

現在のリリースの詳細については、[Secure Mailの新機能](#)を参照してください。

機能フラグ管理

管理者は、プレビュー機能にアクセスし、本番環境で機能を動的に制御するために、機能フラグを管理できます。機能フラグの下にある機能が最適に機能するようにするには、URL `features.netscalergateway.net` へのトラフィックを有効にする必要があります。詳細については、「[機能フラグ管理](#)」を参照してください。

Secure Mailの展開

Citrix Endpoint Management™（旧XenMobile）でSecure Mailを展開するには、以下の一般的な手順に従ってください。

1. Secure MailをExchange ServerまたはIBM Notes Traveler Serverと統合して、Secure MailをMicrosoft ExchangeまたはIBM Notesと同期させることができます。IBM Notesを使用している場合は、IBM Notes Travelerサーバーを構成します。この構成では、Active Directoryの資格情報を使用してExchangeまたはIBM Notes Travelerサーバーに対して認証を行います。詳細については、「[Exchange ServerまたはIBM Notes Traveler Serverの統合](#)」を参照してください。

重要：

Secure MailからIBM Notes Traveler（旧IBM Lotus Notes Traveler）とのメール同期はできません。このLotus Notesのサードパーティ機能は現在サポートされていません。そのため、Secure Mailから返信済みの会議メールを削除しても、IBM Notes Travelerサーバー上ではメールは削除されません。ユーザーがカレンダーイベントを承諾した後、コメント付きでイベントを辞退したり、コメントに対してアクションを実行したりすると、コメントが失われます。

2. Secure HubからSSOをオプションで有効にできます。これを行うには、Endpoint ManagementコンソールでCitrix Filesアカウント情報を構成し、Endpoint ManagementをCitrix FilesのSAML IDプロバイダーとして有効にします。この構成では、Active Directoryの資格情報を使用してCitrix Filesに対して認証を行います。

Endpoint ManagementコンソールでのCitrix Filesアカウント情報の構成は、すべてのCitrixクライアント、Citrix Filesクライアント、および非MDX Citrix Filesクライアントで使用される1回限りの設定です。詳細については、「[SSOのためにEndpoint ManagementコンソールでCitrix Filesアカウント情報を構成するには](#)」を参照してください。

3. Citrix DownloadsサイトからSecure Mailの.mdxファイルをダウンロードします。
4. Secure MailをEndpoint Managementに追加し、MDXポリシーを構成します。詳細については、「[アプリの追加](#)」を参照してください。

注：

Secure Mailバージョン10.6.5以降、iOSおよびAndroid版Secure Mail向けに新しいMDX分析ポリシーを構成できます。Citrixは製品品質向上のために分析データを収集します。Google Analyticsの詳細レベルポリシーを使用すると、データが会社のドメインに関連付けられるか、匿名で収集されるかを指定できます。**匿名**を選択すると、収集されるデータに会社のドメインを含めることをユーザーがオプトアウトします。この新しいポリシーは、以前のGoogle Analyticsポリシーに代わるものです。

ポリシーが匿名に設定されている場合、以下の種類のデータを収集します。ユーザーを特定できる情報を要求しないため、このデータを個々のユーザーや会社に関連付ける方法は一切ありません。個人を特定できる情報はGoogleに送信されません。

- オペレーティングシステムのバージョン、アプリのバージョン、デバイスモデルなどのデバイス統計
- ActiveSyncのバージョンやSecure Mailサーバーのバージョンなどのプラットフォーム情報
- APNs登録、メールの同期と送信、添付ファイルのダウンロードとカレンダーの同期など、製品品質に関する障害点。

会社ドメイン以外に、ポリシーが**Complete**に設定されている場合、他の識別可能な情報は収集されません。デフォルトは**Complete**です。

Secure Mail の構成

Secure Mail で構成および統合できる機能は次のとおりです。

- Office 365 を使用した最新認証(/ja-jp/citrix-secure-mail/modern-authentication-office-365.html)
- オンプレミス Exchange を使用したハイブリッド最新認証(/ja-jp/citrix-secure-mail/hybrid-modern-authentication-on-premises-exchange.html)
- Secure Mail のバックグラウンドサービス(/ja-jp/citrix-secure-mail/configuring-background-services-secure-mail.html)
- Exchange Server または IBM Notes Traveler Server の統合(/ja-jp/citrix-secure-mail/exchange-ibm.html)
- Secure Mail における S/MIME(/ja-jp/citrix-secure-mail/s-mime.html)
- Secure Mail における SSO(/ja-jp/citrix-secure-mail/sso-secure-mail.html)

Microsoft Office 365でのモダン認証

Secure Mail は、Active Directory Federation Services (AD FS) または Identity Provider (IDP) 向けの Microsoft Office 365 でのモダン認証をサポートしています。モダン認証は、ユーザー名とパスワードを使用する OAuth トークンベースの認証です。iOS デバイスを使用する Secure Mail ユーザーは、Office 365 に接続する際に証明書ベースの認証を利用できます。Secure Mail にサインオンする際、ユーザーは資格情報を入力する代わりに、クライアント証明書を使用して認証します。

続行する前に、以下を実行してください。

1. Microsoft Office 365 のモダン認証 (OAuth) を有効にします。
2. 最適なネットワーク接続を確保するために、ファイアウォールで Office 365 のエンドポイント、URL、および IP アドレス範囲を有効にします。詳細については、Microsoft ドキュメントの「[Office 365 URL および IP アドレス範囲](#)」を参照してください。

注:

- ハイブリッド Exchange メールボックスソリューションを移行または作成するには、Microsoft ドキュメントの「[Exchange ハイブリッド展開での Exchange ActiveSync デバイス設定](#)」を参照してください。

Citrix Endpoint Management™ ポリシーの前提条件

Citrix Endpoint Management コンソールで以下のポリシーを有効にします。

iOS を実行しているデバイスの場合:

- **Office 365 認証メカニズム:** このポリシーを使用して、Office 365 でアカウントを構成する際に認証に使用される OAuth メカニズムを示します。このポリシーには、構成する必要がある以下の値があります。
 - **OAuth を使用しない:** アカウント構成時の基本認証には、このポリシーを使用します。
 - **ユーザー名とパスワードで OAuth を使用する:** 認証時の OAuth プロトコルには、このポリシーを使用します。ユーザーは、OAuth フローのためにユーザー名とパスワード、およびオプションで多要素認証コードを提供する必要があります。
 - **クライアント証明書で OAuth を使用する:** Office 365 が証明書ベースの認証を実行するように構成されている場合は、このポリシーを使用します。デフォルトの構成は **OAuth を使用しない** です。

Android を実行しているデバイスの場合:

- **O365の最新認証を使用:** 認証時のOAuthプロトコルにこのポリシーを使用します。
- **トンネリング用Web SSOポリシー:** OAuthトラフィックをトンネル化して、トンネル化された Web SSO 経由で送信するために、このポリシーを使用します。そのためには:
 - **トンネリング用Web SSOを使用ポリシーをオンに設定**します。
 - ネットワークアクセス ポリシーで、**トンネル化された - Web SSO** オプションを選択します。

注:

STAを有効にする方法については、[STA経由でのメールサーバーへの接続](#)を参照してください。

- 。 OAuthに関連するすべてのホスト名をバックグラウンドサービスポリシーから除外します。

iOSおよびAndroidデバイスに共通のポリシー:

- **最新認証用のカスタムユーザーエージェント:** 最新認証のデフォルトのユーザーエージェント文字列を変更するには、このポリシーを使用します。
- **信頼されたExchange Onlineホスト名:** アカウント設定時に認証にOAuthメカニズムを使用する信頼されたExchange Onlineホスト名のリストを定義するには、このポリシーを使用します。これは、server.company.com, server.company.co.uk のようなコンマ区切りの形式です。このリストには、デフォルト値またはバニティURLを含めることができますが、空にすることはできません。デフォルト値はoutlook.office365.comです。
- **信頼されたAD FSホスト名:** Office 365 OAuth認証中にパスワードが自動入力されるWebページ用の信頼されたAD FSホスト名のリストを定義するには、このポリシーを使用します。これは、 sts.companyname.com, sts.company.co.uk のようなコンマ区切りの形式です。リストが空の場合、Secure Mailはパスワードを自動入力しません。Secure Mailは、Office 365認証中に表示されたWebページのホスト名とリストされたホスト名を照合し、そのページがHTTPSプロトコルを使用しているかどうかを確認します。たとえば、 sts.company.com がリストされたホスト名で、ユーザーが https://sts.company.com に移動した場合、そのページにパスワードフィールドがあれば、Secure Mailはパスワードを自動入力します。デフォルト値は login.microsoftonline.com です。
- **Office 365 Exchange Server:** クラウド上にあるOffice 365メールボックスのホスト名を定義するには、このポリシーを使用します。ホスト名は、 outlook.office365.com のような単一の値です。デフォルト値は outlook.office365.com です。
- **Secure Mail Exchange Server:** Exchange Serverのアドレスを定義するには、このポリシーを使用します。このポリシーを使用して、要件に基づいてオンプレミスサーバーアドレスまたはクラウドサーバーアドレスのいずれかを定義できます。
- **HTTP 451リダイレクトの構成:** リダイレクトの構成方法の詳細については、Knowledge Centerの記事[Secure Mail ActiveSync redirect 451](#)を参照してください。

デバイスでポリシーが更新されると、iOS版Secure Mailで最新認証が有効になります。

Exchange Server の構成オプション

Secure Mail は、 outlook.office365.com または Microsoft 統合ドメイン outlook.cloud.microsoft を使用して構成できます。

outlook.office365.com を使用した構成

Secure Mail Exchange Server として outlook.office365.com を使用して Secure Mail を構成するには:

- Secure Mail Exchange Server を outlook.office365.com に設定します。
- Background network services に outlook.office365.com:443 を追加します。
- Trusted Exchange Online Hostnames をデフォルト値の outlook.office365.com のままにします。
- Office 365 Exchange Server をデフォルト値の outlook.office365.com のままにします。

Microsoft 統合ドメイン outlook.cloud.microsoft を使用した構成

Secure Mail Exchange Server として outlook.cloud.microsoft を使用して Secure Mail を構成するには:

- Secure Mail Exchange Server を outlook.cloud.microsoft に設定します。
- Background network services に outlook.cloud.microsoft:443 を追加します。
- Trusted Exchange Online Hostnames に outlook.cloud.microsoft を追加します。
- Office 365 Exchange Server をデフォルト値の outlook.office365.com のままにします。
新しいドメインに置き換えないでください。

制限事項

- 環境でモダン認証を使用している場合、iOSの豊富なプッシュ通知機能は利用できません。豊富なプッシュ通知の詳細については、[Secure Mailのプッシュ通知](#)を参照してください。
- 証明書ベースの認証を実行しているセットアップでは、複数のアカウントはサポートされていません。

Secure Mailポリシー

以下の2つの表に、Exchangeインフラストラクチャに基づいて必要なSecure Mailポリシーを記載します。

EXCHANGEインフラ ストラクチャ	OFFICE 365 認証メカ ニズム/O365 にモダ ン認証を使用	信頼済みAD FSオンラ インホスト名	信頼済みEXCHANGE オンラインホスト名
オンプレミス	オフ	NA	NA

EXCHANGEインフラ ストラクチャ	OFFICE 365 認証メカ ニズム/O365 にモダ ン認証を使用	信頼済みAD FSオンラ インホスト名	信頼済みEXCHANGE オンラインホスト名
ハイブリッド*	オン	AD FS/IDP	Outlook.office365.com またはバニ ティURL
エクスチェンジ オン ライン	オン	AD FS/IDP	Outlook.office365.com またはバニ ティURL

EXCHANGEインフラ ストラクチャ	セキュアメール エクス チェンジ サーバー	バックグラウンドネッ トワークサービス (IOS)	バックグラウンドネッ トワークサービス (ANDROID)
オンプレミス	Exchangeオンプレミ スホスト名	オンプレミス	オンプレミス
ハイブリッド*	オンプレミス、 Exchange Onlineホ スト名	オンプレミス、オン プレミスExchangeホ スト名	オンプレミス、オン プレミスExchangeホ スト名、AD FS/IDP (内部のみ)
エクスチェンジオン ライン	Outlook.office365.com	Exchange Onlineホ スト名	オンプレミス Exchangeホスト名、 AD FS、IDP

*Secure Mailは、移行されたメールボックスを持つハイブリッドExchangeインフラストラクチャをサポートします。

オンプレミスユーザーのメールボックスがExchange Onlineに移行された場合、Secure Mailはこの変更を自動的に検出し、アカウントを再構成することなく、ユーザーに最新の認証を促します。

OAuthサポートマトリックスを備えたSecure Mail

次の表は、iOSおよびAndroidデバイスでのSecure Mail OAuthサポートマトリックスを示しています。

認証タイプ	IDP/外部AD FS	IDP/内部AD FS	アジュール AD	インチューン
ユーザー名とパスワード	はい	はい	はい	はい
クライアント証明書	はい	Androidのみ	いいえ	いいえ

iOSおよびAndroid向けオンプレミスExchangeサポートによるハイブリッド最新認証

ハイブリッド最新認証 (HMA) は、より安全なユーザー認証および承認方法を使用するユーザーID管理ソリューションです。現在、Exchange Serverオンプレミスハイブリッド展開で利用できません。

HMAは、ユーザー名とパスワードを使用したOAuthトークンベースの認証です。これにより、オンプレミスのメールボックスユーザーはOAuthトークンを使用してオンプレミスExchangeにアクセスできます。OAuthトークンはクラウドから取得されます。最新認証でユーザーIDを管理することで、管理者はリソースを保護するためにさまざまなツールを使用でき、オンプレミスExchangeに対してより安全なID管理方法を提供します。

HMAの詳細については、「[Announcing Hybrid Modern Authentication for Exchange On-Premises](#)」を参照してください。

MDXポリシーで必要な変更

Secure Mail iOSおよびAndroidでHMAを機能させるには、**OAuth Support for Office 365**セクションのMDXポリシーで次の変更を実行します。

- Androidの場合、**Use Modern authentication for O365**オプションを有効にします。iOSの場合、**Office 365 authentication mechanism**を**Use OAuth with Username and Password**に設定します。
- **Trusted Exchange Online Hostnames**テキストフィールドに、顧客のオンプレミスExchange URLを入力します。
- **Office 365 Exchange Server**テキストフィールドに、顧客のオンプレミスExchange URLを入力します。
- **Next**をクリックします。

注：MDXポリシーで上記の変更を行う前に、ExchangeでHMA設定が有効になっていることを確認してください。そうでない場合は、**Use Modern authentication for O365**オプションを無効にします。

AndroidのOAuth Support for Office 365セクション：

iOSのOAuth Support for Office 365セクション：

初回ユーザーログインが成功すると、次の同意ページが表示されます。**承諾**をクリックします。

HMA同意ページ(/en-us/mobile-productivity-apps/media/hma-consent-page.png)

オプション：この同意ページが表示されないようにするには、次の手順を実行します。

- Microsoft Azureポータルを開きます。
- ダッシュボードから、**App registrations > HMA-App**に移動します。
- **Configured permissions**セクションで、**Grant admin consent for CRMC3Online**オプションを有効にします。

HMA アプリ Azure(/en-us/mobile-productivity-apps/media/hma-app-azure.png)

制限事項

- HMAから基本認証に切り替えるには、既存のアカウントを削除し、Secure Mailで新しいアカウントを再作成する必要があります。
- MDXポリシーとExchangeポリシーが一致しない場合、ユーザーはSecure Mailにサインインできません。

Secure Mailのバックグラウンドサービス

Citrix Gateway 経由でメールサーバーにアクセスするには、Secure Mail のバックグラウンドサービスを構成する必要があります。Secure Mail を Citrix Endpoint Management™ (旧称: XenMobile) に追加する際は、MDX アプリポリシーの設定でバックグラウンドサービスを構成します。

Secure Mailのバックグラウンドサービスを構成するには

1. 管理者資格情報を使用してEndpoint Managementコンソールにサインオンします。
2. コンソールで、**Configure**タブをクリックし、**Apps**をクリックして、Secure Mailアプリを選択し、**Edit**をクリックします。

バックグラウンドサービスを構成する(/en-us/mobile-productivity-apps/media/configure-bg-services1.png)

3. **MDX policy settings**ページで、**Platform**セクションのiOSまたはAndroidプラットフォームを必要に応じて選択します。
4. **App settings**セクションで、ポリシーを構成します。

プラットフォームを選択してポリシーを構成する(/en-us/mobile-productivity-apps/media/configure-bg-services2.png)

バックグラウンドサービス構成用のMDXアプリポリシー

以下のMDXアプリポリシーは、Secure MailとCitrix Gateway、Citrix Endpoint Managementサーバー、Secure Ticket Authority (STA)サーバー、およびメールサーバーとの通信に影響します。

ネットワークアクセス: ネットワークアクセス ポリシーは、Secure MailがVPNを使用してバックグラウンドネットワークサービスにアクセスできるか、またはすべてのトラフィックがインターネット経由で無制限に送信されるかを指定します。

- ネットワークアクセス ポリシーが **Tunneled to the internal network** に設定されている場合、バックグラウンドネットワークサービスにリストされているURLのみがCitrix Gatewayを通過

します。それ以外のトラフィックはインターネット経由で無制限に送信されます。デフォルトでは、Secure Mailアクセスは **Tunneled to the internal network** です。

- ネットワークアクセス ポリシーが **Unrestricted** に設定されている場合、Secure Mailから発信されるすべてのトラフィックはインターネット経由で無制限に送信されます。バックグラウンドサービスへのアクセスにはVPNは使用されません。

ネットワークアクセスポリシー(/en-us/mobile-productivity-apps/media/network-tunnel.png)

Secure Mail Exchange Server: Secure Mail Exchange Serverポリシーをメールサーバーの完全修飾ドメイン名 (FQDN) に設定します。

Background network service: Background network serviceポリシーは、Citrix Gateway経由でのアクセスが許可されているメールサーバーのリストを指定します。ホスト名とポート番号をカンマ区切りの値としてリストします。値の間に先頭および末尾のスペースがないことを確認してください。メールサーバーのアドレスには、 `hostnameFQDN : portnumber` を含めます。例:

`mail1.example.com:443,mail2.example.com:443` (カンマとカンマの間にスペースなし)。

Background network service gateway: Background network service gatewayポリシーは、Secure Mailがメールサーバーへの接続に使用するCitrix Gatewayを指定します。Citrix Gatewayのアドレスには、 `citrixgatewayFQDN : portnumber` を含めます。例:

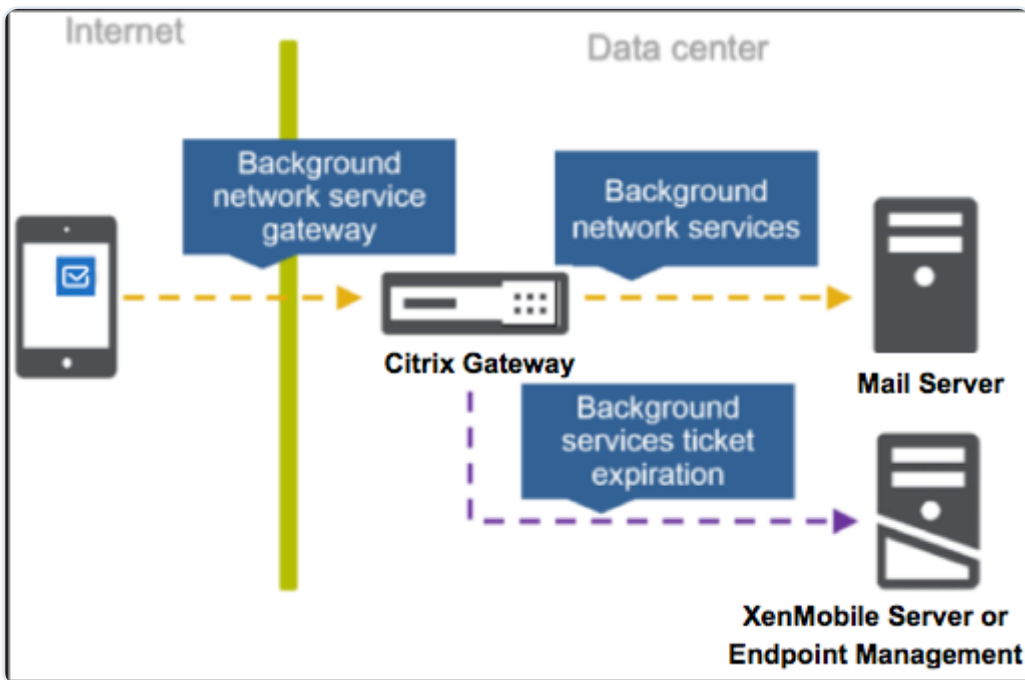
`gateway3.example.com:443`。

Background services ticket expiration: このポリシーは、バックグラウンドネットワークサービスチケットの有効期間を指定します。Secure MailがCitrix Gateway経由でメールサーバーに接続すると、Citrix Endpoint Managementは内部メールサーバーへの接続に使用されるトークンを発行します。この設定は、Secure Mailがこのトークンを使用できる期間を決定します。トークンがアクティブな場合、メールサーバーへの認証と接続のために新しいトークンは必要ありません。時間制限が切れると、ユーザーは新しいトークンを生成するために再度ログオンする必要があります。このトークンのデフォルト値は168時間（7日間）です。

バックグラウンドサービス用のMDXアプリポリシーの詳細については、以下を参照してください。

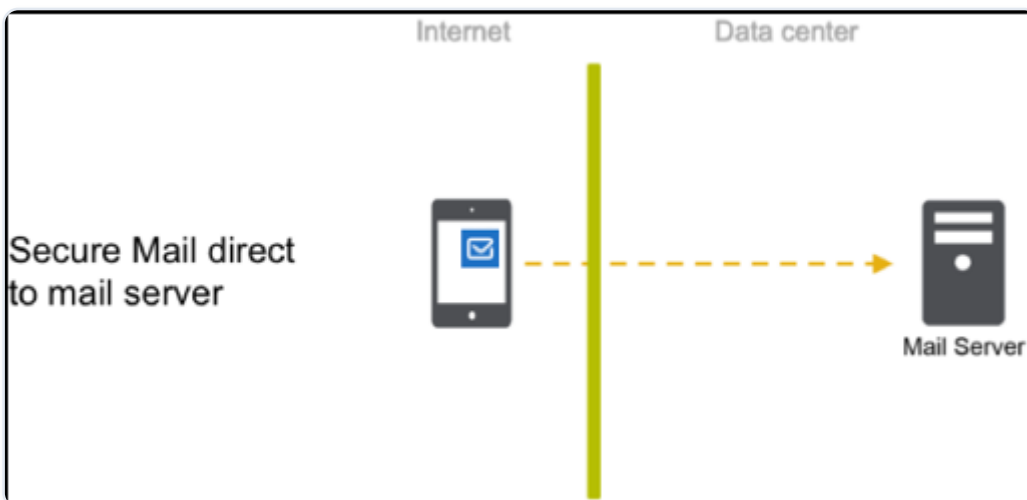
- [Android用Secure Mailアプリ設定ポリシー](#)
- [iOS用Secure Mailアプリ設定ポリシー](#)

次の図は、通信フローとこれらのポリシーが適用される場所を示しています。



次の図は、メールサーバーへのSecure Mail接続の種類を示しています。各図の後には、関連するポリシー設定のリストがあります。

メールサーバーへの直接接続



メールサーバーへの直接接続のポリシー:

- ネットワークアクセス: **無制限**

ネットワークアクセスが無制限の場合、以下のポリシーは適用されません。

- バックグラウンドネットワークサービス: 該当なし
- バックグラウンドサービスチケットの有効期限: 該当なし
- バックグラウンドネットワークサービスゲートウェイ: 該当なし

STA経由でのメールサーバーへの接続

STAを使用するSecure Mailの画像(/en-us/mobile-productivity-apps/media/sta-connection.png)

STA経由でメールサーバーに接続するためのポリシー:

- ネットワークアクセス: **Tunneled - Web SSO**
- バックグラウンドネットワークサービス:
`mail.example.com:443, mail1.example1.com:443, outlook.office365.com:443 or vanity URL:443`
- バックグラウンドサービスチケットの有効期限: **168**
- バックグラウンドネットワークサービスゲートウェイ: `gateway3.example.com:443`

注:

Citrixは、Secure MailにSTA接続を使用することを推奨します。これは、STA接続が長期間のセッション接続をサポートするためです。

STAの詳細については、この[Citrix Knowledge Centerの記事](#)を参照してください。

Exchange Server または IBM Notes Traveler Server の統合

Secure Mail をメールサーバーと同期させるには、Secure Mail を社内ネットワーク内にある、または Citrix Gateway の背後にある Exchange Server または IBM Notes Traveler Server と統合します。

- Secure Mail のバックグラウンドサービスを構成するには、「[Secure Mail のバックグラウンドサービス](#)」を参照してください。
- Secure Mail 用の IBM Notes Traveler Server を構成するには、「[Secure Mail 用の IBM Notes Traveler Server の構成](#)」を参照してください。

重要:

Secure Mail から IBM Notes Traveler (旧 IBM Lotus Notes Traveler) とメールを同期することはできません。この Lotus Notes のサードパーティ機能は現在サポートされていません。そのため、たとえば Secure Mail から会議メールを削除しても、IBM Notes Traveler サーバー上ではメールは削除されません。

Secure Notes および Secure Tasks でも同期が可能です。ただし、Secure Notes および Secure Tasks は December 31, 2018 にサポート終了 (EOL) ステータスに達しました。詳細については、「[EOL および非推奨のアプリ](#)」を参照してください。

- iOS 用 Secure Notes を同期するには、Exchange Server と統合します。
- Android 用 Secure Notes および Secure Tasks を同期するには、Secure Mail for Android アカウントを使用します。

Secure Mail、Secure Notes、および Secure Tasks を Citrix Endpoint Management (旧 XenMobile) に追加する場合は、「[バックグラウンドサービス構成の MDX アプリポリシー](#)」に記載されている MDX ポリシーを構成します。

注:

Android および iOS 用 Secure Mail は、Notes Traveler Server に指定されたフルパスをサポートしています。例: `https://mail.example.com/traveler/Microsoft-Server-ActiveSync`。

Traveler Server の Web サイト置換ルールで Domino Directory を構成する必要はなくなりました。

Secure Mail 用の IBM Notes Traveler サーバーの構成

IBM Notes 環境では、Secure Mail を展開する前に IBM Notes Traveler サーバーを構成する必要があります。このセクションでは、この構成の展開図とシステム要件を示します。

重要:

Notes Traveler Server が SSL 3.0 を使用している場合、SSL 3.0 には Padding Oracle On Downgraded Legacy Encryption (POODLE) 攻撃と呼ばれる脆弱性が含まれていることに注意してください。これは、SSL 3.0 を使用してサーバーに接続するすべてのアプリに影響を与える中間者攻撃です。POODLE 攻撃によって引き起こされる脆弱性に対処するため、Secure Mail はデフォルトで SSL 3.0 接続を無効にし、TLS 1.0 を使用してサーバーに接続します。その結果、Secure Mail は SSL 3.0 を使用する Notes Traveler Server に接続できません。推奨される回避策の詳細については、[Integrating Exchange Server or IBM Notes Traveler Server](#) の「Configuring SSL/TLS Security Level」セクションを参照してください。

IBM Notes 環境では、Secure Mail を展開する前に IBM Notes Traveler サーバーを構成する必要があります。

インフラストラクチャサーバーの要件

- IBM Domino メールサーバー 9.0.1

- ## 認証プロトコル

- Domino データベース

- 19 附件

- Exchange: デフォルトの SSL ポートは

SSL/TLSセキュリティレベルの構成

Citrixは、前述の重要な注意事項に記載されているPOODLE攻撃によって導入された脆弱性に対処するために、Secure Mailに変更を加えました。したがって、Notes Traveler ServerがSSL 3.0を使用して接続を有効にしている場合、推奨される回避策は、IBM Notes Traveler Server 9.0でTLS 1.2を使用することです。

IBMは、Notes Travelerのセキュアなサーバー間通信でSSL 3.0の使用を防止するパッチを提供しています。2014年11月にリリースされたこのパッチは、以下のNotes Travelerサーバーバージョンの中間修正アップデートとして含まれています: 9.0.1 IF7、9.0.0.1 IF8、および8.5.3 Upgrade Pack 2 IF8 (そして、今後のすべてのリリースに含まれる予定です)。

代替の回避策として、Secure MailをEndpoint Managementに追加する際に、接続セキュリティレベルポリシーを**SSLv3 and TLS**に変更します。

以下の表は、接続セキュリティレベルポリシーの値に基づいて、Secure Mailがオペレーティングシステム別にサポートするプロトコルを示しています。メールサーバーもプロトコルをネゴシエートできる必要があります。

以下の表は、接続セキュリティレベルがSSLv3 and TLSの場合のSecure Mailでサポートされるプロトコルを示しています。

オペレーティングシステムの種類	エスエスエルブイスリー	TLS
iOS 9以降	いいえ	はい
Android Mより前	はい	はい
Android M および Android N	はい	はい
アンドロイド O	いいえ	はい

以下の表は、接続セキュリティレベルがTLSの場合のSecure Mailでサポートされるプロトコルを示しています。

オペレーティングシステムの種類	エスエスエル バージョン3	TLS
iOS 9 以降	いいえ	はい
Android M より前	いいえ	はい

オペレーティングシステムの種類	エスエスエル バージョン3	TLS
Android M および Android N	いいえ	はい
アンドロイド O	いいえ	はい

ノーツトラベラーサーバーの構成

以下の情報は、IBM Domino Administrator クライアントの構成ページに対応しています。

- **セキュリティ:** インターネット認証は、より高いセキュリティで名前のバリエーションを少なくするように設定されています。この設定は、LDAP 認証プロトコルで UID を AD ユーザー ID にマッピングするために使用されます。
- **NOTES.INI 設定:** `NTS_AS_ENFORCE_POLICY=false` を追加します。これにより、Secure Mail のポリシーは Traveler ではなく Endpoint Management によって管理されるようになります。この設定は現在の顧客の展開と競合する可能性があります、Endpoint Management の展開におけるデバイスの管理を簡素化します。
- **同期プロトコル:** IBM Notes の SyncML およびモバイルデバイスの同期は、現時点では Secure Mail でサポートされていません。Secure Mail は、Traveler サーバーに組み込まれている Microsoft ActiveSync プロトコルを介して、メール、カレンダー、連絡先アイテムを同期します。SyncML がプライマリプロトコルとして強制された場合、Secure Mail は Traveler インフラストラクチャを介して接続できません。
- **Domino ディレクトリ構成 - Web インターネットサイト:** /traveler のセッション認証を上書きして、フォームベース認証を無効にします。

セキュアメール用 S/MIME

Secure Mail は Secure/Multipurpose Internet Mail Extensions (S/MIME) をサポートしており、ユーザーはメッセージに署名して暗号化することでセキュリティを強化できます。署名により、受信者は、メッセージがなりすましではなく、識別された送信者によって送信されたことを確認できます。暗号化により、互換性のある証明書を持つ受信者のみがメッセージを開くことができます。

S/MIME の詳細については、Microsoft TechNet を参照してください。

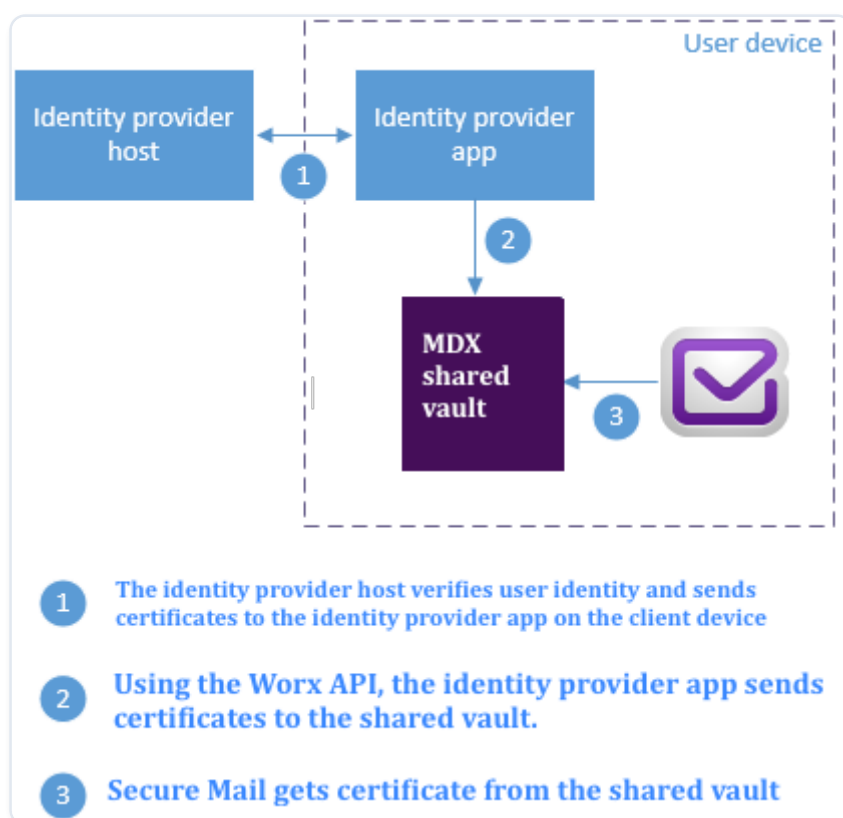
次の表では、X は Secure Mail がデバイス OS で S/MIME 機能をサポートしていることを示します。

S/MIME 機能	IOS	アンドロイド
デジタル ID プロバイダーの統合: Secure Mail をサポートされているサードパーティのデジタル ID プロバイダーと統合できます。ID プロバイダーホストは、ユーザーデバイス上の ID プロバイダーアプリに証明書を提供します。そのアプリは、機密性の高いアプリデータの安全なストレージ領域である Endpoint Management 共有ボールドに証明書を送信します。Secure Mail は共有ボールドから証明書を取得します。詳細については、「 デジタル ID プロバイダーとの統合 」セクションを参照してください。	X	
派生資格情報のサポート	Secure Mail は、証明書ソースとして派生資格情報の使用をサポートしています。派生資格情報の詳細については、Citrix Endpoint Management ドキュメントの「 iOS 用派生資格情報 」の記事を参照してください。	
メールによる証明書の配布: メールで証明書を配布するには、証明書テンプレートを作成し、そのテンプレートを使用してユーザー証明書を要求する必要があります。証明書をインストールして検証した後、ユーザー証明書をエクスポートし、ユーザーにメールで送信します。ユーザーは Secure Mail でメールを開き、証明書をインポートします。詳細については、「 メー	X	X

S/MIME 機能	IOS	アンドロイド
ルによる証明書の配布」セクションを参照してください。		
単一目的証明書の自動インポート: Secure Mail は、証明書が署名または暗号化のみに使用されるかどうかを検出し、証明書を自動的にインポートしてユーザーに通知します。証明書が両方の目的で使用される場合、ユーザーはインポートを求められます。	X	

デジタルIDプロバイダーとの統合

次の図は、デジタルIDプロバイダーホストからSecure Mailへの証明書のパスを示しています。これは、サポートされているサードパーティのデジタルIDプロバイダーとSecure Mailを統合するときに発生します。



MDX共有ボールドは、証明書などの機密性の高いアプリデータを安全に保存する領域です。Endpoint Managementによって有効化されたアプリのみが共有ボールドにアクセスできます。

前提条件

Secure MailはEntrust IdentityGuardとの統合をサポートしています。

統合の構成

1. IDプロバイダーアプリを準備し、ユーザーに提供します:

- ラップする.ipaファイルを入手するには、Entrustに連絡してください。
- MDX Toolkitを使用してアプリをラップします。

Endpoint Management環境外で既にアプリのバージョンを持っているユーザーにこのアプリを展開する場合、このアプリには一意のアプリIDを使用してください。このアプリとSecure Mailには同じプロビジョニングプロファイルを使用してください。

- Endpoint Managementにアプリを追加し、Endpoint Managementアプリストアに公開します。
- ユーザーに、Secure HubからIDプロバイダーアプリをインストールする必要があることを伝えます。必要に応じて、インストール後の手順についてガイダンスを提供します。

次の手順でSecure MailのS/MIMEポリシーをどのように構成するかによって、Secure Mailは、証明書のインストールまたはSecure Mail設定でのS/MIMEの有効化をユーザーに促す場合があります。これらの両方の手順については、[iOS版Secure MailでS/MIMEを有効にする](#)を参照してください。

2. Secure Mail を Endpoint Management に追加する際は、以下のポリシーを必ず構成してください。

- S/MIME 証明書ソースポリシーを **Shared vault** に設定します。この設定は、Secure Mail がデジタルIDプロバイダーによって共有ボールドに保存されている証明書を使用することを意味します。
- Secure Mail の初回起動時に S/MIME を有効にするには、「Enable S/MIME during first Secure Mail startup」ポリシーを構成します。このポリシーは、共有ボールドに証明書がある場合に Secure Mail が S/MIME を有効にするかどうかを決定します。証明書が利用できない場合、Secure Mail はユーザーに証明書のインポートを促します。このポリシーが有効になっていない場合、ユーザーは Secure Mail の設定で S/MIME を有効にできます。デフォルトでは、Secure Mail は S/MIME を有効にしないため、ユーザーは Secure Mail の設定を通じて S/MIME を有効にする必要があります。

派生資格情報の使用

デジタルIDプロバイダーと統合する代わりに、派生資格情報の使用を許可できます。

Secure Mail を Endpoint Management に追加する際は、S/MIME 証明書ソースポリシーを **Derived Credentials** に構成します。派生資格情報の詳細については、「[iOS 用派生資格情報](#)」を参照してください。

メールによる証明書の配布

デジタルIDプロバイダーと統合したり、派生資格情報を使用したりする代わりに、メールでユーザーに証明書を配布できます。このオプションには、このセクションで詳述する以下の一般的な手順が必要です。

1. サーバーマネージャーを使用して、Microsoft Certificate Services の Web 登録を有効にし、IIS の認証設定を確認します。
2. メールメッセージの署名と暗号化のための証明書テンプレートを作成します。これらのテンプレートを使用してユーザー証明書を要求します。
3. 証明書をインストールして検証し、ユーザー証明書をエクスポートしてユーザーにメールで送信します。
4. ユーザーは Secure Mail でメールを開き、証明書をインポートします。これにより、証明書は Secure Mail のみで利用可能になります。S/MIME の iOS プロファイルには表示されません。

前提条件

このセクションの手順は、以下のコンポーネントに基づいています。

- XenMobile® Server 10 以降
- Citrix Gateway のサポート対象バージョン (旧 NetScaler® Gateway)
- Secure Mail for iOS (最小バージョン 10.8.10); Secure Mail for Android デバイス (最小バージョン 10.8.10)
- Microsoft Certificate Services がルート証明機関 (CA) として機能する Microsoft Windows Server 2008 R2 以降
- マイクロソフト エクスチェンジ:
 - Exchange Server 2016 累積更新プログラム 4
 - Exchange Server 2013 累積更新プログラム 15
 - Exchange Server 2010 SP3 更新プログラムのロールアップ 16

S/MIME を構成する前に、以下の前提条件を完了してください:

- ルート証明書と中間証明書を、手動で、または Endpoint Management の資格情報デバイスポリシーを介して、モバイルデバイスに配信します。詳細については、「[資格情報デバイスポリシー](#)」を参照してください。
- Exchange Server への ActiveSync トラフィックを保護するためにプライベートサーバー証明書を使用している場合は、すべてのルート証明書と中間証明書をモバイルデバイスにインストールしてください。

Microsoft Certificate Services の Web 登録を有効にする

1. 管理ツールに移動し、サーバーマネージャーを選択します。
2. **Active Directory 証明書サービス**の下で、**証明機関 Web 登録**がインストールされているかどうかを確認します。
3. 必要に応じて、**役割サービスの追加**を選択して証明機関 Web 登録をインストールします。
4. **証明機関 Web 登録**をチェックし、次へをクリックします。
5. インストールが完了したら、**閉じる**または**完了**をクリックします。

IIS で認証設定を確認する

- ユーザー証明書を要求するために使用される Web 登録サイト（例: `https://ad.domain.com/certsrv/`）が、HTTPS サーバー証明書（プライベートまたはパブリック）で保護されていることを確認します。
 - Web 登録サイトは HTTPS 経由でアクセスする必要があります。
1. 管理ツールに移動し、サーバーマネージャーを選択します。
 2. **Web サーバー (IIS)** で、**役割サービス**の下を確認します。クライアント証明書マッピング認証と IIS クライアント証明書マッピング認証がインストールされていることを確認します。インストールされていない場合は、これらの役割サービスをインストールします。
 3. 管理ツールに移動し、**インターネットインフォメーションサービス (IIS) マネージャー**を選択します。
 4. **IIS マネージャー**ウィンドウの左ペインで、Web 登録用の IIS インスタンスを実行しているサーバーを選択します。
 5. **認証**をクリックします。
 6. **Active Directory クライアント証明書認証**が有効になっていることを確認します。
 7. 右ペインで、**サイト > Microsoft Internet Information Services** の既定の**サイト > バインド**をクリックします。
 8. HTTPS バインドが存在しない場合は、追加します。

9. 既定の Web サイトのホームに移動します。
10. **SSL 設定**をクリックし、**クライアント証明書を受け入れる**をクリックします。

新しい証明書テンプレートを作成する

メールメッセージに署名して暗号化するには、CitrixはMicrosoft Active Directory証明書サービスで証明書を作成することをお勧めします。両方の目的で同じ証明書を使用し、暗号化証明書をアーカイブした場合、署名証明書を回復してなりすましを許可することが可能です。

以下の手順で、証明機関 (CA) サーバー上の証明書テンプレートを複製します。

- Exchange署名のみ（署名用）
 - Exchangeユーザー（暗号化用）
1. 証明機関スナップインを開きます。
 2. CAを展開し、**証明書テンプレート**に移動します。
 3. 右クリックして**管理**をクリックします。
 4. Exchange署名のみテンプレートを検索し、テンプレートを右クリックして**テンプレートの複製**をクリックします。

Exchange署名のみテンプレートの画像(/en-us/mobile-productivity-apps/media/smime-3.png)

5. 任意の名前を割り当てます。
6. **Active Directory**に証明書を発行するチェックボックスを選択します。

注：

Active Directoryに証明書を発行するチェックボックスを選択しない場合、ユーザーはユーザー証明書（署名用および暗号化用）を手動で発行する必要があります。これは、**Outlookメールクライアント > トラストセンター > 電子メールセキュリティ > GALに発行（グローバルアドレスリスト）**から実行できます。

Active Directoryに証明書を発行するチェックボックスの画像(/en-us/mobile-productivity-apps/media/smime-4.png)

7. **要求処理**タブをクリックし、次のパラメーターを設定します。
 - 目的: 署名
 - 最小キーサイズ: 2048
 - 秘密キーのエクスポートを許可するチェックボックス: オン

- ユーザー入力なしでサブジェクトを登録するチェックボックス: オン

リクエスト処理タブの画像(/en-us/mobile-productivity-apps/media/smime-5.png)

8. セキュリティタブをクリックし、グループ名またはユーザー名の下で、**認証済みユーザー**（または任意のドメインセキュリティグループ）が追加されていることを確認します。また、**認証済みユーザーのアクセス許可**の下で、許可に対して読み取りと登録のチェックボックスがオンになっていることを確認します。

セキュリティタブの画像(/en-us/mobile-productivity-apps/media/smime-6.png)

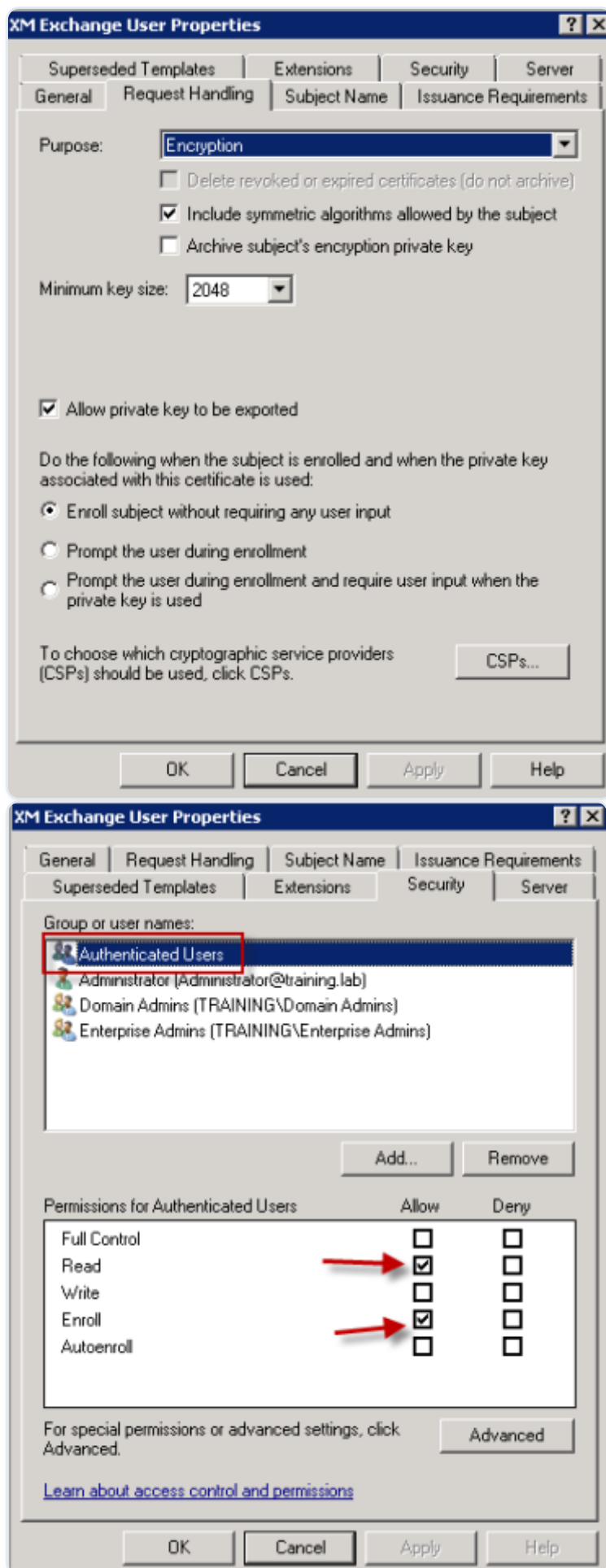
9. その他のすべてのタブと設定については、デフォルト設定のままにします。
10. **証明書テンプレート**で、**Exchangeユーザー**をクリックし、手順4から9を繰り返します。

証明書テンプレートダイアログボックスの画像(/en-us/mobile-productivity-apps/media/smime-7.png)

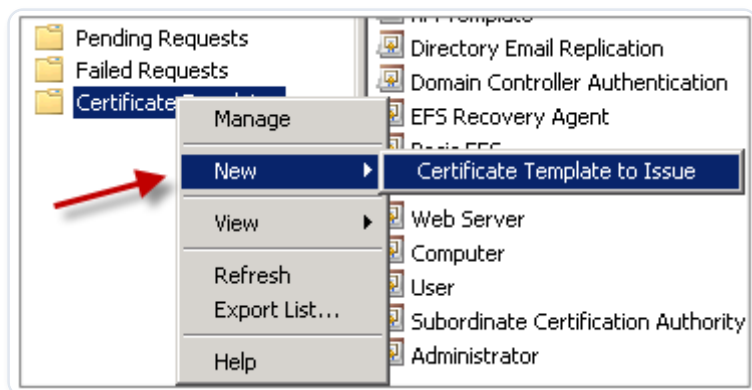
新しいExchangeユーザーテンプレートには、元のテンプレートと同じデフォルト設定を使用します。

11. **リクエスト処理**タブをクリックし、次のパラメーターを設定します。

- 目的: 暗号化
- 最小キーサイズ: 2048
- 秘密キーのエクスポートを許可するチェックボックス: オン
- ユーザー入力なしでサブジェクトを登録するチェックボックス: 選択済み



12. 両方のテンプレートが作成されたら、両方の証明書テンプレートを発行してください。新規をクリックし、発行する証明書テンプレートをクリックします。



ユーザー証明書の要求

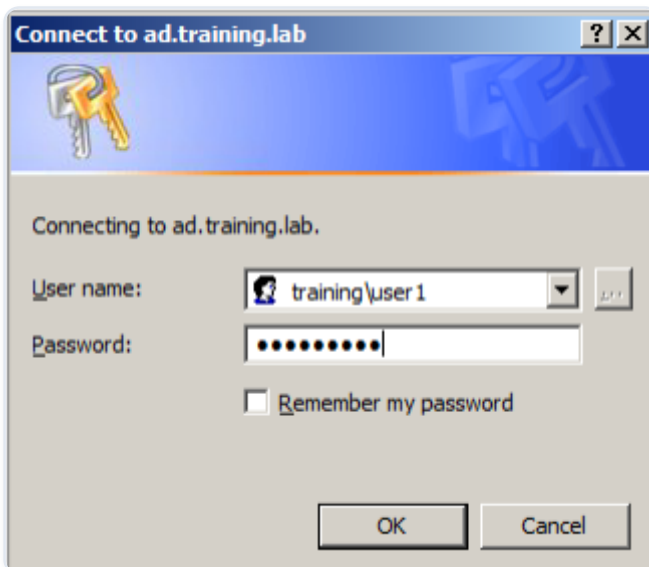
この手順では、「user1」を使用してWeb登録ページに移動します（例: <https://ad.domain.com/certsrv/>）。この手順では、セキュアメール用の新しいユーザー証明書を2つ要求します。1つは署名用、もう1つは暗号化用です。Secure Mailを介してS/MIMEの使用を必要とする他のドメインユーザーに対しても、同じ手順を繰り返すことができます。

署名および暗号化用のユーザー証明書を生成するために、Microsoft Certificate ServicesのWeb登録サイト（例: <https://ad.domain.com/certsrv/>）を介して手動登録が使用されます。代替案として、この機能を使用するユーザーグループに対してグループポリシーを介して自動登録を構成することもできます。

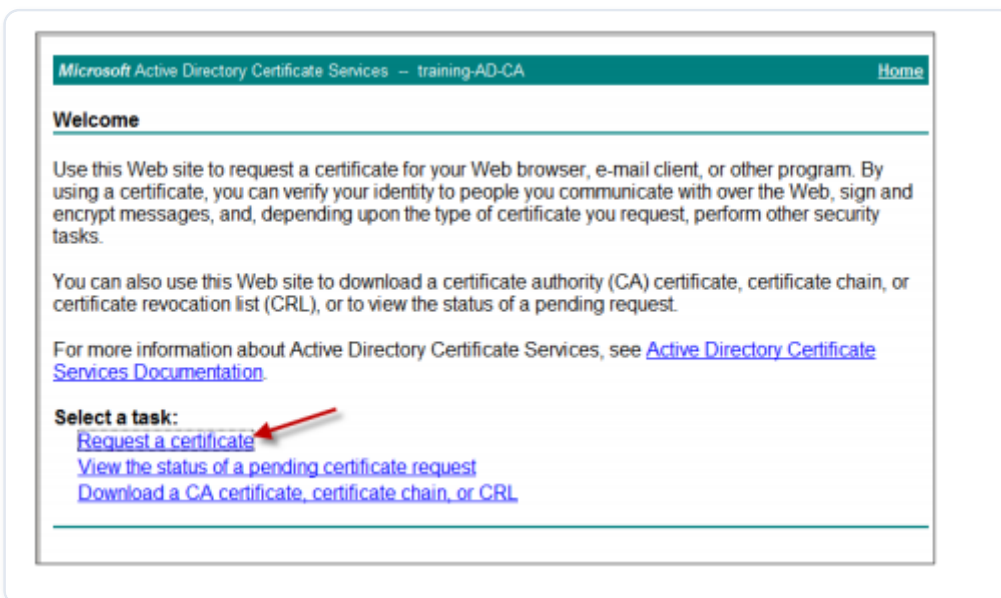
1. Windowsベースのコンピュータで、Internet Explorerを開き、Web登録サイトにアクセスして新しいユーザー証明書を要求します。

注記:

証明書を要求するには、正しいドメインユーザーでログオンしていることを確認してください。



- ログインしたら、**証明書の要求**をクリックします。



- 高度な証明書要求をクリックします。
- 「このCAへの要求を作成して送信」をクリックします。
- 署名用のユーザー証明書を生成します。適切なテンプレート名を選択し、ユーザー設定を入力します。次に、「要求形式」の横で「PKCS10」を選択します。

要求が送信されました。

詳細証明書要求オプションの画像(/en-us/mobile-productivity-apps/media/smime-17.png)

- 「この証明書をインストール」をクリックします。
- 証明書が正常にインストールされたことを確認します。

インストール成功確認の画像(/en-us/mobile-productivity-apps/media/smime-19.png)

8. 同じ手順を繰り返しますが、今度は電子メールメッセージの暗号化用です。同じユーザーが Web 登録サイトにログインした状態で、ホームリンクに移動して新しい証明書を要求します。
9. 暗号化用の新しいテンプレートを選択し、手順5で入力したのと同じユーザー設定を入力します。

新しいテンプレートオプションの画像(/en-us/mobile-productivity-apps/media/smime-21.png)

10. 証明書が正常にインストールされたことを確認し、別のドメインユーザー用のユーザー証明書のペアを生成するために同じ手順を繰り返します。この例では、同じ手順に従って「User2」用の証明書のペアを生成します。

注:

この手順では、同じ Windows ベースのコンピューターを使用して、「User2」用の2番目の証明書のペアを要求します。

発行済み証明書の検証

1. 証明書がドメインユーザープロファイルに適切にインストールされていることを確認するには、「**Active Directory ユーザーとコンピューター > 表示 > 拡張機能**」に移動します。

Advanced Features オプションの画像(/en-us/mobile-productivity-apps/media/smime-22.png)

2. ユーザーのプロパティ (この例では User1) に移動し、**公開済み証明書** タブをクリックします。両方の証明書が利用可能であることを確認します。また、各証明書に特定の用途があることを確認することもできます。

公開済み証明書タブの画像(/en-us/mobile-productivity-apps/media/smime-23.png)

この図は、メールメッセージを暗号化するための証明書を示しています。

メールメッセージを暗号化するための証明書の画像(/en-us/mobile-productivity-apps/media/smime-24.png)

この図は、メールメッセージに署名するための証明書を示しています。

メールメッセージに署名するための証明書の画像(/en-us/mobile-productivity-apps/media/smime-25.png)

正しい暗号化証明書がユーザーに割り当てられていることを確認します。この情報は、**Active Directory ユーザーとコンピューター > ユーザーのプロパティ**で確認できます。

ユーザーのプロパティの画像(/en-us/mobile-productivity-apps/media/smime-49.png)

Secure Mailは、LDAPクエリを介してuserCertificateユーザーオブジェクト属性をチェックすることで機能します。この値は、**属性エディター**タブで読み取ることができます。このフィールドが空であるか、暗号化用のユーザー証明書が正しくない場合、Secure Mailはメッセージを暗号化 (または復号化) できません。

属性エディタータブの画像(/en-us/mobile-productivity-apps/media/smime-50.png)

ユーザー証明書のエクスポート

この手順では、「User1」と「User2」の両方のペア証明書を秘密鍵とともに.PFX (PKCS#12) 形式でエクスポートします。エクスポートされた証明書は、Outlook Web Access (OWA) を使用してメールでユーザーに送信されます。

1. MMCコンソールを開き、**証明書 - 現在のユーザー**のスナップインに移動します。「User1」と「User2」の両方のペア証明書が表示されます。

現在のユーザー証明書の画像(/en-us/mobile-productivity-apps/media/smime-26.png)

2. 証明書を右クリックし、**すべてのタスク > エクスポート**をクリックします。
3. **はい、秘密キーをエクスポートします。**を選択して秘密キーをエクスポートします。
4. **可能であれば、証明のパスにあるすべての証明書を含めるとすべての拡張プロパティをエクスポートする**チェックボックスをオンにします。

個人情報交換オプションの画像(/en-us/mobile-productivity-apps/media/smime-29.png)

5. 最初の証明書をエクスポートしたら、ユーザーの残りの証明書についても同じ手順を繰り返します。

注：

どの証明書が署名証明書で、どの証明書が暗号化証明書であることを明確にラベル付けします。この例では、証明書はuserX-sign.pfxおよびuserX-enc.pfxとラベル付けされています。

証明書ラベルの画像(/en-us/mobile-productivity-apps/media/smime-30.png)

メールで証明書を送信する

すべての証明書がPFX形式でエクスポートされたら、Outlook Web Access (OWA) を使用してメールで送信できます。この例のログオン名はUser1で、送信されたメールには両方の証明書が含まれています。

証明書を送信するためのOWAメールの画像(/en-us/mobile-productivity-apps/media/smime-31.png)

User2またはドメイン内の他のユーザーについても同じ手順を繰り返します。

iOSおよびAndroid版Secure MailでS/MIMEを有効にする

メールが配信されたら、次のステップはSecure Mailを使用してメッセージを開き、署名と暗号化に適した証明書でS/MIMEを有効にすることです。

個別の署名証明書と暗号化証明書でS/MIMEを有効にするには

1. セキュアメールを開き、S/MIME証明書を含むメールに移動します。
2. 署名証明書をタップしてダウンロードおよびインポートします。
3. 署名証明書がサーバーからエクスポートされたときに秘密鍵に割り当てられたパスワードを入力します。

秘密鍵のパスワードオプションの画像(/en-us/mobile-productivity-apps/media/smime-34.png)

証明書がインポートされました。

4. **署名をオンにする**をタップします。

署名用の証明書をインポートするオプションの画像(/en-us/mobile-productivity-apps/media/smime-32.png)

5. または、**設定 > S/MIME**に移動し、S/MIMEをタップして署名証明書をオンにすることもできます。

S/MIME設定用の証明書をインポートする画像(/en-us/mobile-productivity-apps/media/smime-33.png)

6. **署名画面**で、正しい署名証明書がインポートされていることを確認します。

署名証明書の確認の画像(/en-us/mobile-productivity-apps/media/smime-37.png)

7. メールに戻り、暗号化証明書をタップしてダウンロードおよびインポートします。

暗号化用の証明書をインポートするオプションの画像(/en-us/mobile-productivity-apps/media/smime-38.png)

8. 暗号化証明書がサーバーからエクスポートされたときに秘密鍵に割り当てられたパスワードを入力します。

パスワードプロンプトの画像(/en-us/mobile-productivity-apps/media/smime-39.png)

証明書がインポートされました。

9. 暗号化をオンにするをタップします

暗号化をオンにするための証明書をインポートする画像(/en-us/mobile-productivity-apps/media/smime-40.png)

10. または、**設定 > S/MIME**に移動し、S/MIMEをタップして**デフォルトで暗号化**を有効にすることもできます。

署名オプションの証明書をインポートする画像(/en-us/mobile-productivity-apps/media/smime-41.png)

11. **暗号化**画面で、正しい暗号化証明書がインポートされていることを確認します。

署名証明書の確認画像(/en-us/mobile-productivity-apps/media/smime-42.png)

注：

- a. S/MIMEでデジタル署名され、添付ファイルがあり、受信者がS/MIMEを有効にしていない場合、添付ファイルは受信されません。この動作はActive Syncの制限です。S/MIMEメッセージを効果的に受信するには、Secure Mailの設定でS/MIMEをオンにしてください。
- b. **デフォルトで暗号化**オプションを使用すると、メールを暗号化するために必要な手順を最小限に抑えることができます。この機能がオンの場合、メール作成中は暗号化された状態になります。この機能がオフの場合、メール作成中は暗号化されていない状態になり、暗号化するには**ロック**アイコンをタップする必要があります。

暗号化されていないメールの画像(/en-us/mobile-productivity-apps/media/smime-004.png)

単一の署名および暗号化証明書でS/MIMEを有効にするには

1. セキュアメールを開き、S/MIME証明書を含むメールに移動します。

S/MIME証明書の画像(/en-us/mobile-productivity-apps/media/smime-001.png)

2. S/MIME証明書をタップしてダウンロードおよびインポートします。
3. サーバーから証明書をエクスポートしたときに秘密鍵に割り当てられたパスワードを入力します。

S/MIME証明書パスワードの画像(/en-us/mobile-productivity-apps/media/smime-002.png)

4. 表示される証明書オプションから、署名証明書または暗号化証明書をインポートするための適切なオプションをタップします。証明書の詳細を表示するには、**証明書を開く**をタップします。

S/MIME証明書のインポートオプションの画像(/en-us/mobile-productivity-apps/media/smime-003.png)

証明書がインポートされました。

インポートされた証明書は、**設定 > S/MIME** に移動して表示できます。

iOSおよびAndroidでのS/MIMEのテスト

前のセクションに記載されている手順を実行すると、受信者は署名および暗号化されたメールを読み取ることができます。

次の画像は、受信者が読み取った暗号化されたメッセージの例を示しています。

暗号化されたメッセージの画像(/en-us/mobile-productivity-apps/media/smime-46.png)

次の画像は、署名された信頼済み証明書の検証の例を示しています。

検証済みの署名済み証明書の画像(/en-us/mobile-productivity-apps/media/smime-47.png)

Secure Mailは、受信者の公開暗号化証明書についてActive Directoryドメインを検索します。ユーザーが有効な公開暗号化キーを持たない受信者に暗号化されたメッセージを送信した場合、そのメッセージは暗号化されずに送信されます。グループメッセージの場合、1人の受信者でも有効なキーを持っていないと、メッセージはすべての受信者に暗号化されずに送信されます。

暗号化されていないメールの画像(/en-us/mobile-productivity-apps/media/WorxMail-SMIME-not-encrypted.png)

公開証明書ソースの構成

S/MIME公開証明書を使用するには、S/MIME公開証明書ソース、LDAPサーバーアドレス、LDAPベースDN、およびLDAP匿名アクセス ポリシーを構成します。

アプリポリシーに加えて、以下を実行します。

- LDAPサーバーが公開されている場合は、トラフィックがLDAPサーバーに直接送信されるようにします。そのためには、Secure Mailのネットワークポリシーを**内部ネットワークにトンネル接続**するように構成し、Citrix ADCの分割DNSを構成します。
- LDAPサーバーが内部ネットワーク上にある場合は、以下を実行します。

- iOSの場合、バックグラウンドネットワークサービスゲートウェイポリシーを構成しないようにしてください。ポリシーを構成した場合、ユーザーは頻繁に認証プロンプトを受け取ります。
- Androidの場合、バックグラウンドネットワークサービスゲートウェイポリシーのリストに **LDAPサーバーURL**を追加するようにしてください。

セキュアメール向けシングルサインオン

Endpoint Management を構成して、ユーザーが Secure Hub に登録する際に Secure Mail に自動的に登録できるようにすることができます。ユーザーは Secure Mail に登録するために、追加情報を入力したり、追加の手順を実行したりする必要はありません。メール資格情報を使用して Secure Hub に登録するユーザーの場合、この機能には自動検出が有効になっている必要があります。自動検出が有効になっていない場合、以下の登録方法でこの機能を有効にできます。

- Endpoint Management アドレスは Secure Hub から Secure Mail に渡されます。
- ユーザーは Secure Hub に登録する際に Endpoint Management アドレスを入力します。

Secure Mail での自動登録を有効にするには

1. Endpoint Management クライアントプロパティで、**設定**ページに移動し、次の操作を行います。

- a. 次の値を **true** に設定します。

- `ENABLE_PASSCODE_AUTH`
- `ENABLE_PASSWORD_CACHING`
- `ENABLE_CREDENTIAL_STORE`

- b. この構成を追加します。

- **表示名:** `SEND_LDAP_ATTRIBUTES`
- **値:** `userPrincipalName=${user.userprincipalname},sAMAccountName=${user.samaccountname}, displayName= ${ user.displayName} ,mail= ${ user.mail}`

2. **設定**ページで、この構成をサーバープロパティに追加します。

`MAM_MACRO_SUPPORT` を **true** に設定します

3. 以下の Secure Mail プロパティを構成します。

- 初期認証メカニズムをユーザーのメールアドレスに設定します。

- 初期認証資格情報を**userPrincipalName**に設定します。
4. ユーザーのExchange Serverメールボックスに対して、メールベースのAutoDiscovery Serviceを構成します。サポートについては、Microsoft Exchange管理者にお問い合わせください。この記事では、DNSでSRVレコードを照会してAutodiscovery Serviceを構成することを前提としています。

Secure Mailアプリポリシーを構成するには

Secure MailアプリをEndpoint Managementにアップロードします。Secure Mailアプリの正しいバージョンに関連付けられた.mdxファイルをアップロードします。次に、以下のSecure Mailアプリ設定を構成します。

1. 「初期認証メカニズム」で、**ユーザーのメールアドレス**をクリックします。
2. **初期認証資格情報**で、**userPrincipalName**または**sAMAccountName**をクリックします。選択は、ユーザーのExchangeメールサーバーに対して構成されている認証タイプに基づきます。
3. Secure Mail Exchange ServerおよびSecure Mailユーザーのドメインフィールドは空のままにします。
4. Secure Mailアプリのその他のポリシーを必要に応じて構成し、必要なデリバリーグループの割り当てを行います。

自動プロビジョニングによるエンドツーエンドのSecure Mail SSOユーザーエクスペリエンス

以下の前提条件を満たしていることを確認してください。

1. Apple App Store (iOS) またはGoogle Play Store (Android) からSecure Hubをインストールします。
2. Secure Hubを開き、Endpoint Managementに登録するためのメールアドレスとパスワードを入力します。
3. Apple App Store (iOS) またはGoogle Play Store (Android) からSecure Mailをインストールします。
4. Secure Mailを開き、**OK**をタップします。この手順により、Secure HubがSecure Mailを管理できるようになります。Secure Mailは開くと自動的に構成されます。

ユーザーのメールボックスデータベースに対応するExchange Serverは、構成したAutodiscovery Serviceから取得されます。DNS SRVレコードクエリは、Secure Hubから取得されたユーザーのメールアドレスを使用します。

メールアドレス、userPrincipalName/sAMAccountName、パスワードなど、アカウント構成に必要なすべての詳細はSecure Hubから取得されます。

アカウントが構成されると、ユーザーはデバイスで**Secure Mail > 設定 > アカウント**から詳細を表示できます。

問題のトラブルシューティング

SSO構成で問題が発生した場合は、次の手順を試すことができます。

1. XenMobile Serverのバージョンが10.5以降であることを確認します。
2. Endpoint ManagementがAutoDiscovery Service用に構成されており、ユーザー登録がメールアドレスで使用するよう構成されていることを確認します。
3. Exchange Serverドメインが自動検出で構成されていることを確認します。SRVレコードのクエリがActiveSyncメールクライアントの予期されるメールサーバーの詳細を返すことを確認します。
4. この機能に問題がある場合は、次の情報を収集し、Citrixテクニカルサポートにお問い合わせください。
 - Endpoint Management診断ログをダウンロードします。
 - 最高ログレベルでSecure Mail診断ログを収集します。
 - Autodiscovery ServiceをホストしているExchange ServerのディレクトリC:
\\inetpub\\logs\\LogFiles\\W3SVC1からIISログを収集します。Microsoft Autodiscovery Serviceの詳細については、「[Exchange ServerのAutodiscoverサービス](#)」を参照してください。

セキュリティに関する考慮事項

この記事では、Secure Mail のセキュリティに関する考慮事項と、データセキュリティの強化に役立つ特定の有効化可能な設定について説明します。

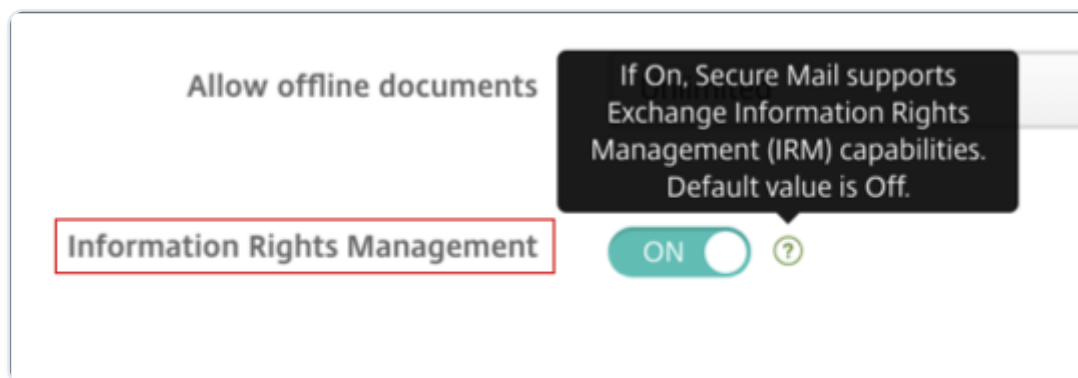
Microsoft IRM および AIP メール権限保護のサポート

Android および iOS 用 Secure Mail は、Microsoft Information Rights Management (IRM) および Azure Information Protection (AIP) ソリューションで保護されたメッセージをサポートしています。このサポートは、Citrix Endpoint Management で構成されている IRM ポリシーに準拠します。

この機能により、IRM を使用する組織はメッセージングコンテンツに保護を適用できます。また、モバイルデバイスユーザーは、権限保護されたコンテンツを作成および利用できるようになります。デフォルトでは、IRM サポートはオフです。IRM サポートを有効にするには、情報権限管理ポリシーをオンに設定します。

Secure Mail で情報権限管理を有効にするには

1. Endpoint Management にログオンし、**Configure > Apps** の順に移動して、**Add** をクリックします。
2. **Add App** 画面で、**MDX** をクリックします。
3. **App Information** 画面で、アプリの詳細を入力し、**Next** をクリックします。
4. デバイスの OS に基づいて、.mdx ファイルを選択してアップロードします。
5. **App Settings** で情報権限管理を有効にします。

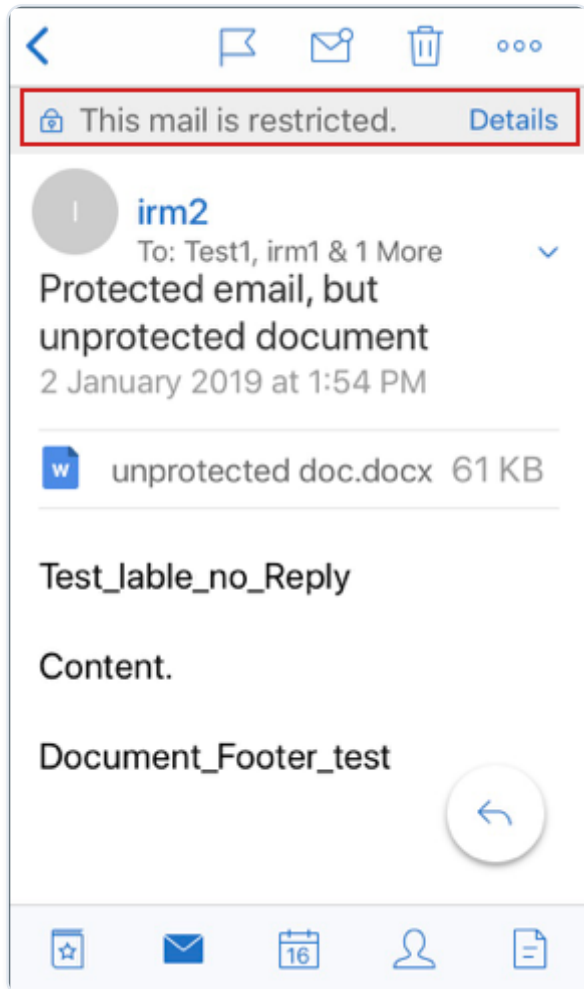


注：

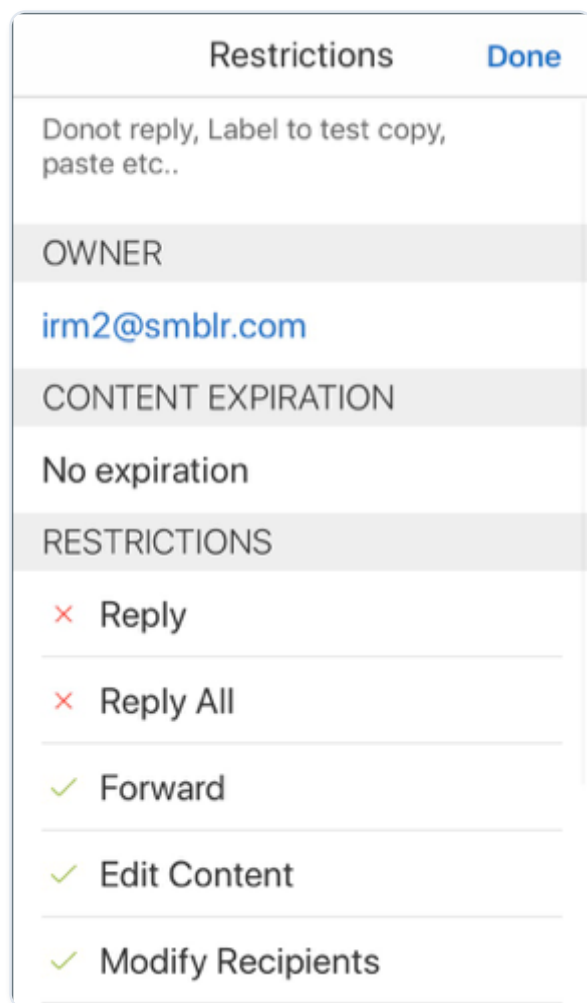
iOS と Android の両方で情報権限管理を有効にします。

権限保護されたメールを受信した場合

ユーザーが保護されたコンテンツを含むメールを受信すると、次の画面が表示されます。



ユーザーに付与されている権限の詳細を表示するには、**詳細**をタップします。



権限保護されたメールを作成する場合

ユーザーがメールを作成する際、メール保護を有効にするために制限プロファイルを設定できます。

メールに制限を設定するには：

1. Secure Mailにログインし、**作成**アイコンをタップします。
2. 作成画面で、**メール制限**アイコンをタップします。

Secure Mail のメール作成(/en-us/mobile-productivity-apps/media/IRM-Compose-email.png)

3. **制限プロファイル**画面で、メールに適用する制限をタップし、戻るをクリックします。

Secure Mail の制限プロファイル(/en-us/mobile-productivity-apps/media/irm-restriction-profiles.png)

適用された制限は、件名フィールドの下に表示されます。

Secure Mail の適用された制限(/en-us/mobile-productivity-apps/media/irm-applied-restrictions.png)

一部の組織では、IRMポリシーの厳格な順守を求める場合があります。Secure Mailにアクセスできるユーザーは、Secure Mail、オペレーティングシステム、またはハードウェアプラットフォームを改ざんしてIRMポリシーをバイパスしようとする可能性があります。

Endpoint Managementは特定の攻撃を検出できますが、セキュリティを強化するために次の予防措置を検討してください。

- デバイスベンダーが提供するセキュリティガイダンスを確認してください。
- Endpoint Managementの機能を使用するか、その他の方法で、デバイスを適切に構成します。
- IRM機能（Secure Mailを含む）の適切な使用法について、ユーザーにガイダンスを提供します。
- この種の攻撃に対抗するため、追加のサードパーティ製セキュリティソフトウェアを展開します。

メールセキュリティ分類

iOSおよびAndroid版Secure Mailは、メール分類マーキングをサポートしており、ユーザーはメール送信時にセキュリティ（SEC）および配布制限マーカー（DLM）を指定できます。SECマーキングには、Protected、Confidential、Secretが含まれます。DLMには、Sensitive、Legal、Personalが含まれます。メールを作成する際、Secure Mailユーザーは、以下の画像に示すように、メールの分類レベルを示すマーキングを選択できます。

Secure Mailのセキュリティ分類リンク(/en-us/mobile-productivity-apps/media/worx-mail-security-class-selection1.png)

Secure Mailのセキュリティ分類リスト(/en-us/mobile-productivity-apps/media/worx-mail-security-class-selection2.png)

受信者は、メールの件名で分類マーキングを表示できます。例：

- 件名：計画
- 件名：計画
- 件名：計画

メールヘッダーには、インターネットメッセージヘッダー拡張として分類マーキングが含まれており、この例では太字で示されています。

日付: Fri, 01 May 2015 12:34:50 +530

件名: 計画

優先度: 通常

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

差出人: **operations@example.com**

宛先: チーム **<mylist@example.com>**

MIME-Version: 1.0 コンテンツタイプ: **multipart/alternative;boundary="_com.example.email_6428E5E4-9DB3-4133-9F48-155913E39A980"**

Secure Mailは分類マーキングのみを表示します。アプリはこれらのマーキングに基づいてアクションを実行しません。

ユーザーが分類マーキングのあるメールに返信または転送する場合、SECおよびDLMの値は元のメールのマーキングにデフォルト設定されます。ユーザーは別のマーキングを選択できます。Secure Mailは、元のメールに関連するそのような変更を検証しません。

以下のMDXポリシーを通じて、メール分類マーキングを構成します。

- **メール分類:** オンの場合、Secure MailはSECおよびDLMのメール分類マーキングをサポートします。分類マーキングは、メールヘッダーに「X-Protective-Marking」値として表示されます。関連するメール分類ポリシーを必ず構成してください。デフォルト値は**オフ**です。
- **メール分類ネームスペース:** 使用される分類標準によってメールヘッダーで要求される分類ネームスペースを指定します。たとえば、ネームスペース「gov.au」はヘッダーに「NS=gov.au」として表示されます。デフォルト値は空です。
- **メール分類バージョン:** 使用される分類標準によってメールヘッダーで要求される分類バージョンを指定します。たとえば、バージョン「2012.3」はヘッダーに「VER=2012.3」として表示されます。デフォルト値は空です。
- **デフォルトのメール分類:** ユーザーがマーキングを選択しない場合にSecure Mailがメールに適用する保護マーキングを指定します。この値は、メール分類マーキングポリシーのリストに含まれている必要があります。デフォルト値は**UNOFFICIAL**です。
- **メール分類マーキング:** ユーザーが利用できる分類マーキングを指定します。リストが空の場合、Secure Mailは保護マーキングのリストを含みません。マーキングリストには、セミコロンで区切られた値のペアが含まれています。各ペアには、Secure Mailに表示されるリスト値と、Secure Mailのメール件名およびヘッダーに追加されるテキストであるマーキング値が含まれます。たとえば、マーキングペア「UNOFFICIAL,SEC=UNOFFICIAL;」では、リスト値は「UNOFFICIAL」で、マーキング値は「SEC=UNOFFICIAL」です。

デフォルト値は、変更可能な分類マーキングのリストです。Secure Mailには以下のマーキングが用意されています。

- UNOFFICIAL,SEC=UNOFFICIAL
- UNCLASSIFIED,SEC=UNCLASSIFIED
- 公務使用限定,DLM=For-Official-Use-Only
- センシティブ,DLM=Sensitive
- センシティブ:リーガル,DLM=Sensitive:Legal
- センシティブ:パーソナル,DLM=Sensitive:Personal
- PROTECTED,SEC=PROTECTED
- プロテクトド+センシティブ,SEC=PROTECTED
- プロテクトド+センシティブ:リーガル,SEC=PROTECTED DLM=Sensitive:Legal
- プロテクトド+センシティブ:パーソナル,SEC=PROTECTED DLM=Sensitive:Personal
- プロテクトド+センシティブ:キャビネット,SEC=PROTECTED,DLM=Sensitive:Cabinet
- CONFIDENTIAL,SEC=CONFIDENTIAL
- コンフィデンシャル+センシティブ,SEC=CONFIDENTIAL,DLM=Sensitive
- コンフィデンシャル+センシティブ:リーガル,SEC=CONFIDENTIAL DLM=Sensitive:Legal
- コンフィデンシャル+センシティブ:パーソナル
,SEC=CONFIDENTIAL,DLM=Sensitive:Personal
- コンフィデンシャル+センシティブ:キャビネット,SEC=CONFIDENTIAL
DLM=Sensitive:Cabinet
- SECRET,SEC=SECRET
- シークレット+センシティブ,SEC=SECRET,DLM=Sensitive
- シークレット+センシティブ:法務,セック=シークレット,ディーエルエム=センシティブ:法務
- シークレット+センシティブ:個人,セック=シークレット,ディーエルエム=センシティブ:個人
- シークレット+センシティブ:閣議,セック=シークレット,ディーエルエム=センシティブ:閣議
- TOP-SECRET,SEC=TOP-SECRET
- トップシークレット+センシティブ,セック=トップシークレット,ディーエルエム=センシティブ
- トップシークレット+センシティブ:法務,セック=トップシークレット ディーエルエム=センシ
ティブ:法務
- トップシークレット+センシティブ:個人,セック=トップシークレット ディーエルエム=センシ
ティブ:個人

- トップシークレット+センシティブ:閣議,セック=トップシークレット ディーエルエム=センシティブ:閣議

iOS データ保護

オーストラリア信号局 (ASD) のデータ保護要件を満たす必要がある企業は、Secure Mail および Secure Web の **iOS データ保護を有効にする** ポリシーを使用できます。デフォルトでは、これらのポリシーは **オフ** になっています。

Secure Web で **iOS データ保護を有効にする** が **オン** の場合、Secure Web はサンドボックス内のすべてのファイルにクラス A の保護レベルを使用します。Secure Mail のデータ保護の詳細については、[オーストラリア信号局のデータ保護](#) を参照してください。このポリシーを有効にすると、最高のデータ保護クラスが使用されるため、**最小データ保護クラス** ポリシーを別途指定する必要はありません。

iOS データ保護を有効にするポリシーを変更するには

1. Endpoint Management コンソールを使用して、Secure Web および Secure Mail の MDX ファイルを Endpoint Management にロードします。新しいアプリの場合は、**構成 > アプリ > 追加** に移動し、**MDX** をクリックします。アップグレードの場合は、**MDX またはエンタープライズアプリのアップグレード** を参照してください。
2. Secure Mail の場合は、**アプリ** 設定を参照し、**iOS データ保護を有効にする** ポリシーを見つけて **オン** に設定します。このポリシーが有効になっている場合でも、古いオペレーティングシステムバージョンを実行しているデバイスには影響しません。
3. Secure Web の場合は、**アプリ** 設定を参照し、**iOS データ保護を有効にするポリシー** を見つけて **オン** に設定します。このポリシーが有効になっている場合でも、古いオペレーティングシステムバージョンを実行しているデバイスには影響しません。
4. アプリポリシーを通常どおり構成し、設定を保存して、Endpoint Managementアプリストアにアプリを展開します。

オーストラリア信号局のデータ保護

Secure Mailは、オーストラリア信号局 (ASD) のコンピューターセキュリティ要件を満たす必要がある企業向けに、ASDデータ保護をサポートしています。デフォルトでは、ポリシーは**オフ**になっており、Secure MailはクラスCデータ保護を提供するか、プロビジョニングプロファイルで設定されたデータ保護を使用します。

ポリシーが**オン**の場合、Secure Mailはアプリサンドボックスでファイルを作成および開くときに保護レベルを指定します。Secure Mailは、以下の項目にクラスAデータ保護を設定します。

- 送信トレイのアイテム
- カメラまたはカメラロールからの写真
- 他のアプリから貼り付けられた画像
- ダウンロードされたファイル添付

Secure Mailは、以下の項目にクラスBデータ保護を設定します。

- 保存されたメール
- カレンダーアイテム
- 連絡先
- ActiveSyncポリシーファイル

クラスB保護により、ロックされたデバイスの同期が可能になり、ダウンロード開始後にデバイスがロックされた場合でもダウンロードが完了できるようになります。

データ保護が有効になっている場合、デバイスがロックされているとファイルを開くことができないため、キューに入っている送信トレイのアイテムは送信されません。デバイスが終了し、ロックされた状態でSecure Mailが再起動した場合、デバイスのロックが解除されSecure Mailが起動するまで、Secure Mailは同期できません。

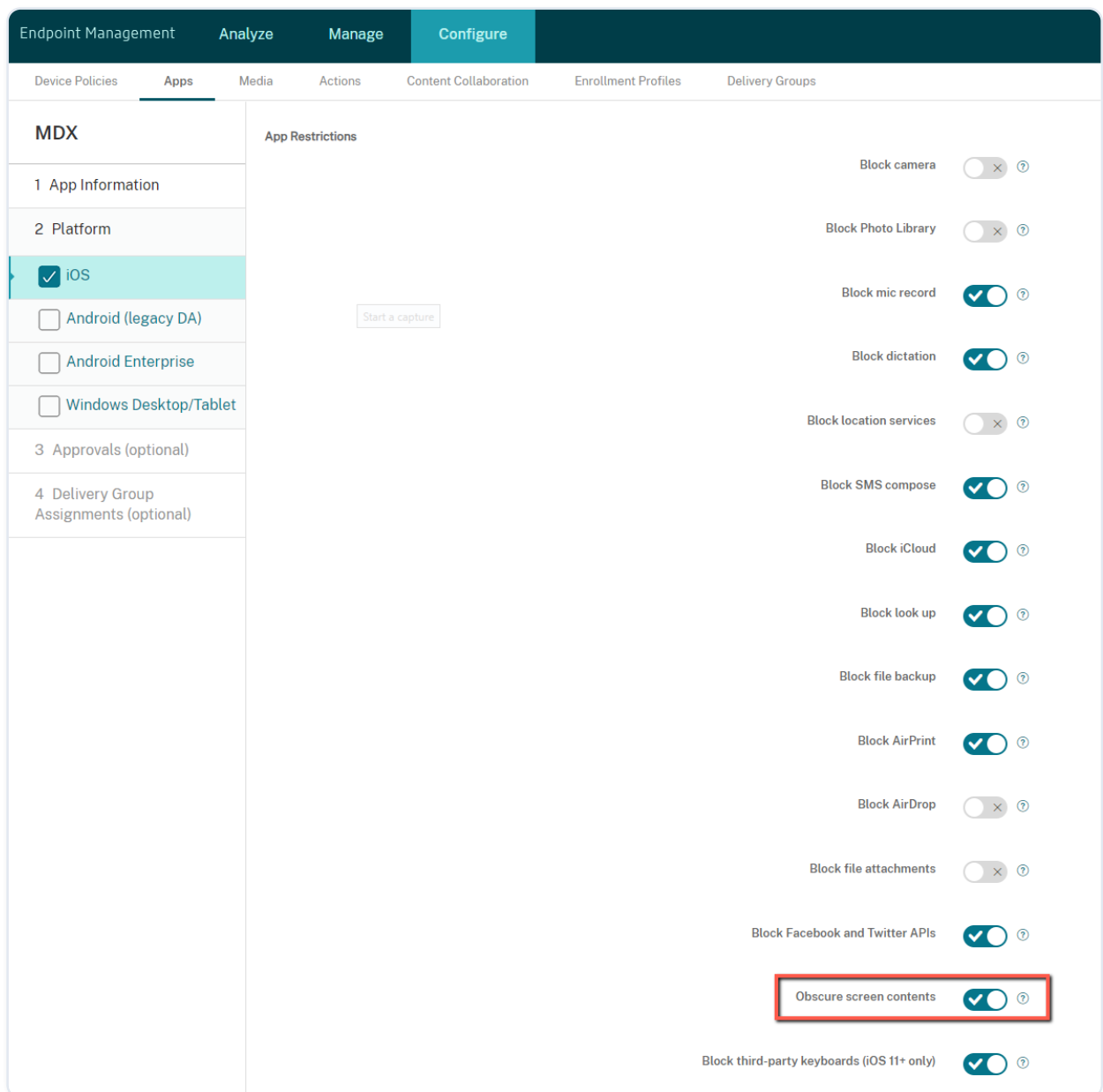
Citrix® は、このポリシーを有効にする場合、クラス C データ保護を含むログファイルの作成を避けるため、必要な場合にのみ Secure Mail のログ記録を有効にすることを推奨します。

画面コンテンツの隠蔽

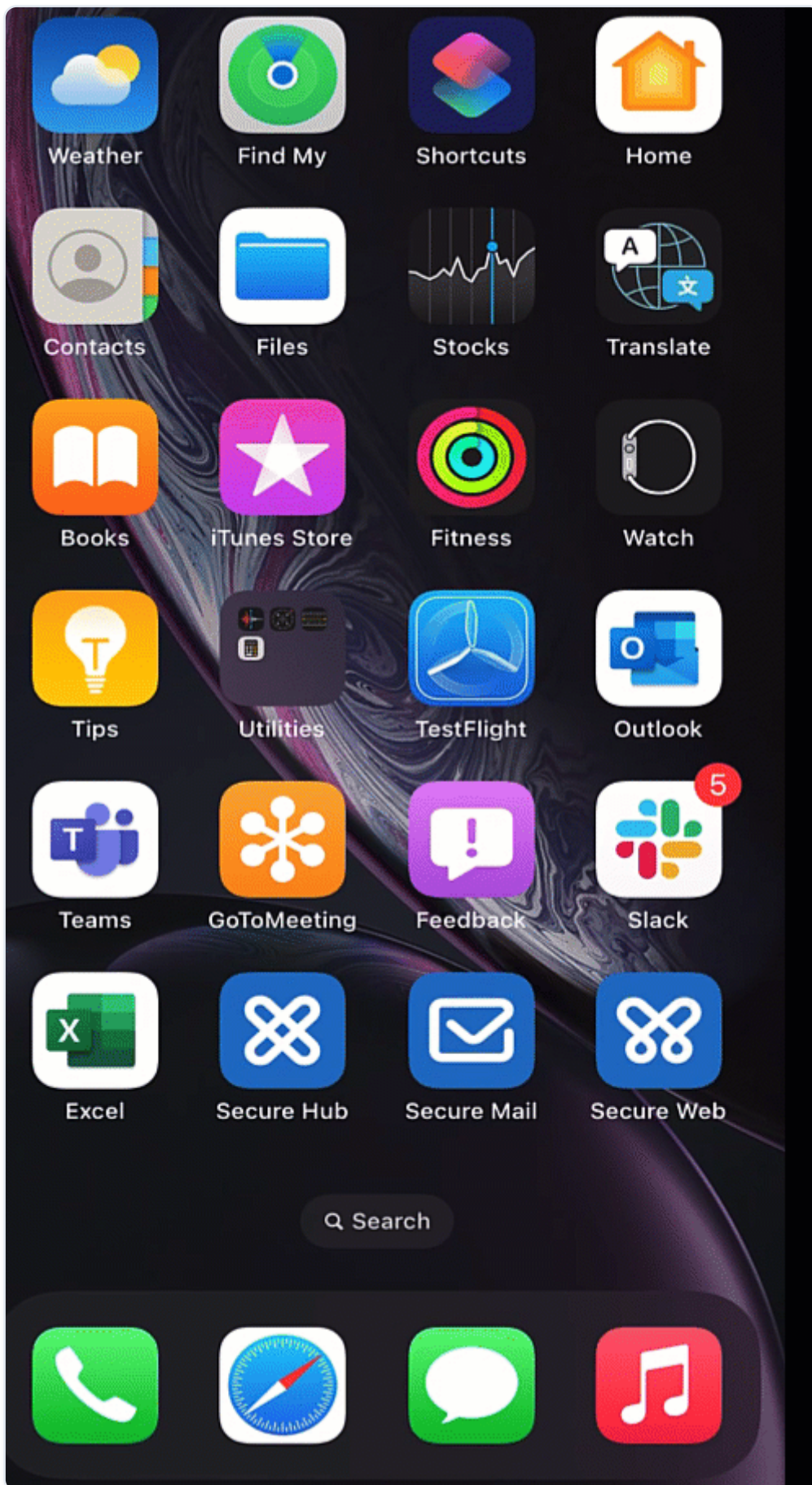
Android および iOS 版 Secure Mail は、アプリがバックグラウンドに入ったときに画面を隠蔽する機能をサポートしています。この機能は、ユーザーのプライバシーを強化し、機密データを保護し、不正アクセスを防止します。iOS または Android デバイスで Secure Mail のこの機能を有効にするには、以下のセクションを参照してください。

iOS デバイスの場合:

1. 管理者資格情報を使用して Citrix Endpoint Management コンソールにサインインします。
2. **構成 > アプリ > MDX** に移動します。
3. **プラットフォーム** セクションで **iOS** オプションを選択します。
4. **アプリの制限** セクションで **画面コンテンツの隠蔽** オプションを有効にします。



画面コンテンツの隠蔽 オプションを有効にすると、アプリがバックグラウンドに入ったときに Secure Mail はグレースクリーンを表示します。



Android デバイスの場合:

Secure Mail アプリのコンテンツを隠蔽するには、画面キャプチャを制限するために使用するポリシーである **画面キャプチャを許可** ポリシーを使用できます。このポリシーを無効にすると、アプリがバックグラウンドに入ったときにアプリのコンテンツも隠蔽されます。**画面キャプチャを許可** ポリシーを無効にする詳細については、Citrix Endpoint Management ドキュメントの [Android 設定](#) を参照してください。

iOS の機能

この記事では、Secure Mail でサポートされている iOS の機能について説明します。

Secure Mail をデフォルトのメールアプリとして設定するサポート

iOS 版 Secure Mail では、Secure Mail をデバイスのデフォルトのメールアプリとして設定できます。デフォルトとして設定すると、連絡先、Safari、またはその他のアプリでメールアドレスをタップすると、Secure Mail で新しいメッセージが開きます。この機能を有効にするには、次の手順を実行します。

- **管理者:** Secure Mail MDX ポリシーで `mailto:` スキームを許可します。
- **ユーザー:** デバイスで Secure Mail をデフォルトのメールアプリとして選択します。

mailto: スキームを許可するには:

1. Endpoint Management コンソールで、**【構成】 > 【アプリ】** の順に移動します。
2. **【Secure Mail】** を選択し、**【編集】** をクリックします。
3. iOS プラットフォームで、**【アプリの操作】** を展開し、**【アプリの URL スキーム】** に `,mailto:` を追加します。

アプリの URL スキームポリシーの画像(/en-us/mobile-productivity-apps/media/secure-mail-mailto-app-url-schemes.png)

Secure Mail をデフォルトのメールアプリとして設定するには:

1. デバイスで、iOS の **【設定】** アプリを開きます。
2. **【アプリ】 > 【デフォルトのアプリ】 > 【メール】** をタップします。
3. **【Secure Mail】** を選択します。

Secure MailカレンダーイベントでMicrosoft Teams会議を作成する

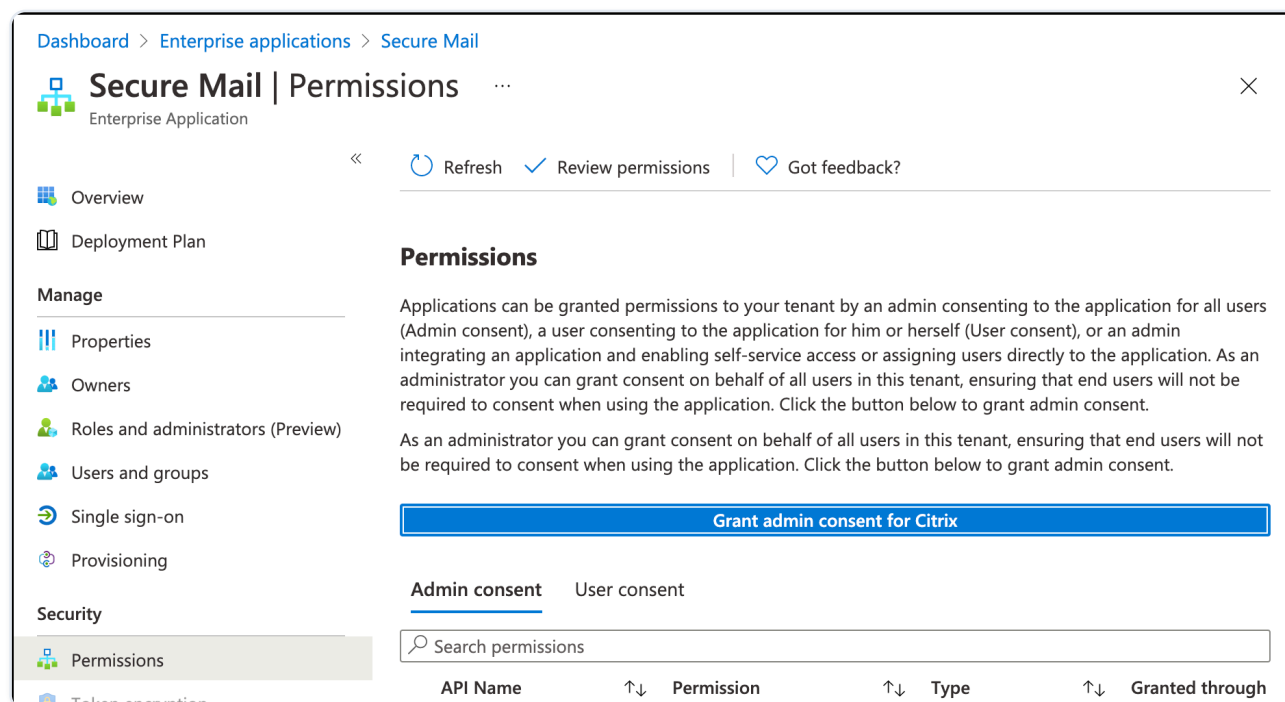
iOS版Secure Mailでは、カレンダーイベントの作成中にMicrosoft Teams会議の招待を作成できます。Microsoft Teams会議を作成するには、**Microsoft Teams会議**トグルをオンにします。会議の招待リンクと詳細は、イベントの詳細とともに自動的に送信されます。詳細については、

「Secure MailカレンダーイベントでMicrosoft Teams会議を作成する」を参照してください(/ja-jp/citrix-secure-mail/ios-features.html#create-microsoft-teams-meetings-in-secure-mail-calendar-events)

前提条件:

Azure Active Directoryのグローバル管理者が以下を実行していることを確認してください。

- 最新の認証（OAuth）を有効にし、有効なMicrosoft Teamsライセンスを持つExchange Online メールボックスユーザーであることを確認してください。
- Secure Mailアプリにテナント全体の管理者同意を提供します。
- Secure MailアプリでExchangeアカウントを設定し、すべてのユーザーがサインインできるようにアプリのアクセス許可を付与します。次の画面を参照してください。



- Microsoft Teams統合ポリシーを有効にします。

Microsoft Teams integration

ON



制限事項:

Secure Mailで作成された会議の場合、現在、この機能にはMicrosoft Outlookカレンダーで以下の制限があります。

- オンラインで参加オプションは利用できません
- 会議が開始されました通知は利用できません

下書きを最小化する

Secure Mail for iOSでは、メール作成中に下書きを最小化してアプリ内を移動できます。この機能はiOS 13以降を実行しているデバイスで利用できます。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[下書きメールを最小化する](#)」を参照してください。

MIMEヘッダーを使用したフィッシングメールの報告

Secure Mail for iOSでは、ユーザーがフィッシングメールを報告すると、そのメールに対応するEMLファイルが添付ファイルとして生成されます。管理者はこのメールを受信し、報告されたメールに関連付けられたMIMEヘッダーを表示できます。この機能を有効にするには、管理者はCitrix Endpoint Managementコンソールで「フィッシングメールアドレスの報告」ポリシーを構成し、「フィッシング報告メカニズム」を「添付ファイルによる報告」に設定する必要があります。詳細については、「[フィッシングメールを添付ファイルとして報告する](#)」を参照してください。

WkWebViewのサポート

Secure Mail for iOSはWkWebViewをサポートしています。この機能により、Secure Mailのメールとカレンダーイベントがデバイスにレンダリングされる方法が改善されます。

Slack EMMのサポート

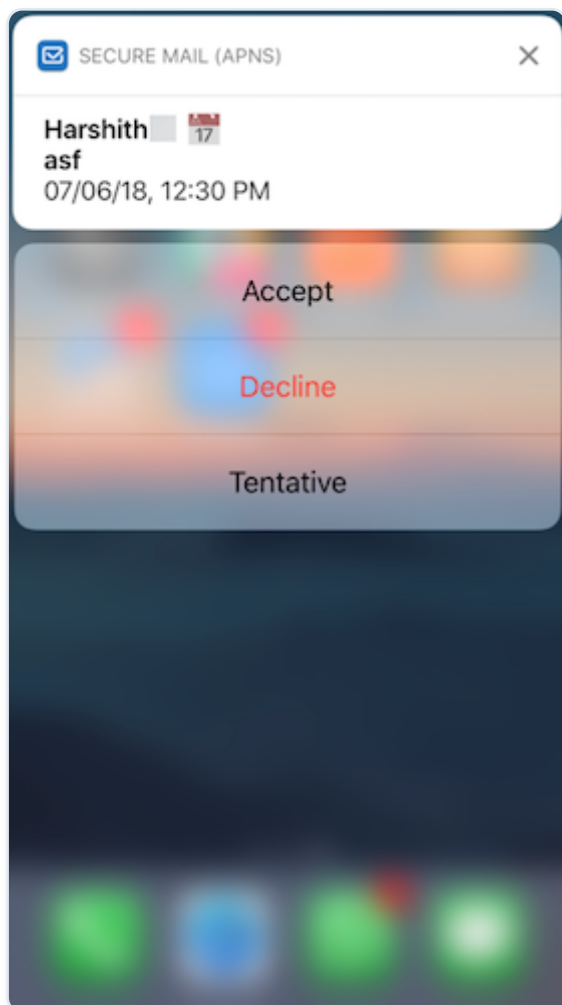
Slack EMMは、Enterprise Mobility Management (EMM) が有効になっているSlackのお客様向けです。Secure Mail for iOSは、アプリケーション**Slack EMM**をサポートしており、管理者はSecure Mailと**Slack**アプリまたは**Slack EMM**アプリのいずれかとの統合を選択できます。

グループ通知

グループ通知機能を使用すると、メールスレッド内の会話がグループ化されます。デバイスのロック画面でグループ化された通知をすばやく確認できます。グループ通知設定は、デバイスでデフォルトで有効になっています。この機能にはiOS 12が必要です。

通知応答オプション

Secure Mail for iOSでは、ユーザーは会議通知（承諾、辞退、仮承諾など）に応答できます。メッセージ通知には、返信と削除で応答できます。



リッチプッシュ通知の失敗メッセージの機能強化

Secure Mail for iOSでは、通知失敗の種類に基づいて、適切なプッシュ通知失敗メッセージがデバイスの通知センターに表示されます。詳細については、「[Secure Mail通知](#)」を参照してください。

Microsoftセットアップでのリッチプッシュ通知のサポート

iOS版Secure Mailは、最新の認証（O365）を使用するMicrosoft Enterprise Mobility + Security (EMS)/Intuneを実行しているセットアップで、リッチプッシュ通知をサポートしています。リッチプッシュ通知機能を有効にするには、以下の前提条件が満たされていることを確認してください。

- Endpoint Managementコンソールで、**プッシュ通知**をONに設定します。
- ネットワークアクセスポリシーが**無制限**に設定されていること。
- ロック画面通知の制御ポリシーが許可またはメール送信者またはイベントのタイトルに設定されていること。
- **Secure Mail > 設定 > 通知**に移動し、**メール通知**を有効にします。

派生資格情報に対するS/MIMEのサポート

iOS向けのSecure Mailは、派生資格情報のためのS/MIMEに対応しています。この機能を使うには、以下のことを行う必要があります。

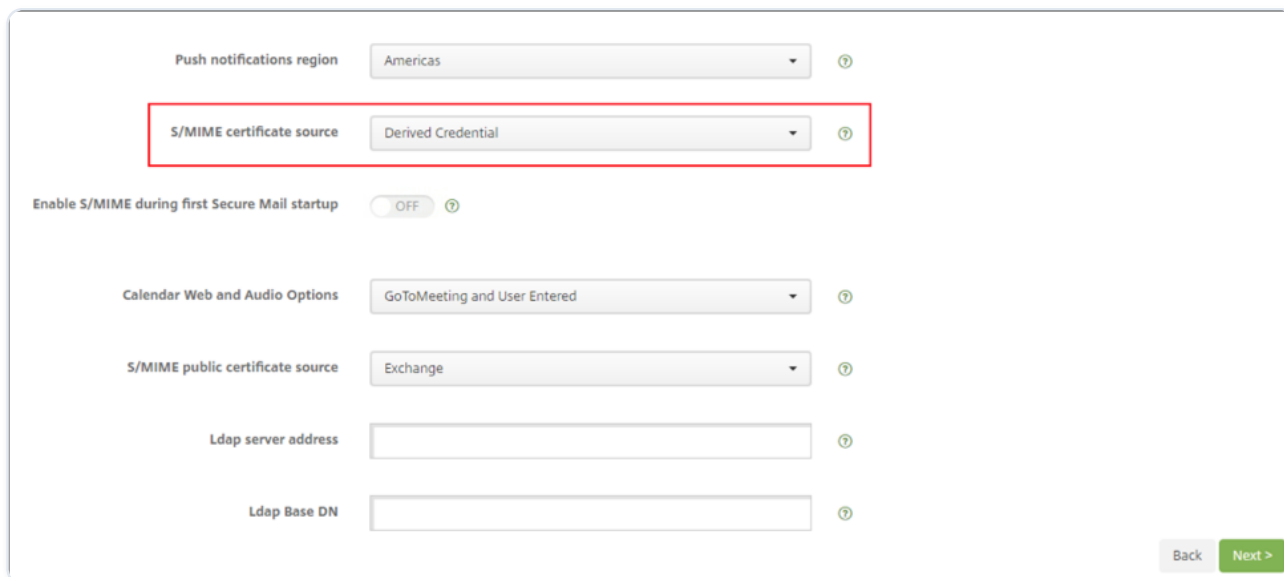
- S/MIME証明書ソースとして「派生資格情報」を選択します。詳細については、「[iOS用派生資格情報](#)」を参照してください。
- Citrix Endpoint ManagementでLDAP属性クライアントプロパティを追加します。以下の情報を使用してください。
 - **キー:** SEND_LDAP_ATTRIBUTES
 - **値:** `userPrincipalName=${user.userprincipalname}, sAMAccountName=${user.samaccountname}, displayName=${user.displayName}, mail=${user.mail}`

クライアントプロパティの追加手順については、XenMobile Serverの場合は「[クライアントプロパティ](#)」を、Endpoint Managementの場合は「[クライアントプロパティ](#)」を参照してください。

派生資格情報を使用してデバイスが登録される方法の詳細については、「[派生資格情報を使用したデバイスの登録](#)」を参照してください。

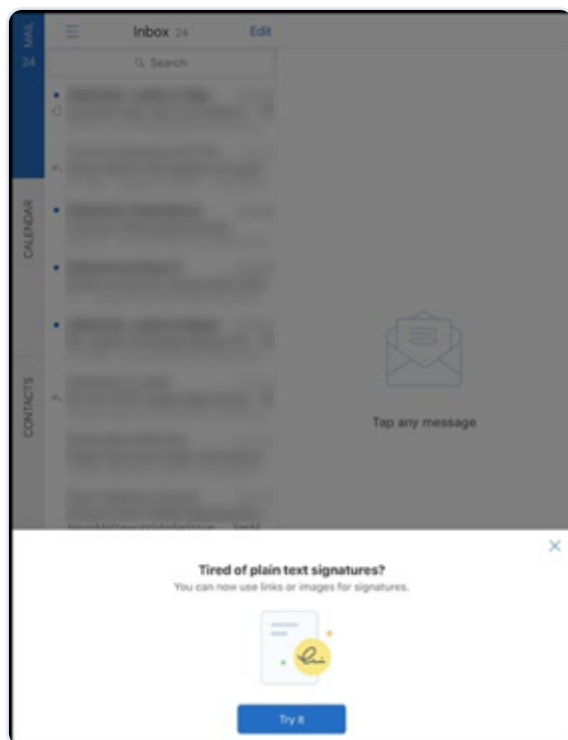
1. Endpoint Managementコンソールで、**構成 > アプリ**に移動します。

2. **Secure Mail**を選択し、**編集**をクリックします。
3. iOSプラットフォームでは、S/MIME証明書ソースとして**Derived Credential**を選択します。



リッチテキスト署名

メールの署名に画像やリンクを使用できます。署名を更新するには、署名フィールドに画像やリンクをコピー＆ペーストするだけです。



リッチテキスト署名を追加するには

1. 使用したい画像またはURLをコピーします。

2. **Secure Mail > 設定 > 署名**に移動します。
3. 画像またはURLを貼り付けます。

または、署名フィールドを長押しして**画像を挿入**をタップすると、ギャラリーから画像を選択できます。

Secure Mail発信者ID

Secure Mail for iOSでは、デバイス設定でSecure Mail発信者IDを有効にすることで、Secure Mailの連絡先からの着信を識別できます。以下の管理上の前提条件を有効にする必要があります。Citrix Endpoint Managementで、CallerIDSupportEnabled MDXポリシーが有効になっていることを確認してください。

この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[発信者IDを設定する](#)」を参照してください。

カレンダーの色を設定する

このカレンダー機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[同期されたSecure Mailカレンダーの色を設定する](#)」を参照してください。

「ファイル」アプリからファイルを添付する

Secure Mail for iOS では、iOS ネイティブのファイルアプリからファイルを添付できます。iOS のファイルアプリの詳細については、Apple の記事「[アプリ](https://support.apple.com/en-in/102570)」(https://support.apple.com/en-in/102570) を参照してください。この機能に関するユーザーヘルプドキュメントについては、Citrix ユーザーヘルプセンターの記事「[」](https://help-docs.citrix.com/ja-jp/secure-mail/attachments.html) (https://help-docs.citrix.com/ja-jp/secure-mail/attachments.html) を参照してください。

スペルチェック機能

Secure Mail のスペルチェックは、デバイスの**一般 > キーボード**にある自動大文字入力とスペルチェックの設定と、次の方法で連携します。

デバイスの自動修正	デバイスのスペルチェック	SECURE MAIL のスペルチェック	動作
オン	オン	オン	赤い下線が表示されます。タップすると、単語がピンク色

デバイスの自動修正	デバイスのスペル チェック	SECURE MAIL のス ペルチェック	動作
			で強調表示され、候補が表示されます。
オフ	オフ	オン	赤い線が表示されます。タップしても、候補は表示されません。
オン	オン	オフ	赤い下線は表示されません。タップすると、単語がピンク色で強調表示され、候補が表示されます。
オフ	オフ	オフ	赤い下線、強調表示、または候補は表示されません。
オン	オフ	オン	赤い下線が表示されます。タップすると、単語がピンク色で強調表示され、候補が表示されます。
オフ	オン	オン	赤い下線が表示されます。タップすると、単語がピンク色で強調表示され、候補が表示されます。
オン	オフ	オフ	赤い下線は表示されません。タップすると、単語がピンク色で強調表示され、候補が表示されます。
オフ	オン	オフ	赤い下線は表示されません。タップすると、単語がピンク色

デバイスの自動修正	デバイスのスペル チェック	SECURE MAIL のス ペルチェック	動作
			で強調表示され、候補が表示されます。

メールボックス画面

メールボックス画面には、設定したすべてのアカウントが表示され、次のビューがあります。

- **すべてのアカウント:** 設定したすべてのExchangeアカウントからのメールが含まれます。
- **個別のアカウント:** 個々のアカウントのメールとフォルダーが含まれます。これらのアカウントはリストとして表示され、展開してサブフォルダーを表示できます。

すべてのアカウントメールボックスは、デフォルトでグローバルビューです。このビューには、デバイスで設定したすべてのExchangeアカウントからの添付ファイルとメールが含まれます。

「**すべてのメールアカウント**」メールボックスには、次のメニュー項目があります。

- すべての添付ファイル
- 受信トレイ
 - 未読
 - フラグ付き
- 下書き
- 送信済みアイテム
- 送信トレイ
- 削除済みアイテム

「**すべてのメールアカウント**」ビューでは複数のアカウントからのメールがまとめて表示されますが、次のアクションではデフォルトまたはプライマリアカウントのメールアドレスが使用されます。

- 新規メッセージ
- 新規イベント

「**すべてのメールアカウント**」ビューから新規メールを作成中に送信者のメールアドレスを変更するには、「**差出人:**」フィールドのデフォルトアドレスをタップし、表示されるメールアカウントから別のアカウントを選択します。

注:

会話ビューからメールを作成すると、「差出人:」フィールドにその会話の宛先であるメールアドレスが自動的に入力されます。

個別アカウント

設定したすべてのアカウントは、**すべてのアカウント**の下にリストとして表示されます。デフォルトまたはプライマリアカウントが常に最初に表示され、その後に他のアカウントがアルファベット順に表示されます。

個々のアカウントには、作成したサブフォルダーが表示されます。フォルダーの横にある**V**アイコンをタップすると、サブフォルダーを表示できます。

次のアクションは、個別アカウントにのみ制限されます。

- アイテムの移動。
- 会話ビューからのメール作成。
- vCardのインポート。
- 連絡先の保存。

カレンダー

カレンダーには、デバイス上の複数のアカウントに関連するすべてのイベントが表示されます。個別のアカウントに関連するカレンダーイベントを区別するために、個別のアカウントに色を設定できます。

カレンダーイベントに色を設定するには

1. フッターバーのカレンダーアイコンをタップし、左上のハンバーガーアイコンをタップします。 **カレンダー**画面には、設定したすべてのアカウントが表示されます。
2. Exchangeアカウントの右側に表示されているデフォルトの色をタップします。「色」画面に、そのアカウントで利用可能な色が表示されます。
3. 任意の色を選択し、**保存**をタップします。
4. 前の画面に戻るには、**キャンセル**をタップします。選択した色は、そのExchangeアカウントに関連するすべてのカレンダーイベントに設定されます。

カレンダーの招待またはイベントを作成する際、**Organizer**フィールドにはデフォルトアカウントのメールアドレスが自動入力されます。メールアカウントを変更するには、このメールアドレスをタップして別のアカウントを選択します。

注:

Secure Mailを終了してから再度起動すると、アプリはデバイス上の最後に設定されたカレンダー設定を復元します。

検索

メールボックスまたは連絡先ビューからグローバル検索を実行できます。この操作により、アプリ内のすべてのアカウントを検索した後、適切な結果が表示されます。個々のアカウント内からのすべての検索では、そのアカウントにのみ関連する結果が表示されます。

iOSでメール、カレンダーイベント、またはインライン画像を印刷する

iOSデバイスからメール、カレンダーイベント、またはインライン画像を印刷できるようになりました。

前提条件

開始する前に、以下の要件が満たされていることを確認してください。

- **Block AirPrint**オプションが**OFF**に設定されていること。
- IRMで**Allow viewers to print**オプションが無効になっていること。

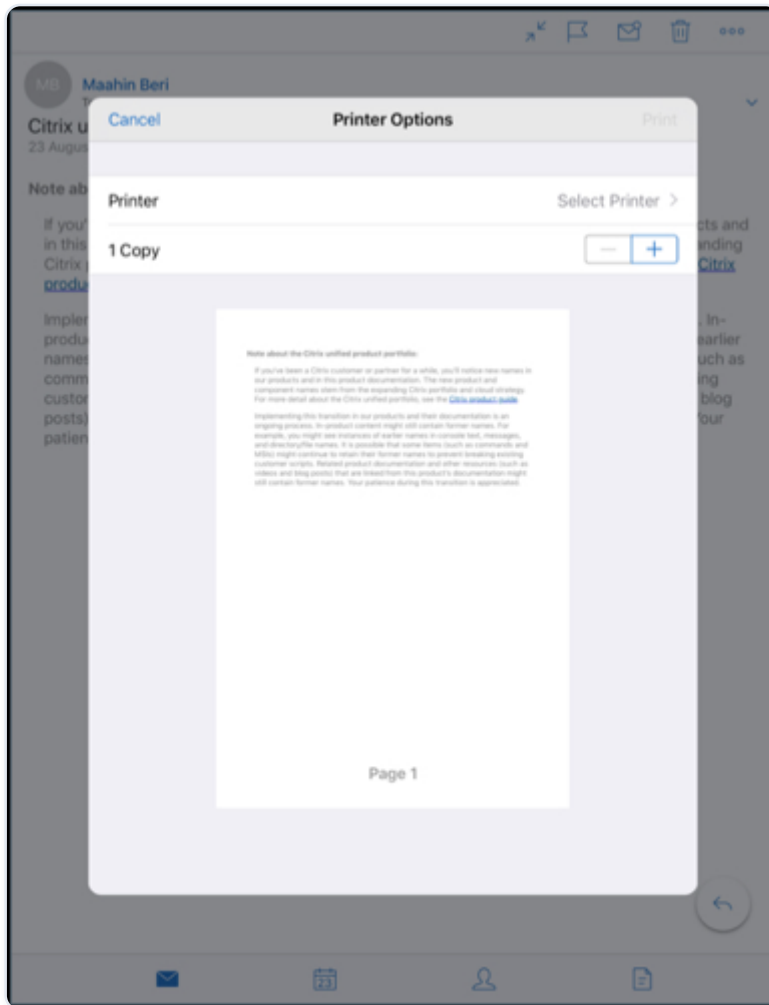
デフォルトでは、Secure Mail for iOSで印刷機能は有効になっています。印刷機能は、Apple AirPrintまたはMicrosoft Information Rights Management (IRM) を介した管理ポリシーによって管理者が制御している場合があります。これらのシナリオでは、メール、カレンダーイベント、またはインライン画像の印刷は機能せず、エラーメッセージが表示されることがあります。

メールを印刷するには

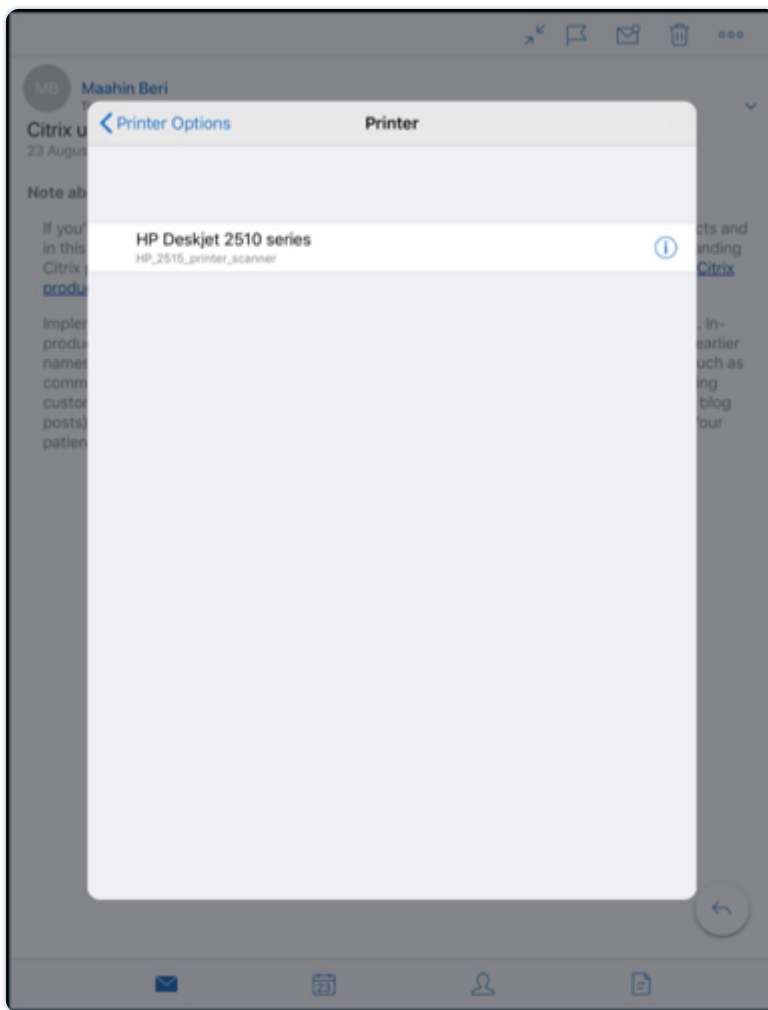
1. 印刷したいメールアイテムを開きます。
2. 画面左上の「その他」アイコンをタップします。以下のオプションが表示されます。
 - 移動
 - 印刷

印刷するメールの画像(/en-us/mobile-productivity-apps/media/SM-iOS-Print1.png)

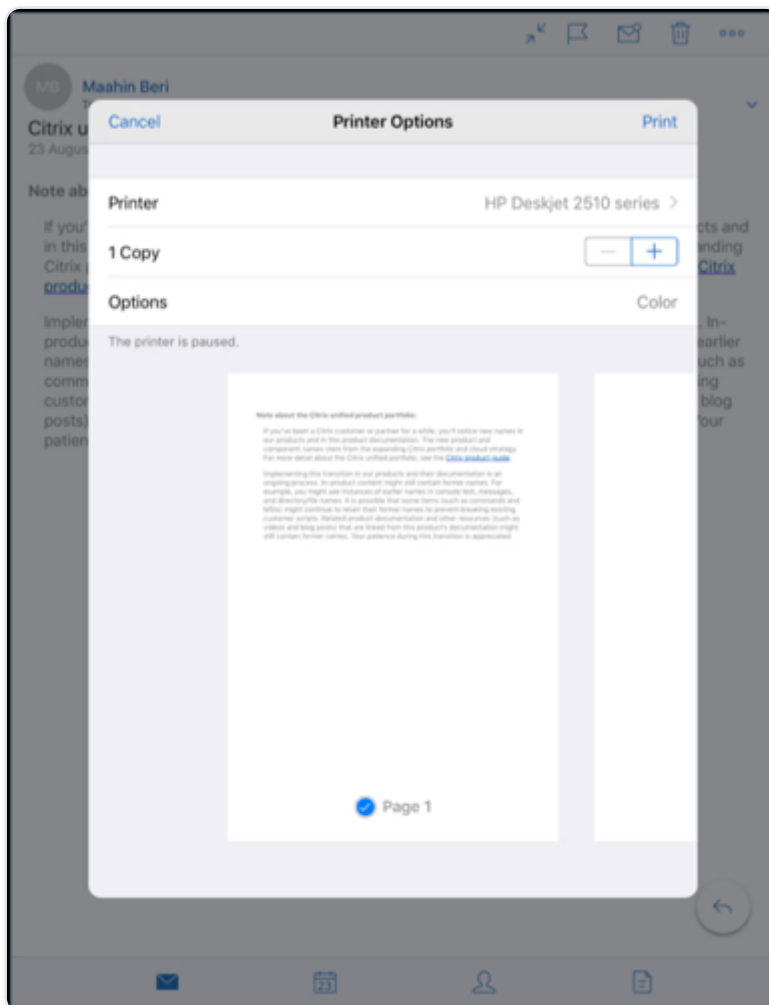
3. 印刷をタップします。 **プリンターオプション**画面が表示されます。



4. プリンターを選択するには、**プリンターを選択**をタップします。 **プリンター**画面が表示されます。



5. 印刷するプリンターを選択します。



6. 印刷する部数を減らすには**-を、増やすには+**をタップします。
7. 特定のページまたはページ範囲を印刷するには、**範囲**をタップします。 **ページ範囲**画面が表示されます。デフォルトでは、**すべてのページ**が選択されています。



8. ページ選択を変更するには、ページ番号を上下にスワイプします。



9. プリンターオプションをタップして、プリンターオプション画面に戻ります。

印刷オプションリストの画像(/en-us/mobile-productivity-apps/media/SM-iOS-Print9.png)

10. 白黒で印刷するには、**Black & White** ボタンをタップします。デフォルトでは、Secure Mail はカラーで印刷します。
11. メールを印刷するには、右上の **Print** をタップします。
12. 印刷ジョブをキャンセルするには、左上の **Cancel** をタップします。

カレンダーイベントを印刷するには

1. カレンダーに移動し、イベントを選択します。

カレンダーイベントの画像(/en-us/mobile-productivity-apps/media/SM-iOS-Print11.png)

2. 印刷アイコンをタップし、前のセクション「メールを印刷するには」で説明されているのと同じ手順に従います。

メールオプションの画像(/en-us/mobile-productivity-apps/media/SM-iOS-Print12.png)

インライン画像を印刷するには：

1. インライン画像を含むメールアイテムを開きます。
2. その他アイコンをタップします。次のオプションが表示されます。

- 移動
- 印刷
- キャンセル

メールオプションの画像(/en-us/mobile-productivity-apps/media/SM-iOS-Print14.png)

3. 印刷をタップし、次のセクション「メールを印刷するには」に記載されている指示に従います。

複数の会議コード（会議へのダイヤルイン）

iOS版Secure Mailは複数の会議コードをサポートしています。利用可能な会議コードのリストから会議コードを選択して、会議に参加できるようになりました。

会議にダイヤルインするには

1. 会議の招待を開き、**ダイヤルイン**をタップします。
2. 表示される電話番号のリストから、ダイヤルインする番号を1つ選択します。
3. 表示される会議コードのリストから、会議に参加するコードを1つ選択します。
4. **通話**をタップして会議に参加します。

メール添付ファイルの印刷サポート

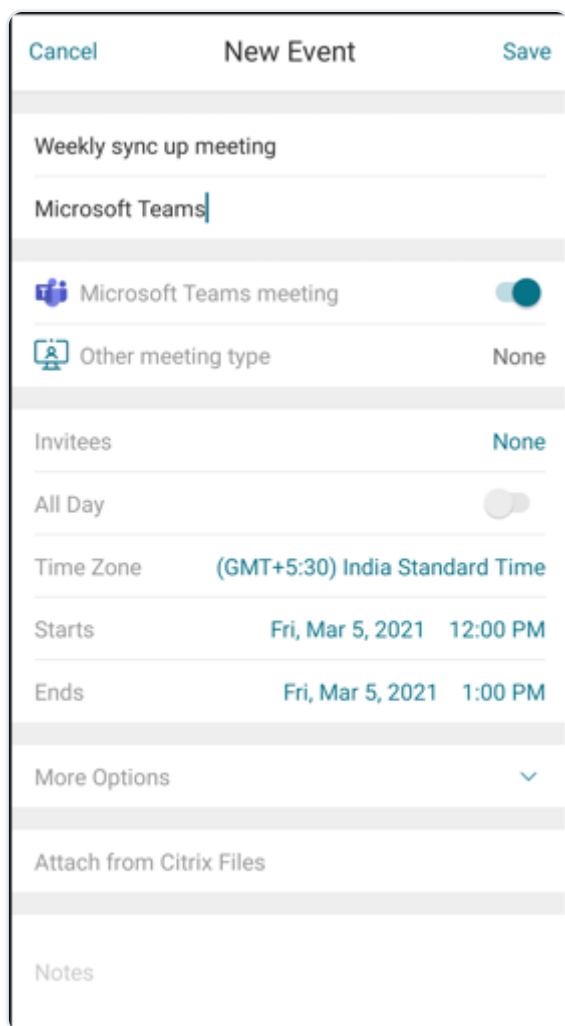
iOS版Secure Mailはメール添付ファイルの印刷をサポートしています。

Android の機能

この記事では、Secure Mail でサポートされている Android の機能について説明します。

Secure Mail のカレンダーイベントで Microsoft Teams 会議を作成する

Android 版 Secure Mail では、カレンダーイベントの作成中に Microsoft Teams 会議の招待を作成できます。Microsoft Teams 会議を作成するには、**Microsoft Teams Meeting** トグルをオンにします。会議の招待リンクと詳細は、イベントの詳細とともに自動的に送信されます。



前提条件:

Azure Active Directory のグローバル管理者が以下を実行していることを確認してください。

- 最新の認証 (OAuth) を有効にし、有効な Microsoft Teams ライセンスを持つ Exchange Online メールボックスユーザーであることを確認してください。
- Secure Mail アプリにテナント全体の管理者同意を提供します。
- Secure Mail アプリで Exchange アカウントを設定し、すべてのユーザーがサインインできるようにアプリのアクセス許可を付与します。次の画面を参照してください。

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 統合ポリシーを有効にします。

Microsoft Teams integration

ON ?

制限事項:

Secure Mail で作成された会議の場合、現在、この機能には Microsoft Outlook カレンダーで以下の制限があります。

- 「オンラインで参加」オプションは利用できません
- 「会議が開始されました」通知は利用できません

双方向連絡先同期

Android版Secure Mailでは、ローカルの連絡先リストからSecure Mailの連絡先を作成、編集、削除できます。

送信済みメールの取り消し

Android版Secure Mailでは、送信済みメールを取り消すことができます。「送信」ボタンをタップすると、送信操作を取り消すことができるトーストメッセージが表示されます。「元に戻す」をタップすると、送信操作が元に戻り、メールの編集、メール受信者の変更、添付ファイルの追加または削除、またはメールの破棄ができます。

下書きフォルダーでの添付ファイルの同期

Android版Secure Mailでは、「下書き」フォルダーが同期されると、添付ファイルも同期され、すべてのデバイスで利用できるようになります。この機能は、Exchange ActiveSyncバージョン16以降を実行しているデバイスで利用できます。

PDFファイルのアプリ内表示

Android版Secure Mailでは、ブックマークや注釈とともに、アプリ内でPDFファイルを表示できます。他のMicrosoft Office添付ファイルの拡張表示も利用できます。

Microsoft Office 365でモダン認証を実行するセットアップのトンネリングポリシーにWeb SSOを使用する

Android版Secure Mailに、「トンネリングにWeb SSOを使用」という新しいポリシーが追加されました。このポリシーを使用すると、OAuthトラフィックをトンネル化されたWeb SSO経由でルーティングできます。これを行うには：

- 「トンネリングにWeb SSOを使用」ポリシーを「オン」に設定します。
- ネットワークアクセスポリシーで「トンネル化 - Web SSO」オプションを選択します。
- 「バックグラウンドサービス」ポリシーからOAuthに関連するホスト名を除外します。

カレンダーイベントのドラッグアンドドロップ

Android版Secure Mailでは、既存のカレンダーイベントをドラッグアンドドロップして時間を変更できます。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[カレンダーイベントの時間を変更する](#)」を参照してください。

Google Play向け64ビットアプリのサポート

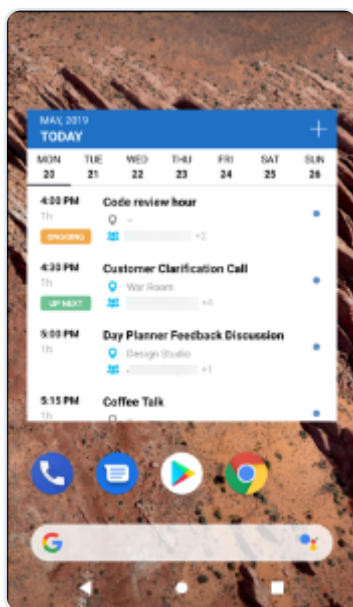
Android版Secure Mailは64ビットアーキテクチャをサポートしています。

Android版Secure MailのプルツリーフレッシュUIの改善

マテリアルデザインのガイドラインに沿って、プルツリーフレッシュ機能に若干の改善を加えました。ハンバーガーアイコンをタップすると、同期タイムスタンプが画面の下部に表示されます。

カレンダーアジェンダのウィジェット

Android版Secure Mailでは、カレンダーアジェンダがウィジェットとして利用できます。このウィジェットから、1週間分のカレンダーの今後のイベントを表示できます。この機能を使用すると、カレンダーイベントの作成、既存イベントの表示、詳細の編集が可能です。画面キャプチャのブロックポリシーは、ホーム画面に配置されたウィジェットには適用されません。ただし、カレンダーアジェンダウィジェットを許可ポリシーを使用してウィジェットを無効にできます。



ネットワークアクセスポリシー

Android版Secure Mailでは、ネットワークアクセスMDXポリシーにトンネル化 - Web SSOという新しいオプションが追加されました。このポリシーを構成すると、トンネル化されたWeb SSOとSecure Ticket Authority (STA) を介して内部トラフィックを並行してトンネル化する柔軟性が得られます。NTLM、Okta、Kerberosなどの認証サービスに対して、トンネル化されたWeb SSO接続を許可することもできます。STAを最初に構成するときは、個々のFQDNとサービスアドレスのポートをバックグラウンドネットワークサービスポリシーに追加する必要があります。ただし、トンネル化 - Web SSOオプションを構成する場合は、これらの構成を行う必要はありません。

Citrix Endpoint Management™ コンソールでAndroid版Secure Mailにこのポリシーを有効にするには：

1. Android用の.mdxファイルをダウンロードして使用します。詳細については、「[MDXアプリを追加する](#)」の手順を参照してください。
2. ネットワークアクセスポリシーで、トンネル化 - **Web SSO** オプションをクリックします。詳細については、「[アプリのネットワークアクセス](#)」を参照してください。

フィードカードの機能強化

Secure Mail for Android の既存のフィードフォルダーに、以下の機能強化が加えられました。

- 自動同期されたすべてのフォルダーからの会議の招待が、フィードカードに表示されます。
- フィードカードで最大5件の今後の会議を表示できます。
- 今後の会議は、現在の時刻から24時間に基づいて表示されるようになりました。これらの会議の招待は、**今日**と**明日**に分類されます。以前のリリースでは、その日の終わりまでの今後の会議がフィードに表示されていました。

添付ファイルの表示

Secure Mail for Android では、メールとカレンダーの添付ファイルを簡単に表示できます。この機能に関するユーザーヘルプドキュメントについては、Citrix User Help Center の記事「[ファイルの表示と添付](#)」を参照してください。

メールとカレンダーイベントの印刷

Secure Mail for Android では、Android デバイスからメールとカレンダーイベントを印刷できます。この印刷機能は、Android Print フレームワークを使用します。

前提条件

- 管理者が Citrix Endpoint Management コンソールで**印刷ブロックポリシー**を**OFF**に設定していることを確認してください。Android 用のこのポリシーについては、「[印刷ブロックポリシー](#)」を参照してください。
- メールが IRM で保護されている場合は、メールで**閲覧者に印刷を許可**オプションを有効にしてください。

これらのポリシーが不適切に設定されている場合、メールやカレンダーイベントを印刷することはできません。

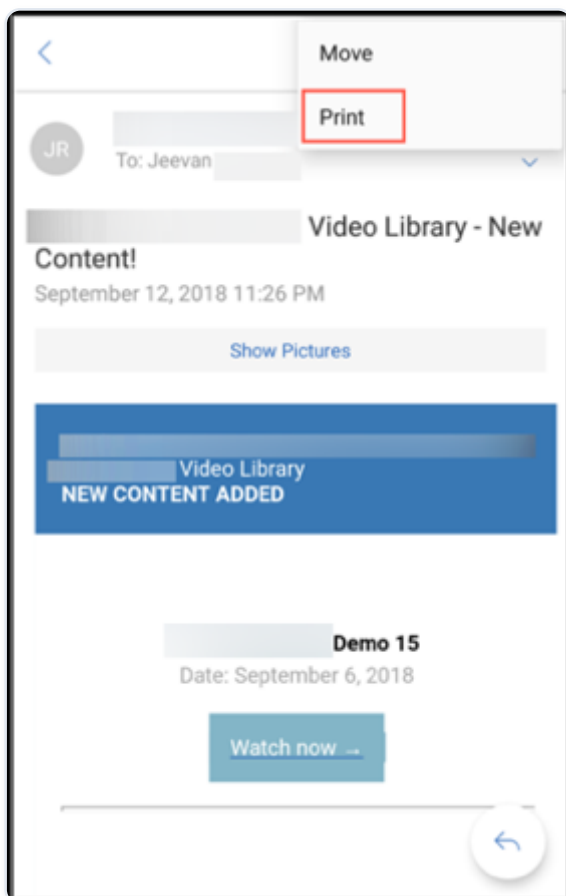
注:

この印刷機能には、以下の既知の制限があります。

- インライン画像は、**画像を表示**をタップして画像をダウンロードした場合にのみ印刷されます。**画像を表示**をタップしない場合、画像のプレースホルダーのみが印刷されます。
- Secure Mail では、サイズの大きいメールは切り詰められます。印刷する前に、**完全なメッセージをダウンロード**をタップして、完全なメールを印刷します。完全なメッセージがダウンロードされない場合、切り詰められたメールが印刷されます。
- これらのアイテムを印刷する際、メールやイベントのメタデータは追加されません。

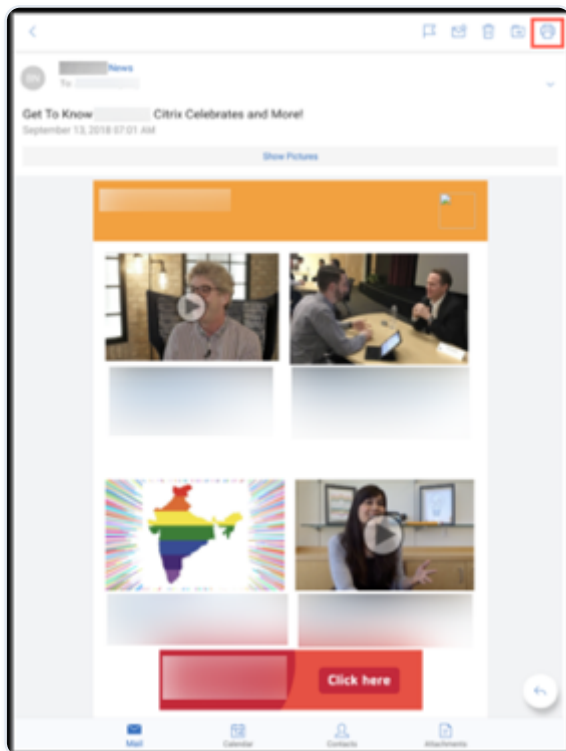
メールを印刷するには

1. 印刷したいメールを開きます。
2. 画面左上の「その他」アイコンをタップします。次のオプションが表示されます。
 - 移動
 - 印刷



注:

タブレットでは、画面左上の印刷アイコンを直接使用してメールを印刷できます。



1. 印刷をタップします。メールのプレビューが表示されます。
2. リストをタップすると、次のオプションが表示されます。

- PDFとして保存
- すべてのプリンター

「印刷オプション画面」 (/en-us/mobile-productivity-apps/media/printing-options.png)

3. メールをPDF形式で保存するには、「**PDFとして保存**」をタップします。
4. 「**すべてのプリンター**」をタップします。必要に応じてプリンターをインストールします。
5. プリンターがインストールされたら、プリンターを選択するために「**プリンターを選択**」をタップします。「**プリンター**」画面が表示されます。

注:

印刷オプションは、選択したプリンターによって異なります。次の画像はCanon E480プリンターのものであり、説明のみを目的としています。

「プリンターオプションの画像」 (/en-us/mobile-productivity-apps/media/printer-options.png)

6. 印刷したいプリンターを選択します。次の印刷オプションを使用します。

- 印刷したい部数を手動で入力します。
- リストから用紙サイズを選択します。
- リストから色を選択します。
- 必要に応じてページの向きを選択します。
- ページまたはページ範囲を選択し、ページ範囲を手動で入力します。

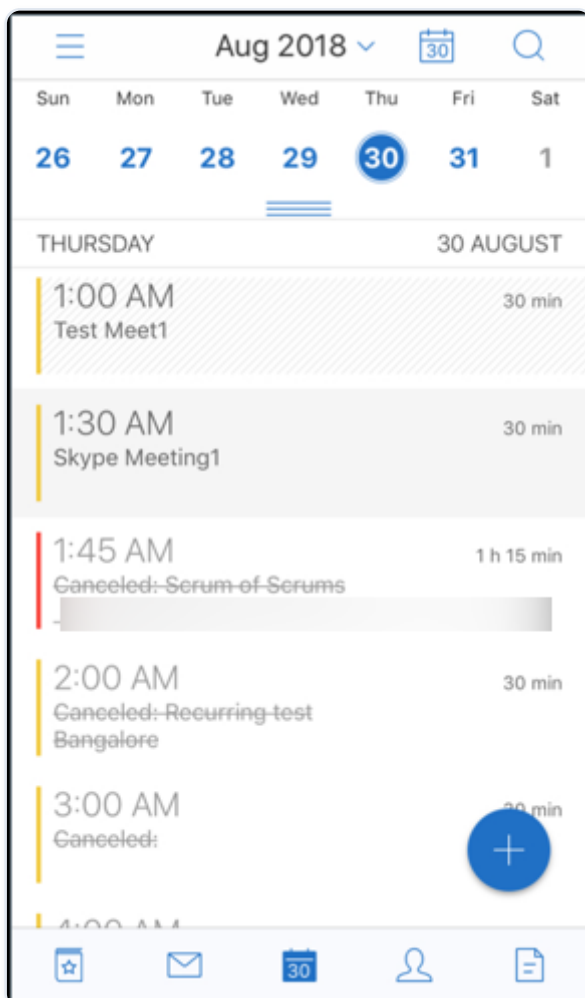
7. 印刷オプションを設定したら、画面上の印刷アイコンをタップします。

インライン画像を印刷するには

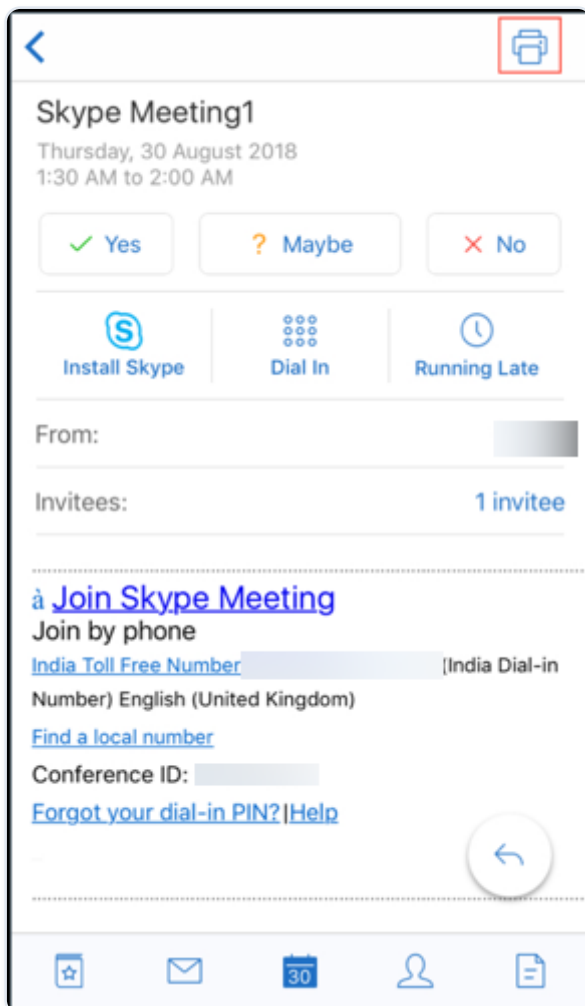
- メール内で「**画像の表示**」をタップし、前のセクション「**メールを印刷するには**」に記載されている手順に従います。

カレンダーイベントを印刷するには

1. カレンダーに移動し、イベントをタップします。



2. 印刷アイコンをタップし、前のセクション「メールを印刷するには」に記載されている手順と同じ手順に従います。



ActiveSyncヘッダー付きでフィッシングメールを報告する

Android版Secure Mailでは、ユーザーがフィッシングメールを報告すると、そのメールに対応するEMLファイルが添付ファイルとして生成されます。管理者はこのメールを受信し、報告されたメールに関連付けられたActiveSyncヘッダーを表示できます。

この機能を有効にするには、管理者は「Report Phishing Email Address」ポリシーを構成し、Citrix Endpoint Managementコンソールで「Report Phishing Mechanism」を「**Report Via Attachment**」に設定する必要があります。Secure MailのMDXポリシーの構成の詳細については、「[モバイル生産性アプリのMDXポリシー](#)」を参照してください。

サブフォルダー通知

Android版Secure Mailでは、メールアカウントのサブフォルダーからのメール通知を受信できません。

注：

- サブフォルダーの通知を受信するには、Endpoint ManagementコンソールでFCMベースのプッシュ通知が有効になっていることを確認してください。FCMベースのプッシュ通知を構成する手順については、「[Secure Mailのプッシュ通知](#)」を参照してください。
- サブフォルダー通知機能はLotus Notesサーバーでは利用できません。

サブフォルダーの通知を有効にするには

1. 設定に移動し、一般の下にある**通知**をタップします。

サブフォルダー通知設定(/en-us/mobile-productivity-apps/media/select-notifications.png)

2. **通知**画面で、**メールフォルダー**をタップします。受信トレイ内のサブフォルダーのリストが表示されます。

メールフォルダーの選択(/en-us/mobile-productivity-apps/media/mail-folder-selection.png)

3. 通知を受け取りたいサブフォルダーをタップして選択します。受信トレイはデフォルトで選択されています。

注：

サブフォルダーの通知を有効にすると、自動同期が有効になります。

サブフォルダーの選択(/en-us/mobile-productivity-apps/media/folder-selection-screen.png)

サブフォルダーの通知を無効にするには、通知を受け取りたくないサブフォルダーのチェックボックスをオフにします。

通知チャネル

Android O以降を実行しているデバイスでは、通知チャネル設定を使用して、メールとカレンダーの通知の処理方法を管理できます。この機能により、通知をカスタマイズおよび管理できます。

メールまたはカレンダーのリマインダーの通知を設定するには、Secure Mailを開き、**設定 > 通知**に移動して、目的の通知オプションを選択します。Secure Mail通知設定(/en-us/mobile-productivity-apps/media/notification-channels-settings.png)

その後、**メール通知の管理**または**カレンダー通知の管理**に移動して、それぞれメールまたはカレンダーの通知を管理できます。

メール通知チャネル設定(/en-us/mobile-productivity-apps/media/notification-channel-mail.png)

カレンダー通知チャネル設定(/en-us/mobile-productivity-apps/media/notification-channel-calendar.png)

または、デバイスのSecure Mailアプリのアイコンを長押しし、**アプリ情報**を選択してから、**通知**をタップします。

以前にバイブレーション設定が**サイレント時のみ**に設定されていた場合、この機能によりバイブレーション設定はデフォルトのバイブレーション設定（**オフ**）に変更されます。

注：

ロック画面の通知は、管理者が「ロック画面通知の制御」MDXポリシーをどのように構成したかに基づいて利用できます。

メール内の会議応答ボタン

Android版Secure Mailでは、会議応答ボタンがメール内に表示されます。会議の招待に関するメール通知を受信すると、以下のいずれかのオプションをタップして招待に応答できます。

- はい
- 未定
- いいえ

Android版Secure Mailでの会議招待オプションの画像(/en-us/mobile-productivity-apps/media/meeting-response-in-android-message.png)

添付ファイルの機能強化

Android版Secure Mailでは、添付ファイルの表示が簡素化されました。より良いエクスペリエンスのために、不要な手順が削除され、以前のリリースに存在した添付ファイルオプションは保持されています。

Secure Mailアプリ内で添付ファイルを表示できます。Secure Mailを使用して表示できる場合、添付ファイルは直接開きます。Secure Mailを使用して添付ファイルを表示できない場合は、アプリのリストが表示されます。必要なアプリを選択して添付ファイルを表示できます。この機能に関する

るユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[ファイルの表示と添付](#)」を参照してください。

戻るボタンの機能強化

Android版Secure Mailでは、デバイスの戻るボタンをタップして、**フローティングアクションボタン**の展開されたオプションを折りたたむことができます。この操作により、メッセージまたはイベントの詳細ビューに戻ります。

Androidの戻るボタンの機能強化の画像(/en-us/mobile-productivity-apps/media/secure-mail-android-back-button.png)

Androidでギャラリーからファイルを添付できるようにするための管理者向け手順

Secure Mailバージョン10.3.5以降では、受信ドキュメント交換 (Open-in) ポリシーが**制限付き**に設定されている場合、ユーザーはギャラリーアプリから画像を直接添付できません。このポリシーを**制限付き**のままにしつつ、ユーザーがギャラリーから写真を追加できるようにするには、Endpoint Managementコンソールで以下の手順に従ってください。

1. **ギャラリーをブロックをオフ**に設定します。
2. デバイスのギャラリーパッケージIDを取得します。例をいくつか示します。
 - **LG Nexus 5 (エルジー ネクサス 5):** com.google.android.gallery3d, com.google.android.apps.photos
 - **Samsung Galaxy Note 3 (サムスン ギャラクシー ノート 3):** com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photos
 - **Sony Expire (ソニー エクスパイア):** com.sonyericsson.album, com.google.android.apps.photos
 - **HTC:** com.google.android.apps.photos, com.htc.album
 - **Huawei (ファーウェイ):** com.android.gallery3d, com.google.android.apps.photos
3. 非表示のポリシーInboundDocumentExchangeWhitelistを表示にします。
 - WorxMail APKファイルをダウンロードし、MDX Toolkitでファイルをラップします。
 - コンピューターで.mdxファイルを見つけ、ファイルのサフィックスを.zipに変更します。
 - .zipファイルを開き、policy_metadata.xmlファイルを見つけます。

- InboundDocumentExchangeWhitelistを `PolicyHidden>true</PolicyHidden>` から `<PolicyHidden>false</PolicyHidden>` に検索して変更します。
- policy_metadata.xml ファイルを保存します。
- そのフォルダー内のすべてのファイルを選択し、圧縮して .zip ファイルを作成します。

注:

外側のフォルダーを圧縮しないでください。フォルダー内のすべてのファイルを選択し、選択したファイルを圧縮します。

- 結果として作成された圧縮ファイルをクリックします。
 - **情報を見る**を選択し、ファイルサフィックスを .mdx に戻します。
4. 変更した .mdx ファイルを Endpoint Management コンソールにアップロードし、ギャラリーパッケージIDのリストを、表示されるようになった「受信ドキュメント交換ホワイトリスト」ポリシーに追加します。

受信ドキュメント交換許可リストの画像(/en-us/mobile-productivity-apps/media/secure-mail-exchange-allow-list.png)

パッケージIDがコンマで区切られていることを確認してください。

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

5. Secure Mail を保存して展開します。

Androidユーザーは、ギャラリーアプリから画像を添付できるようになりました。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[ファイルの表示と添付](#)」を参照してください。

サポートされているファイル形式

X は、Secure Mail で添付、表示、および開くことができるファイル形式を示します。

形式	IOS	アンドロイド
ビデオ: H.263 AMR NB コーデック_Mp4		X

形式	IOS	アンドロイド
ビデオ: H.263 AMR NB コーデック_3gp		X
ビデオ: H.264 AAC コーデック_3gp	X	X
ビデオ: H.264 AAC コーデック_mp4	X	X
ビデオ: H.264 Acclc コーデック_mp4	X	X
GTM recorded_wmv		X
AVI		X
WAV	X	X
MP4	X	X
3GP	X	X
FLAC		X
AAC	X	X
M4A	X	X
スリージーピー(エーエムアールエヌビー)	X	X
MP3	X	X
WAV	X	X
OGG		X
ICO	X	X
JPEG	X	X
PNG	X	X

形式	IOS	アンドロイド
TIF (単一ページのみ)	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
HTML	X	X

形式	IOS	アンドロイド
ZIP	X	X
EML	X	X

カレンダー

デバイス上の複数のアカウントに関連するすべてのイベントがカレンダーに表示されます。個々のアカウントに関連するカレンダーイベントを区別するために、個々のアカウントに色を設定できます。

注:

パーソナルカレンダー機能は、有効になっている場合、常にプライマリまたはデフォルトのアカウントに関連付けられます。

プライマリまたはデフォルトのアカウントに関連付けられたカレンダーの画像(/en-us/mobile-productivity-apps/media/Multiple-EA-Calendar-view.png)

カレンダーイベントに色を設定するには

1. フッターバーのカレンダーアイコンをタップし、左上のハンバーガーアイコンをタップします。 **カレンダー**画面に、設定したすべてのアカウントが表示されます。
2. Exchangeアカウントの右側に表示されているデフォルトの色をタップします。色の画面に、そのアカウントで利用可能な色が表示されます。
3. 任意の色を選択し、**保存**をタップします。
4. 前の画面に戻るには、**キャンセル**をタップします。選択した色は、そのExchangeアカウントに関連するすべてのカレンダーイベントに設定されます。

カレンダーの色のオプションの画像(/en-us/mobile-productivity-apps/media/Multiple-EA-Calendar-colors.png)

色分けされたアカウントの画像(/en-us/mobile-productivity-apps/media/Multiple-EA-Calendar-colors-change.png)

色付きのカレンダーの画像(/en-us/mobile-productivity-apps/media/Multiple-EA-Calendar-colors-changed.png)

カレンダーの招待またはイベントを作成するとき、**主催者**フィールドにはデフォルトアカウントのメールアドレスが自動入力されます。メールアカウントを変更するには、このメールアドレスをタップして別のアカウントを選択します。

主催者フィールドの画像(/en-us/mobile-productivity-apps/media/Multiple-EA-Calendar-new-event.png)

主催者の選択の画像(/en-us/mobile-productivity-apps/media/Multiple-EA-Calendar-new-event-change-org.png)

検索

メールボックスまたは**すべての連絡先**ビューからグローバル検索を実行できます。この操作により、アプリ内のすべてのアカウントを検索した後に適切な結果が表示されます。

個々のアカウント内からのすべての検索では、そのアカウントにのみ関連する結果が表示されます。

バックグラウンドサービスの更新

Android 8.0 (APIレベル26)以降を実行しているデバイスでGoogle Playのバックグラウンド実行制限要件を満たすため、Secure Mailのバックグラウンドサービスをアップグレードしました。デバイスでのメール同期と通知を中断なく行うには、Firebase Cloud Messaging (FCM)サービスプッシュ通知を有効にしてください。FCMベースのプッシュ通知の有効化に関する詳細については、「[Secure Mailのプッシュ通知](#)」を参照してください。

デバイスのSecure Mail設定で**メール通知**がオンになっていることを確認してください。 **制限事項:**

- FCMベースのプッシュ通知を有効にしていない場合、バックグラウンド同期は15分ごとに1回行われます。この間隔は、アプリがバックグラウンドで実行されているかフォアグラウンドで実行されているかによって異なります。
- ユーザーがデバイス設定から時刻を手動で更新しても、カレンダーウィジェットの日付は自動的に更新されません。

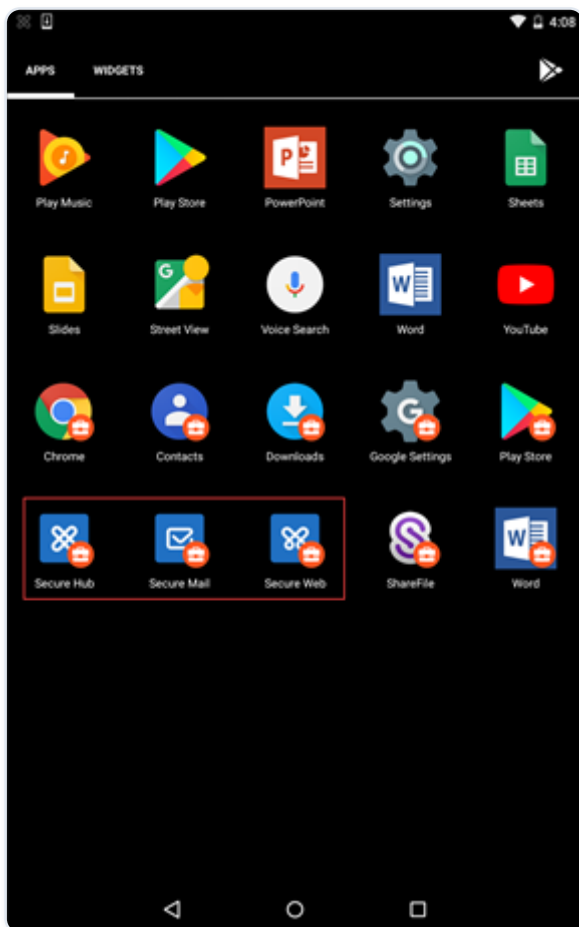
セキュアメールにおけるアンドロイドエンタープライズ

Android版Secure MailおよびSecure Webは、以前はAndroid for Workとして知られていたAndroid Enterpriseと互換性があります。

前提条件

- この機能を使用するには、デバイスがAndroid 5.0以降を実行していることを確認してください。
- オンプレミス展開の場合、**afw.accounts** Endpoint Managementプロパティを**TRUE**に設定する必要があります。

Endpoint ManagementでAndroid Enterpriseを設定すると、モバイル生産性向上アプリがデバイスで利用可能になります。次の画像で強調表示されているように、Android Enterpriseアイコンがアプリを識別します。



Android Enterpriseと互換性のある機能

次の表に、Android Enterpriseと互換性のあるSecure Mailの機能を示します。

機能	サポート
Exchange Serverの自動検出	X
セキュアチケットオーソリティ (STA)	X

機能	サポート
連絡先のエクスポート	X
マイクロソフト情報権限管理	X
ロック画面通知	X
メール同期	X
メール分類	X
S/MIME署名と暗号化	X
ファイアベース クラウド メッセージング (FCM) サービス	X
最新の認証 (OAuth)	
複数のExchangeアカウント	X
個人カレンダー	
メール設定のエクスポート	X
共有デバイス	
マイクロソフト インチューン/EMS との エンドポイント管理 統合	
オフィス 365	X
LDAP Exchange Server 2010、2013、および 2016	X
証明書ベースの認証 (CBA)	
Go ToMeeting	X
スカイプ フォー ビジネス	
個人配布リスト	X
Citrix Filesの互換性	X

機能	サポート
シングルサインオンによるメール登録	X

以下の表に、Android Enterpriseと互換性のあるSecure Webの機能を示します。

機能	サポート
トンネル化 – Web SSO モード	X
フル VPN モード	X
すべてのアプリ機能	X
Secure Mail との互換性	X

制限事項

- Android Enterprise のワークプロファイルモードで、デバイス制限ポリシーの が に設定されている場合、Android 版 Secure Mail のカレンダーのエクスポートの進行状況とプッシュ通知はステータスバーに表示されません。ただし、これらの通知は許可されている場合、ロック画面に表示されます。詳しくは、[Android Enterprise の設定](#)を参照してください。

Secure Mail の iOS および Android 機能

この記事では、Secure Mail でサポートされている iOS および Android の機能について説明します。

アジュール ガバメント クラウド コンピューティング のサポート

Secure Mail は、Azure Active Directory テナントでの最新の認証 (OAuth) 用に Government Cloud Computing (GCC) High をサポートしています。Secure Mail は、すべての GCC High サービスに対する Microsoft の必須要件を満たすために、GCC High のエンドポイントとして登録されています。詳細については、「[Microsoft 365 Government の Azure Active Directory の新機能](#)」を参照してください。

この変更により、認証のために Azure Active Directory テナント上の GCC High にルーティングされます。また、管理者は Azure Active Directory テナントで Secure Mail のアクセス許可を許可する必要があります。

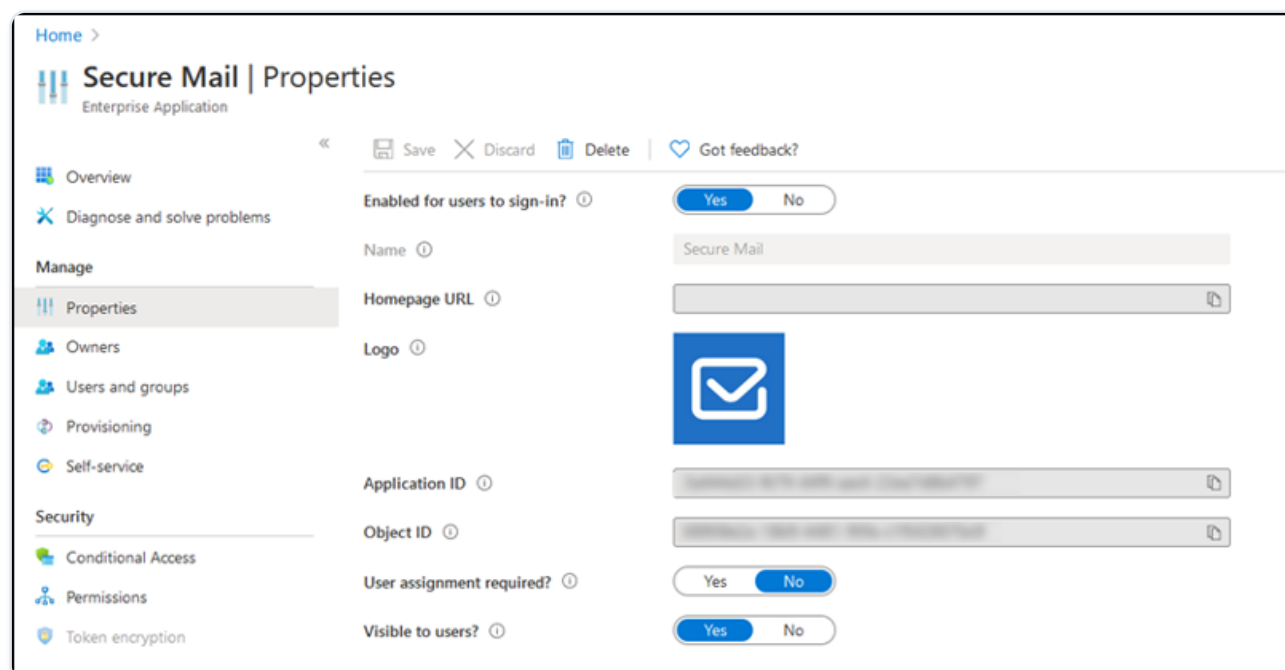
前提条件

Azure Active Directory のグローバル管理者が以下を実行していることを確認してください。

- デバイスに Secure Mail の最新バージョンをダウンロードします。
- Secure Mail アプリで Exchange アカウントを構成し、すべてのユーザーがサインインできるように Azure Active Directory でアプリのアクセス許可を許可します。次の画面を参照してください。

注:

これらの手順は、グローバル管理者のみが一度だけ実行する必要があるものです。アプリへのアクセスが許可されれば、App Store から簡単にアップグレードできます。



アップグレード後

アップグレード後、更新トークンの有効期限が切れると再認証を求められ、Azure AD 上の GCC High にリダイレクトされます。認証要求が Azure AD 上の GCC High に送信されることを確認するために、上記のワークフローを検証してください。

ワークフローは、次のいずれかの方法で検証できます。

- アプリ名 **Secure Mail-GCC High** を持つ Secure Mail が、Azure Active Directory テナントのサインインページに表示されます。
- 再認証後にリダイレクトが `<https://login.microsoftonline.us>` 経由で発生するかどうかを確認するには、Secure Mail のログを確認してください。

ICS ファイルのサポート

Secure Mail では、添付ファイルとして受信した ICS ファイルをプレビューし、イベントとしてカレンダーにインポートできます。

Secure Mail の連絡先写真

Secure Mail では、メールや会議の招待状で受信者を追加する際に、連絡先の写真を表示できます。この機能に関するユーザーヘルプドキュメントについては、Citrix ユーザーヘルプセンターの記事「[連絡先の写真を表示する](#)」を参照してください。

フィードの管理

Secure Mailでは、要件に基づいてフィードカードを整理できるようになりました。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[メールを整理する](#)」を参照してください。

Office 365 Exchange Serverポリシーを使用してOffice 365サーバーアドレスを定義する

Secure Mailでは、「Office 365のOAuthサポート」セクションに**Office 365 Exchange Server**という新しいポリシーが追加されました。このポリシーを使用すると、クラウド上にあるOffice 365メールボックスのホスト名を定義できます。このポリシーは、政府機関向けのOffice 365のサポートも有効にします。ホスト名は、*outlook.office365.com*のような単一の値です。デフォルト値は*outlook.office365.com*です。

暗号化管理のサポート

暗号化管理を使用すると、最新のデバイスプラットフォームセキュリティを利用できると同時に、デバイスがプラットフォームセキュリティを効果的に使用できる十分な状態を維持できます。暗号化管理を使用することで、ファイルシステム暗号化はiOSまたはAndroidプラットフォームによって提供されるため、ローカルデータ暗号化の冗長性を排除できます。この機能を有効にするには、管理者はCitrix Endpoint Management™ コンソールで**暗号化の種類MDXポリシーをコンプライアンス強制付きプラットフォーム暗号化**に構成する必要があります。

暗号化管理機能を使用するには、Citrix Endpoint Managementコンソールで**暗号化の種類**ポリシーを**コンプライアンス強制付きプラットフォーム暗号化**に設定します。これにより暗号化管理が有効になり、ユーザーデバイス上の既存の暗号化されたすべてのアプリケーションデータは、MDXではなくデバイスによって暗号化された状態にシームレスに移行します。この移行中、アプリは1回限りのデータ移行のために一時停止されます。移行が成功すると、ローカルに保存されたデータの暗号化の責任はMDXからデバイスプラットフォームに移管されます。MDXは、アプリの起動ごとにデバイスのコンプライアンスチェックを続行します。この機能は、MDM + MAM環境とMAMのみの環境の両方で機能します。

暗号化の種類ポリシーを**コンプライアンス強制付きプラットフォーム暗号化**に設定すると、新しいポリシーが既存のMDX暗号化に優先します。

Secure Mailの暗号化管理MDXポリシーの詳細については、次の**暗号化**セクションを参照してください。

- Android向けモバイル生産性アプリのMDXポリシー(/ja-jp/mobile-productivity-apps/administrator-tasks/policies-android.html#encryption)
- iOS向けモバイル生産性アプリのMDXポリシー(/ja-jp/mobile-productivity-apps/administrator-tasks/policies-ios.html)

デバイスが最小コンプライアンス要件を下回った場合、**非準拠デバイスの動作**ポリシーにより、実行するアクションを選択できます。

- **アプリを許可** – アプリの通常実行を許可します。
- **警告後にアプリを許可** – アプリが最小コンプライアンス要件を満たしていないことをユーザーに警告し、アプリの実行を許可します。これがデフォルト値です。
- **アプリをブロック** – アプリの実行をブロックします。

iOSを実行しているデバイス

iOSを実行しているデバイスが最小コンプライアンス要件を満たしているかどうかは、以下の基準によって決定されます。

- iOS 10 - アプリが指定されたバージョン以上のオペレーティングシステムバージョンで実行されていること。
- デバッガーアクセス - アプリでデバッグが有効になっていないこと。
- ジェイルブレイクされたデバイス - アプリがジェイルブレイクされたデバイスで実行されていないこと。
- デバイスパスコード - デバイスパスコードがオンであること。
- データ共有 - アプリでデータ共有が有効になっていないこと。

Androidを実行しているデバイス

Androidを実行しているデバイスが最小コンプライアンス要件を満たしているかどうかは、以下の基準によって決定されます。

- Android SDK 24 (Android 7 Nougat) - アプリが指定されたバージョン以上のオペレーティングシステムバージョンで実行されています。
- デバッガーアクセス - アプリでデバッグが有効になっていません。
- ルート化されたデバイス - アプリがルート化されたデバイスで実行されていません。
- デバイスロック - デバイスのパスコードがオンになっています。
- デバイスの暗号化 - アプリが暗号化されたデバイスで実行されています。

レスポンスメールのサポート

Secure Mailは、レスポンスメールを配信するために最適化されました。以前は、大きなテーブルや画像を含むメールコンテンツが正しくレンダリングされませんでした。この機能により、メールの形式やサイズに関係なく、サポートされているすべてのデバイスでメールコンテンツがより読みやすくなります。

カレンダーイベントのドラッグアンドドロップ

Secure Mailでは、既存のカレンダーイベントをドラッグアンドドロップすることで、その時間を変更できます。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[カレンダーイベントの時間を変更する](#)」を参照してください。

フィードの管理

Secure Mailでは、要件に基づいてフィードカードを整理できるようになりました。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[メールを整理する](#)」を参照してください。

自動送り

Secure Mailで会話内のメッセージを削除すると、どのメッセージに戻るかを選択できます。この機能を使用するには、**設定 > 自動送り**に移動します。次に、利用可能な選択肢から優先設定を選択します。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[会話でメールを削除して自動的に次に進む](#)」を参照してください。

下書きフォルダーの自動同期

下書きフォルダーは自動的に同期され、下書きはすべてのデバイスで利用できます。この機能は、Office 365またはExchange Server 2016以降を実行しているデバイスで利用できます。

注記:

Secure Mail の下書きに添付ファイルが含まれている場合、添付ファイルはサーバーに同期されません。

この機能に関するユーザーヘルプドキュメント（ビデオを含む）については、Citrix User Help Center の記事「[下書きフォルダーの自動同期](#)」を参照してください。

MDM + MAM モードで Microsoft Intune を使用する場合は シングルサインオンのサポート

iOS を実行しているデバイスの場合:

この機能を使用するには、デバイスに Microsoft Authenticator アプリがインストールされていることを確認してください。Microsoft Authenticator アプリのインストールについて詳しくは、Docs.microsoft.com の「**Microsoft Authenticator アプリのダウンロードとインストール**」を参照してください。

Android を実行しているデバイスの場合:

この機能を使用するには、デバイスに Intune Company Portal アプリがインストールされていることを確認してください。Intune Company Portal アプリにログインすると、Secure Mail で資格情報を使用して再認証することなく、MDM + MAM モードで SSO を使用できます。

連絡先の機能強化

Secure Mail で、**連絡先**をタップして連絡先を選択すると、その連絡先の詳細が**連絡先**タブに表示されます。**組織**タブをタップすると、**マネージャー**、**直属の部下**、**同僚**などの組織階層の詳細が表示されます。画面右上のその他アイコンをタップすると、次のオプションが表示されます:

- 編集
- VIP に追加
- キャンセル

組織タブで、**マネージャー**、**直属の部下**、または**同僚**の右側にあるその他アイコンをタップできます。この操作により、メールまたはカレンダーイベントを作成できます。メールまたはカレンダーイベントの宛先:フィールドには、**マネージャー**、**直属の部下**、または**同僚**の詳細が自動的に入力されます。メールを作成して送信できます。

前提条件

Exchange Web Services (EWS) が Exchange Server で有効になっていることを確認してください。

連絡先の詳細は、Active Directory から取得された組織の詳細 (Outlook 連絡先) に基づいて表示されます。連絡先に正しい詳細が表示されるように、管理者が Active Directory で組織階層を構成していることを確認してください。

注:

この機能は IBM Lotus Notes サーバーではサポートされていません。

会議の時間と場所をネイティブカレンダーにエクスポートする

Secure Mail では、**Export Calendar** MDXポリシーに新しい値 **Meeting Time, Location** が追加されました。この機能強化により、Secure Mail のカレンダーイベントの会議の時間と場所をネイティブカレンダーにエクスポートできます。

複数のExchangeアカウント

Secure Mail 内の から、複数の Exchange メールアカウントを追加し、それらを切り替えることができます。この機能により、すべてのメール、連絡先、カレンダーを1か所で監視できます。管理者の前提条件は次のとおりです。

- 追加のアカウントを構成するには、ユーザー名とパスワードが必要です。自動登録または資格情報ストアの構成は、アプリで最初に設定されたアカウントにのみ適用されます。追加のすべてのアカウントについて、ユーザー名とパスワードを入力してください。
- 最初に作成するアカウントが証明書ベースの場合、それ以上の証明書ベースのアカウントを追加することはできません。追加のアカウントは、Active Directory に基づく認証を使用する必要があります。Secure Mail は、複数のアカウントを構成する際に証明書ベースの認証をサポートしていません。
- 外部ネットワークのドメインまたはExchange Serverにさらに多くのアカウントを接続できるようにするには、Citrix ADCでスプリットトンネリングを**ON**に設定する必要があります。
- iOS版Secure Mailは、ExchangeおよびOffice 365メールサーバーのみをサポートしています。

この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[Exchangeアカウントを追加する](#)」を参照してください。

連絡先

連絡先に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[連絡先を表示して同期する](#)」を参照してください。

カレンダーで色を設定する

このカレンダー機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[同期されたSecure Mailカレンダーの色を設定する](#)」を参照してください。

内部ドメイン

外部組織に属するメール受信者を識別して編集できます。

前提条件: Citrix Endpoint Managementで**内部ドメイン**ポリシーを有効にし、アプリケーションを再起動していることを確認してください。

メールを作成、返信、または転送すると、外部の受信者がメーリングリストで強調表示されます。画面左下に警告として**連絡先**アイコンが表示されます。**連絡先**アイコンをタップして、メーリングリストを変更します。

iOSデバイスの場合：

Cancel

New Message

Send

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

Cc: john@yahoo.com | +

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

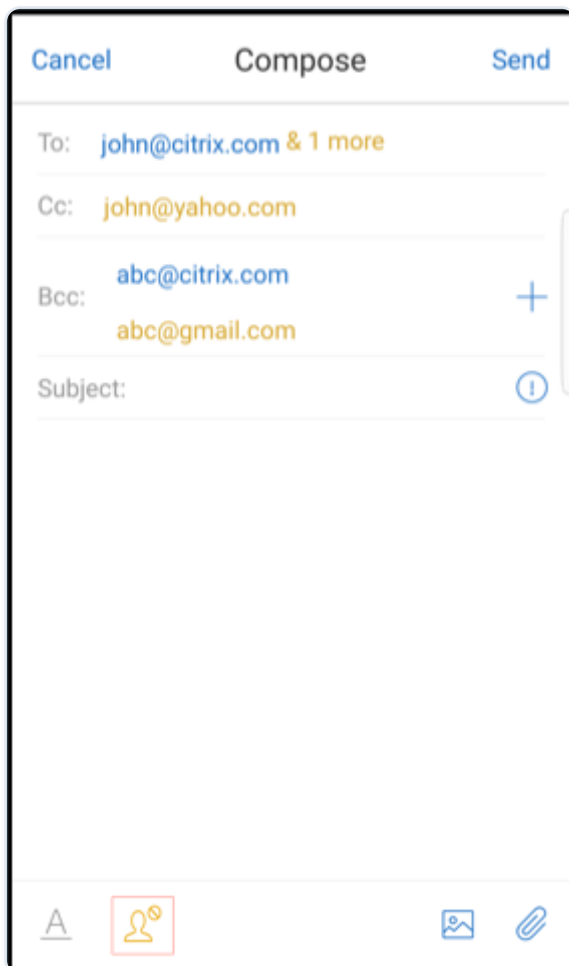
Subject: ⓘ





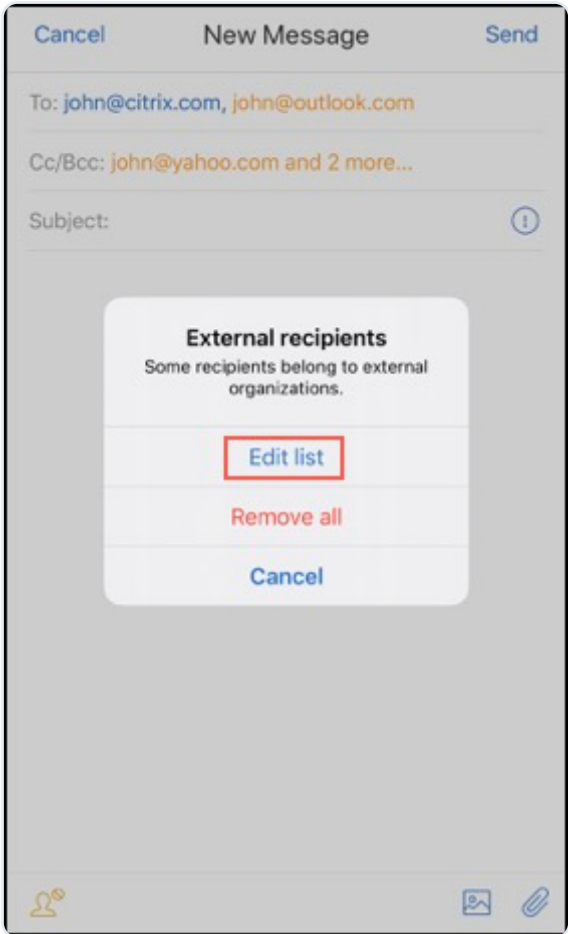


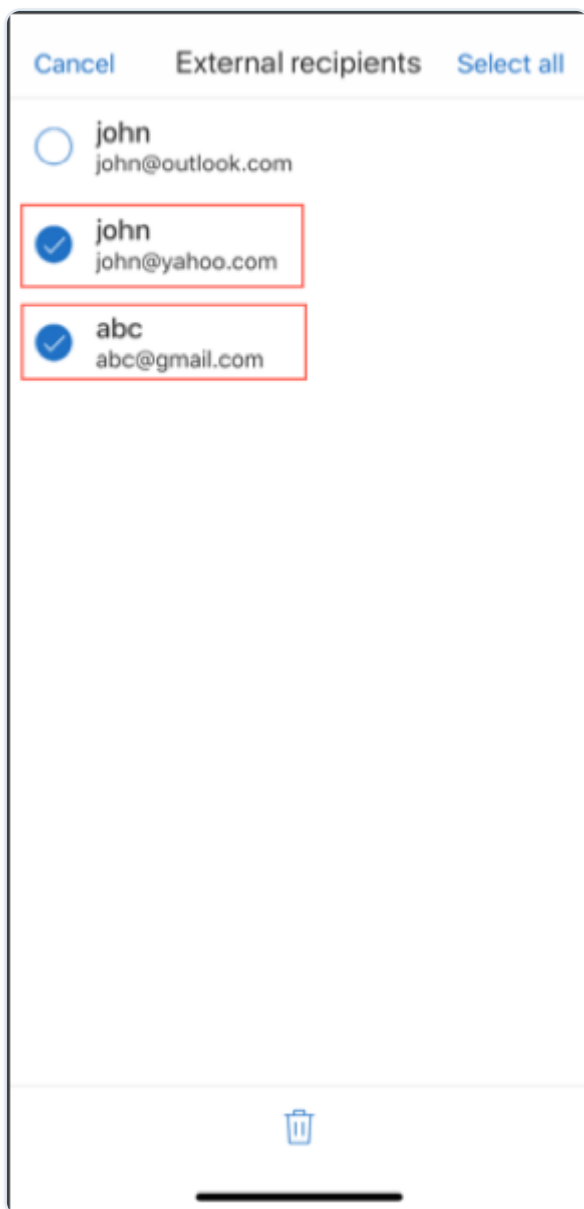
Androidデバイスの場合：



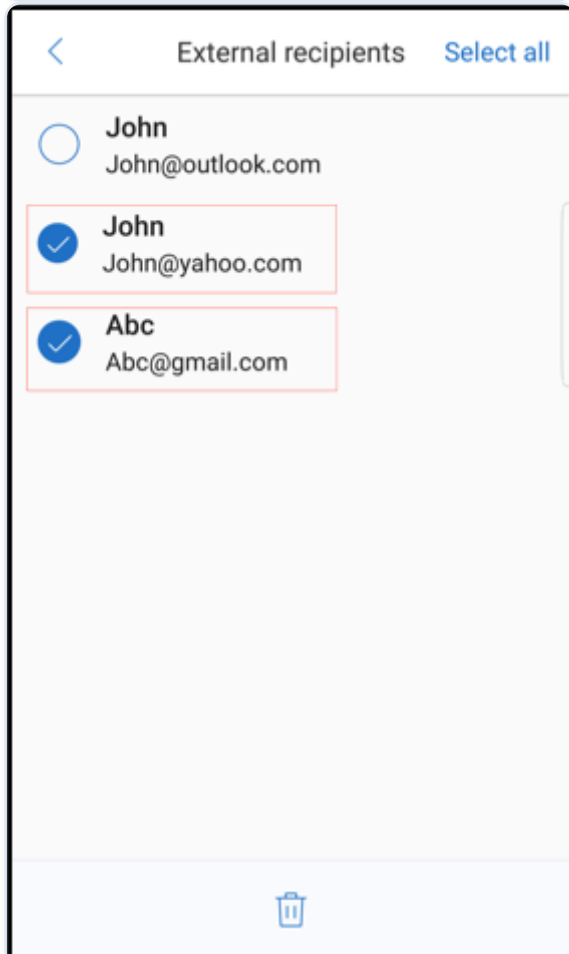
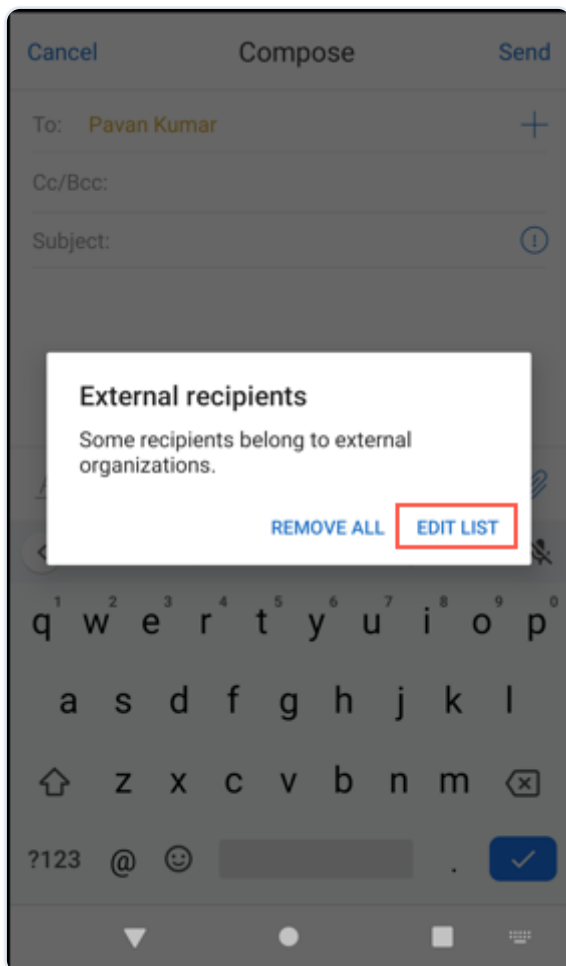
連絡先アイコンをタップすると、リストの編集またはすべて削除のオプションが表示されたポップアップウィンドウが表示されます。リストの編集をタップして、削除する受信者を選択します。受信者を選択したら、ゴミ箱アイコンをタップします。

iOSデバイスの場合：





Androidデバイスの場合：



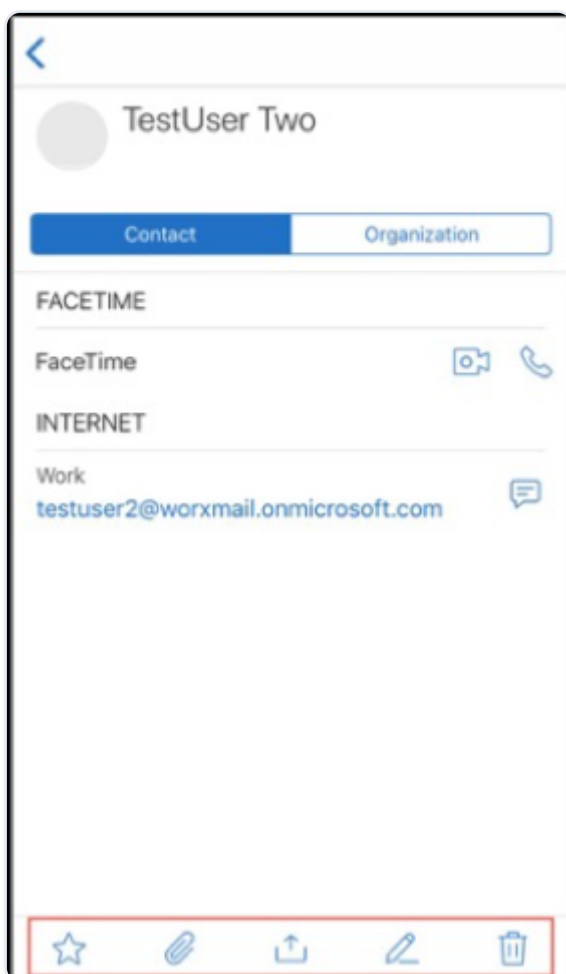
人間工学に基づいた改善

この機能強化により、アクションボタンは画面上部から下部に移動され、簡単にアクセスできるようになりました。これらの変更は、受信トレイ、カレンダー、および連絡先画面に適用されます。

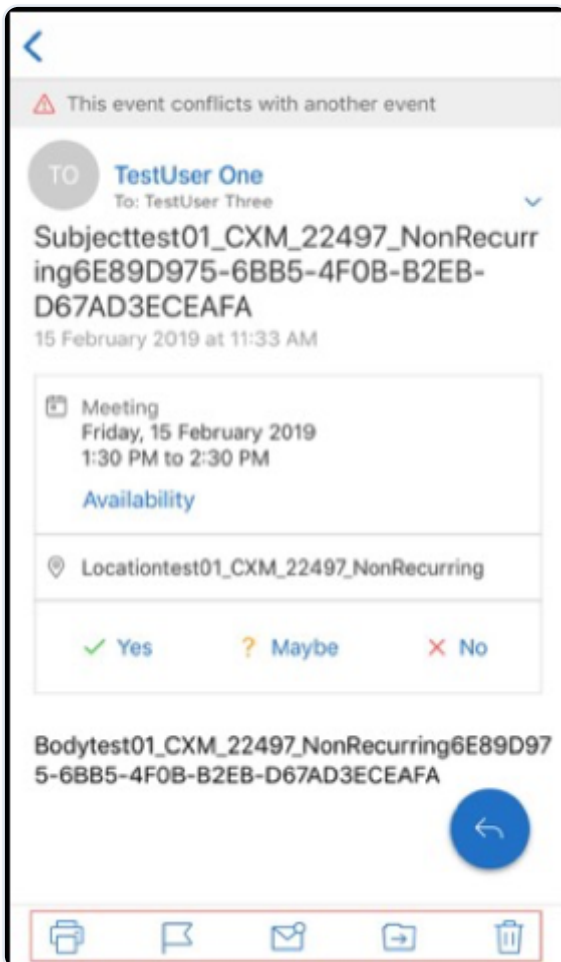
注:

Androidの場合、変更は受信トレイとカレンダー画面に適用されます。

iOSを実行しているデバイスの場合



Androidを実行しているデバイスの場合



返信フローティングアクションボタンは、Citrixのブランディングおよびスタイルガイドに準拠するように強化されました。

また、この機能強化により、開いているメールからメインの受信トレイ画面のボタンにアクセスするオプションが削除されました。フィード、カレンダー、連絡先、添付ファイルなどの項目にアクセスするには、開いているメールを終了する必要があります。

iOSのフッターバーのオプションが変更され、iOSとAndroidの両方で統一性が保たれるようになりました。

Secure MailとSlackの統合（プレビュー）

iOSまたはAndroidを実行しているデバイスで、メールの会話をSlackアプリに引き継ぐことができるようになりました。詳細については、「[Secure MailとSlackの統合（プレビュー）](#)」を参照してください。

フィッシングメールを報告する（転送として）

Secure Mailでは、フィッシングの疑いがあるメールを（転送として）報告する「フィッシングとして報告」機能を使用できます。管理者がポリシーで構成したメールアドレスに、疑わしいメッ

セージを転送できます。この機能を有効にするには、管理者が「フィッシングメール報告アドレス」ポリシーを構成し、「フィッシング報告メカニズム」を「転送による報告」に設定する必要があります。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[フィッシングメールを報告する](#)」を参照してください。

フィッシングメールを報告する

管理者が構成するポリシーに基づいて、フィッシングメールを報告できます。この機能に関するユーザーヘルプドキュメント（管理者設定の詳細を含む）については、Citrixユーザーヘルプセンターの記事「[フィッシングメールを報告する](#)」を参照してください。

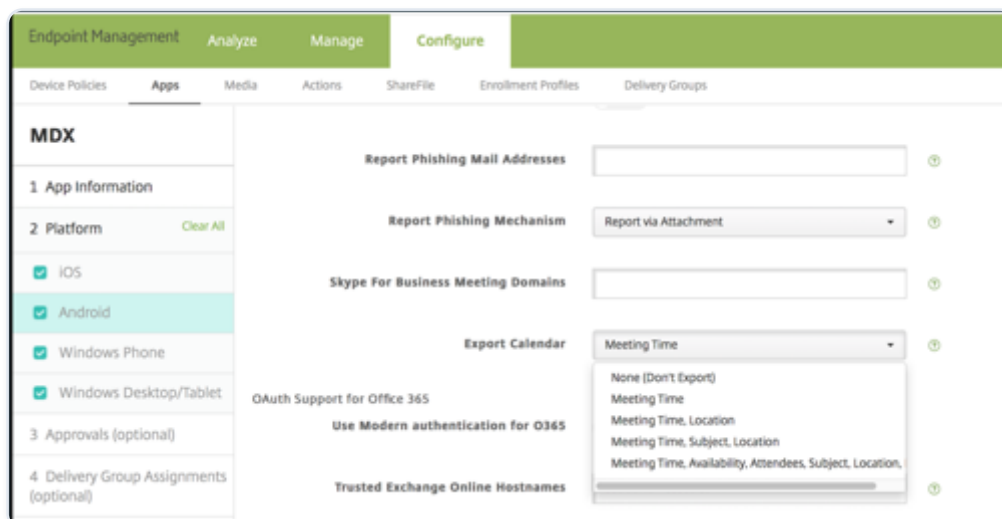
Secure Mailの予定をエクスポートする

iOSおよびAndroid版Secure Mailを使用すると、Secure Mailの予定をデバイスのネイティブカレンダーアプリにエクスポートできます。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事「[Secure Mailの予定をエクスポートする](#)」を参照してください。

個人用カレンダーに表示される予定のフィールドには、以下のMDXポリシー値を使用できます。

- なし（エクスポートしない）
- 会議時間
- 会議時間、場所
- 会議時間、件名、場所
- **（Androidの場合）** 会議時間、空き時間、出席者、件名、場所、メモ
- **（iOSの場合）** 会議時間、件名、場所、メモ

Androidのオプション：



iOS オプション:

iOSカレンダーのエクスポートオプションの画像(/en-us/mobile-productivity-apps/media/export-calendar-ios-mdx-settings.png)

iOSの場合

Secure Mailからエクスポートされたカレンダーイベントは読み書き可能ですが、Secure Mailの外部で行われたイベントへの変更は利用できません。

重要:

- 次のいずれかに該当する場合、この機能はSecure Mailで表示されますが無効になります。
 - カレンダーエクスポートポリシーが**OFF**に設定されている。
 - お使いのMDXバージョンにポリシーが含まれていない
- 個人のカレンダーアプリにメールアカウントがすでに設定されており、iCloudアカウントが無効になっている場合、この機能は動作しません。個人のカレンダーアプリに他のアカウントが設定されていない場合、この機能は動作します。
- 個人のカレンダーからURLを起動してSecure Mailカレンダーイベントを編集するには、アプリURLスキームMDXポリシーに値**「ctxevent:」**が含まれていることを確認してください。

Androidの場合

Secure Mailからエクスポートされたカレンダーイベントは読み取り専用です。Secure Mailイベントを編集するには、カレンダーイベント内の**Secure Mail**イベントリンクをタップします。

重要:

- 次のいずれかに該当する場合、この機能はSecure Mailで表示されますが無効になります。

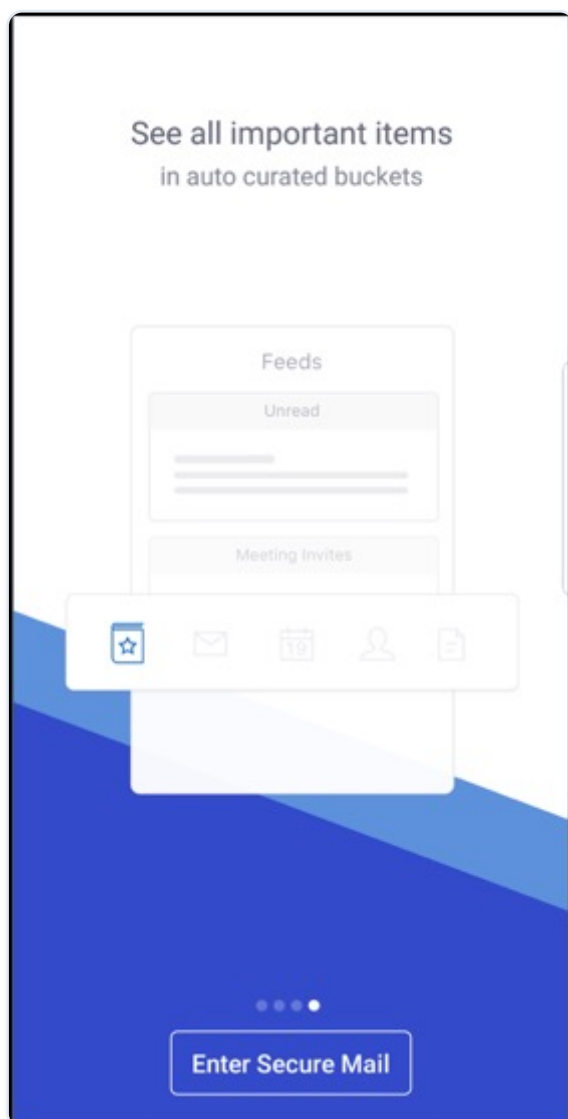
- カレンダーエクスポートポリシーが**OFF**に設定されている。
- お使いのMDXバージョンにはポリシーが含まれていません。
- インバウンドドキュメント交換MDXポリシーが**無制限**に設定されていることを確認してください。
- Secure Mailイベントリンクは、SamsungおよびHuaweiデバイスでは利用できません。

フィードフォルダー

Secure Mailは、すべての未読メール、注意が必要な会議の招待、および今後の会議をフィードフォルダーに表示します。

フィードカードを表示するには

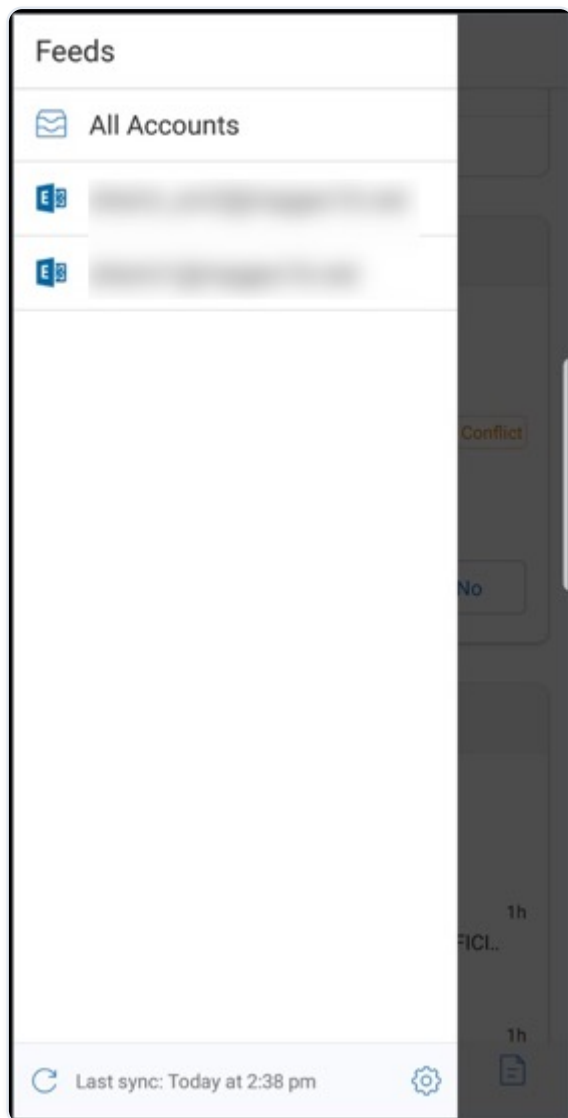
フッタータブバーの右下にあるフィードアイコンをタップします。



以下のフィードカードが表示されます。

- 未読
- 会議の招待
- 今後の会議

デフォルトでは、Secure Mailはプライマリアカウントからのフィードのみを表示します。複数のアカウントを設定している場合は、別のアカウントからのフィードを表示できます。他のアカウントからのフィードを表示するには、**フィード**をタップし、ハンバーガーアイコンをタップして、該当するアカウントを選択します。



フィードはアイテムのタイムスタンプに基づいてソートされ、以下の最大値で表示されます。

- 5件の未読メール
- 2件の会議招集
- 3件の今後の会議

フィードカード内のすべての項目を表示するには、**すべて表示**をタップします。

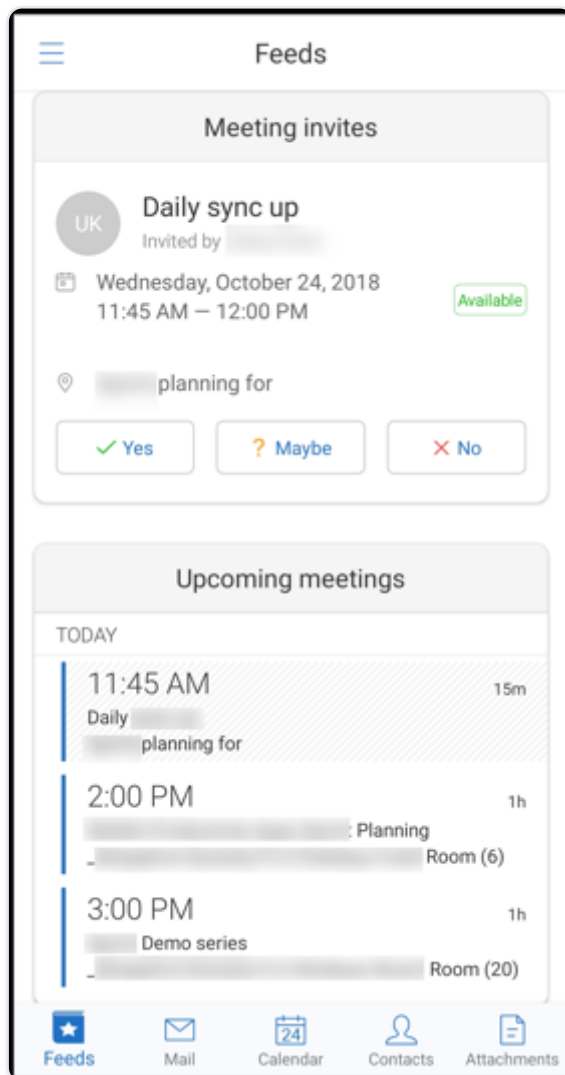
注:

各カードに表示されるフィードの数は、デバイスで設定したメール同期期間によって異なります。

フィードフォルダーの機能強化

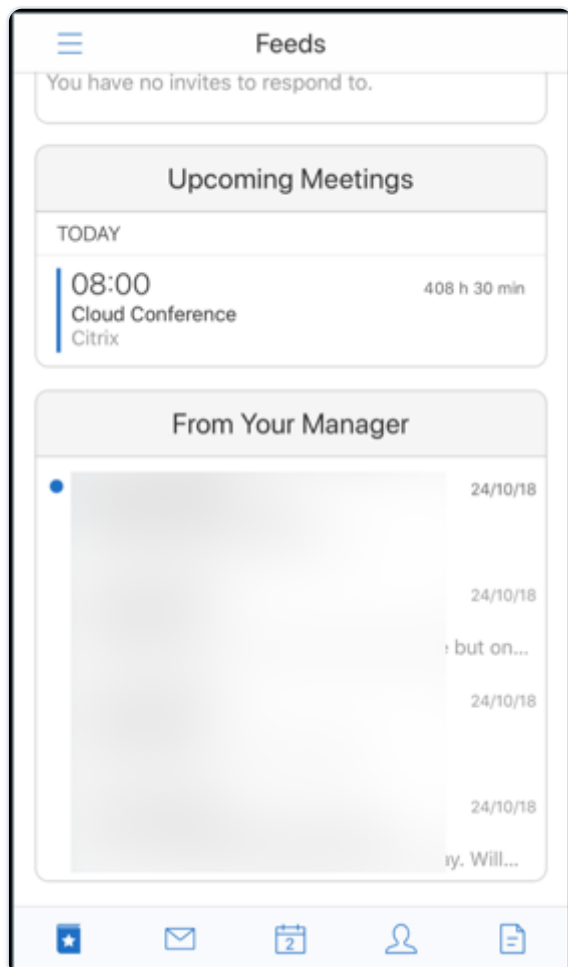
既存のフィードフォルダーに対する機能強化は次のとおりです。

- 自動同期されたすべてのフォルダーからの会議招集がフィードカードに表示されます。
- フィードカードで最大5件の今後の会議を表示できます。
- 今後24時間以内の会議はフィードカードに表示され、**今日**と**明日**のセクションに分類されます。



マネージャーからのフィード

Secure Mailでは、フィード画面でマネージャーからのメールを表示できます。メール同期期間の設定に基づいて、最大5件のメールがマネージャーからのフィードの下に表示されます。マネージャーからのメールをさらに表示するには、**すべて表示**をタップします。



前提条件:

Exchange ServerでExchange Web Services (EWS)が有効になっていることを確認してください。

マネージャーカードは、Active Directoryから取得された組織の詳細 (Outlook連絡先) に基づいて表示されます。マネージャーフィードに正しい詳細が表示されるようにするには、管理者がActive Directoryで組織階層を構成していることを確認してください。

注:

この機能はIBM Lotus Notesサーバーではサポートされていません。

カレンダーから会議に参加する

Secure Mailでは、ユーザーはカレンダーの招待から直接会議に参加できます。次の表に、サポートされている会議の種類と電話番号の形式、およびそれぞれのダイヤルイン要件を示します。

サポートされている会議の種類

会議の種類	識別要件	会議に参加をタップした後のアクション
マイクロソフト チームズ		Microsoft Teamsアプリがインストールされている場合、アプリが開き、ユーザーは会議に参加します。アプリがインストールされていない場合、ユーザーはアプリストアからMicrosoft Teamsをインストールするオプションが表示されます。
GoToMeeting (GTM)	会議コンテンツ内の次のいずれか: 1) この種類のURL: <code>https://www1.gotomeeting.com/join/1234567892</code> ; 2) 次のいずれかの形式のGTMアクセスコード: GTM: 123456789, GTM – 123456789, G2M – 123456789, G2M: 123456789	GTMアプリがインストールされている場合、アプリが開き、ユーザーは会議に参加します。アプリがインストールされていない場合、ユーザーはアプリストアにアクセスしてGTMをインストールするオプションが表示されます。 gotomeet.me/username形式のGTMの場合、アプリが開き、ユーザーは会議に参加します。
WebEx		Citrix Secure Web™が開き、デバイスにインストールされている場合は、ラップされていないWebExアプリが開きます。WebExは、AndroidのSecure Webの制限付きOpen-in例外リストと、iOSの許可されたURLポリシーに例外として追加する必要があります。

会議の種類	識別要件	会議に参加をタップした後のアクション
スカイプ フォー ビジネス		ユーザーはSecure Webで開くリンクをクリックでき、デバイスにインストールされている場合は、ラップされていないSkype for Businessアプリが開きます。Skype for BusinessアプリをAndroidのSecure Webの制限付きOpen-In例外リストポリシーに例外として追加します。iOSの許可されたURLポリシーに例外を追加します。

以下のポリシーリストを設定すると、ユーザーは会議リンクをタップして関連するアプリを開くことができます。

Microsoft Teamsアプリ

- ****iOS** - 「URLを許可」 ポリシー: `\^msteams:`
- ****Android** - 「オープンイン除外」 ポリシー: `{action=android.intent.action.VIEW scheme=msteams package=com.microsoft.teams}`

Zoomアプリ

- **iOS** - 「URLを許可」 ポリシー: `+^\zoomus:`
- **Android向け「Open-in除外」** ポリシー: `{action=android.intent.action.VIEW scheme=zoomus package=us.zoom.videomeetings}`

Webex (ラップされていないアプリ)

- **iOS** - 「URLを許可」 ポリシー: `+^\^wbx:` ポリシー文字列の例は `\^http;\^https;\^mailto:=ctxmail;,\^citrixreceiver;,\^telprompt;,\^tel;,\^col-g2m-2;,\^col-g2w-2;,\^wbx;,\^mmaps:ios\_addr:`
- **Android向け「Open-in除外」** ポリシー: `{action=android.intent.action.VIEW scheme=wbx package=com.cisco.webex.meetings}`

Skype for Business (スカイプ フォー ビジネス)

- **iOS** - 「URLを許可」 ポリシー: `+^\lync:`

- アンドロイド - 「Open-in 除外」ポリシー: {action=android.intent.action.VIEW scheme=lync package=com.microsoft.office.lync15}

Skype (スカイプ)

- iOS - 「URLを許可」ポリシー: +\^skype:
- Android - 「Open-inからの除外」ポリシー: {action=android.intent.action.VIEW scheme=skype package=com.skype.raider}

ダイヤルインの仕様

以下の一覧は、会議の種類と、それぞれでサポートされている電話番号形式および会議コード形式を示しています。

GoToMeeting (GTM):

サポートされている電話番号形式:

- GTM形式の任意の電話番号。例:
 - インド (フリーダイヤル): 000 800 100 7855
 - 米国 (フリーダイヤル): 1 877 309 2073
- RFC 3966形式の標準を満たす任意の電話番号。詳細については、[インターネット標準トラッキングプロトコル文書](#)を参照してください。

サポートされている会議コード形式:

会議コードは、会議本文内の以下のいずれかの形式から取得されます。

- URL (*.gotomeeting.com/join/123456789)
- URL (`gotomeet.me/username` 形式)
- "GTM:123456789" のような "GTM" 形式
- "G2M:123456789" のような "G2M" 形式
- "Access Code: 123456789" のような形式

WebEx:

サポートされている電話番号の形式:

- WebEx の通話形式の電話番号。例 (Verizon と米国):
 - 1-866-652-5088

- 1-517-466-3109
- WebEx の音声接続形式の電話番号。例:
 - 1-650-479-3207 (米国有料)
- RFC 3966 形式の標準を満たす電話番号。

サポートされている会議コードの形式:

会議のコンテンツには、次のいずれかの形式が含まれている必要があります。

- 会議番号: 123 456 789
- アクセスコード: 123 456 789

注:

会議コードが9桁以下の場合、会議にダイヤルインするために#キーが自動的に追加されます。

スカイプ フォー ビジネス

サポートされている電話番号の形式:

- RFC 3966形式の任意の電話番号。詳細については、[インターネット標準プロトコル文書](#)を参照してください。

サポートされている会議コードの形式:

会議本文には、次のテキストが含まれています: 「Conference ID: 123456789」

注:

Skype for Business会議の場合、#キーは自動的に追加されます。

一般的な音声会議情報

サポートされている電話番号の形式:

- RFC 3966形式の任意の電話番号。詳細については、[インターネット標準トラックプロトコル文書](#)を参照してください。例:
 - 5555555555

- (555) 555-5555
- 555-555-5555
- 555-555-555-5555 (国コードがある場合)
- 1-555-555-5555
- +1-555-555-5555

注：

電話番号の数字間には単一の区切り文字を使用してください。たとえば、「) -」を使用すると、番号が認識されない場合があります。

サポートされている会議コード形式：

推奨形式：「(電話番号)」、「(コード)」

必要に応じて、最大4つのコンマを指定し、#キーを提供できます。サポートされている形式のリストについては、このドキュメントの後の表を参照してください。

音声会議の場合、以下の形式ではユーザーが**ダイヤルイン**をタップできます。ただし、カレンダー会議の本文から電話番号をタップした場合、会議にダイヤルインできます。その場合、会議コードを手動で入力する必要があります。以下の電話番号と会議コードの形式がサポートされています。

サポートされている電話番号形式	会議コード区切り文字	例
RFC 3966形式の電話番号。 例: 5555555555; (555) 555-5555; 555-555-5555; 555-555-555-5555 (国コードの場合); 1-555-555-5555; +1-555-555-5555	参加者コード	1-888-999-9999 参加者コード: 9999999
	参加者PIN	1-888-999-9999 参加者PIN: 99999999
	ゲストコード	1-888-999-9999 ゲストコード: 99999999

サポートされている電話番号形式	会議コード区切り文字	例
	ゲストPIN	1-888-999-9999 ゲスト PIN:99999999
	参加者/ゲストコード	1-888-999-9999 参加者/ゲスト コード:99999999
	主催者コード	1-888-999-9999 主催者コー ド:99999999
	主催者PIN	1-888-999-9999 主催者 PIN:99999999
	議長コード	1-888-999-9999 議長コー ド:99999999
	議長PIN	1-888-999-9999 議長 PIN:99999999
	ホストPIN	1-888-999-9999 ホスト PIN:99999999
	PIN	1-888-999-9999 PIN:99999999
	アクセスコード	1-888-999-9999 アクセス コード:99999999
	コード	1-888-999-9999 コー ド:99999999
	会議コード	1-888-999-9999 会議コー ド:99999999
	会議ID	1-888-999-9999 会議 ID:99999999
	,	+1 (631) 992-3240,958209234#
	,	+1 (631) 992-3240,,958209234#

サポートされている電話番号形式	会議コード区切り文字	例
	,,,	+1 (631) 992-3240,,,958209234#
	,,,,	+1 (631) 992-3240,,,,958209234#
	パスコード	+1 (631) 992-3240 パスコード 958209234#
	内線	+1 (631) 992-3240 内線:958209234#
	内線.	+1 (631) 992-3240 内線 958209234#
	;内線=	+1 (631) 992-3240; 内線 958209234#
	内線	+1 (631) 992-3240 内線 958209234#
	HC	+1 (631) 992-3240 HC 958209234#
	内線	+1 (631) 992-3240 内線 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#

個人カレンダーのオーバーレイ

iOSおよびAndroidデバイスでは、ネイティブカレンダーアプリから個人カレンダーをインポートし、Secure Mailで個人のイベントを表示できます。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事[個人カレンダーイベントの表示](#)を参照してください。

インライン画像を挿入する

次の手順では、インライン画像を挿入する方法について説明します。

1. メールにインライン画像を添付するには、メール本文を長押しします。表示されるオプションから、[画像を挿入](#)をタップします。

画像を挿入オプションの画像(/en-us/mobile-productivity-apps/media/xenmobile-secure-mail-insert-image1.png)

2. Secure Mailは、写真へのアクセスを求める場合があります。写真ギャラリーが表示されます。ギャラリーに移動し、挿入したい画像をタップします。

フォトギャラリーの画像(/en-us/mobile-productivity-apps/media/xenmobile-secure-mail-insert-image2.png)

3. メールに選択した画像が挿入されました。

写真が挿入されたメッセージの画像(/en-us/mobile-productivity-apps/media/xenmobile-secure-mail-insert-image3.png)

スワイプアクション

iOSおよびAndroidデバイスでは、メールを左右にスワイプしてアクションを実行します。この機能に関するユーザーヘルプドキュメントについては、Citrixユーザーヘルプセンターの記事、[スワイプアクションの使用](#)を参照してください。

iOSおよびAndroidでSkype for Business会議に参加する

Secure Mailを介してSkype for Business会議にシームレスに参加できます。この機能を使用するには、Skype for Businessアプリがデバイスにインストールされている必要があります。

Skype for Business会議に参加するには

1. Skype for Business会議のリマインダーまたはカレンダーイベントをタップします。

2. イベントの詳細画面で、Skypeの会議に参加をタップします。Skype for Business会議が新しいウィンドウで開始されます。

デバイスにSkype for Businessがインストールされていない場合は、**Skype**をインストールをタップしてアプリをインストールします。

添付ファイルのアプリ内プレビューとその他の機能強化

QuickEditなどのサードパーティ製アプリを使用して開く代わりに、Secure Mailアプリ内で添付ファイル（MS Officeおよび画像）をプレビューできるようになりました。

添付ファイルを表示する際に、次の操作を実行できます。

- メールボックスから既存のメッセージを選択し、ファイルを添付します。
- 新しいメッセージを選択し、ファイルを添付します。
- オフラインアクセス用に添付ファイルを保存します。
- オフラインファイルから添付ファイルを削除します。
- 別のアプリケーションを使用して添付ファイルを開きます。
- 添付ファイルの元のメールまたはカレンダーイベントを表示します。

注：

添付ファイルリポジトリから添付ファイルを表示している場合にのみ、元のメールまたはカレンダーイベントを表示できます。

添付ファイルは、以下のケースでもプレビューできます。

- メッセージの表示中。
- 新しいメッセージの作成中。
- 添付ファイルフォルダー。
- カレンダーイベント。

ファイルを添付するメッセージを選択するには

1. 添付ファイル付きのメールを開きます。

添付ファイル付きメールの画像(/en-us/mobile-productivity-apps/media/inapp-preview.png)

2. 添付ファイルをタップします。

3. 添付アイコンをタップします。

受信トレイが表示されます。

受信トレイの画像(/en-us/mobile-productivity-apps/media/Attach-icon.png)

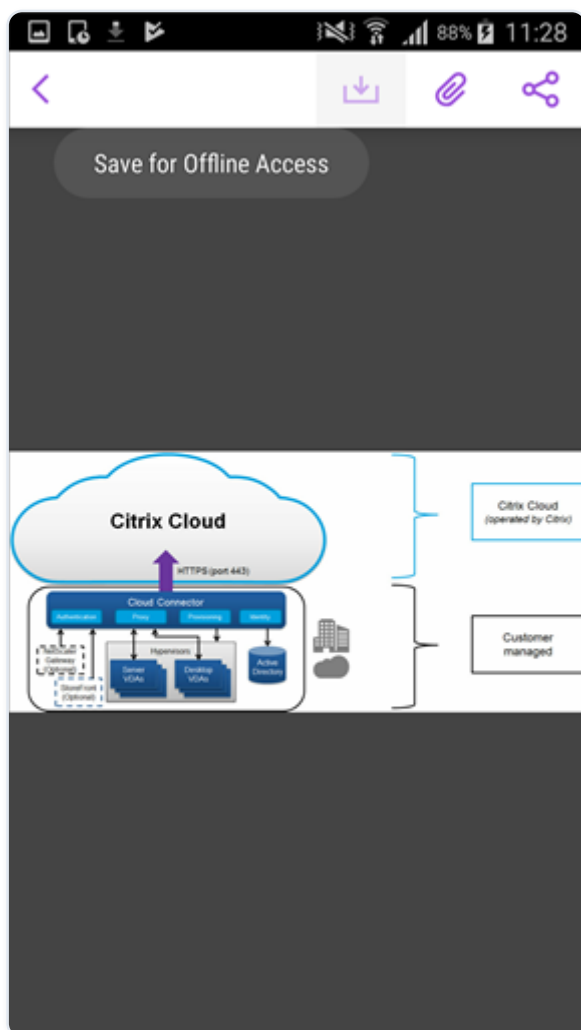
4. このファイルを添付する既存のメッセージを選択するか、**新しいメッセージ**をタップして新しいメッセージにこのファイルを添付します。

メッセージの画像(/en-us/mobile-productivity-apps/media/attach-inbox.png)

新しいメッセージの画像(/en-us/mobile-productivity-apps/media/add-to-new-mail.png)

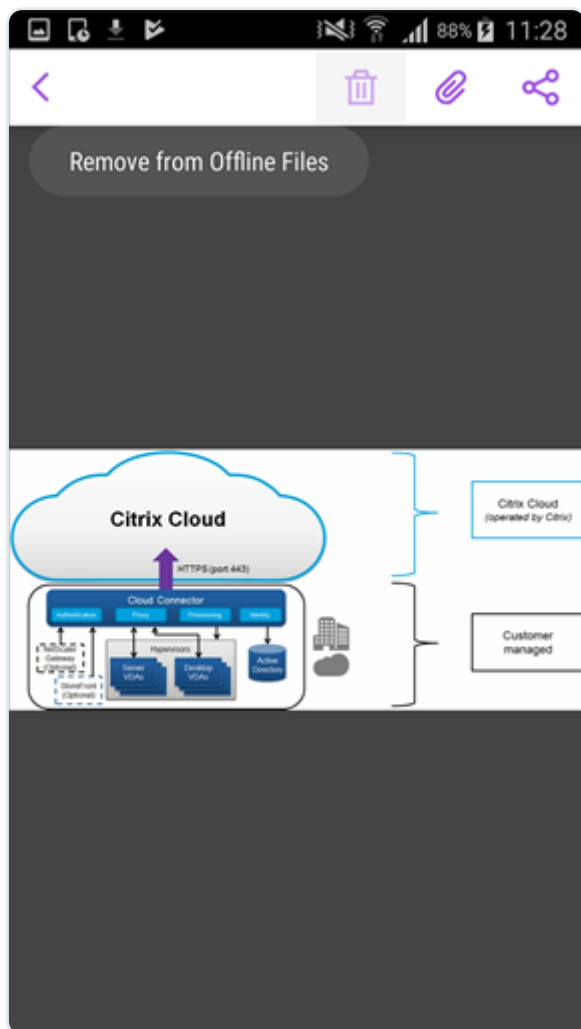
オフラインアクセス用に添付ファイルを保存するには

1. 添付ファイルを開きます。
2. ページの右上にある**その他**アイコンをタップし、**オフラインアクセス用に保存**をタップして、添付ファイルをオフラインアクセス用に保存します。



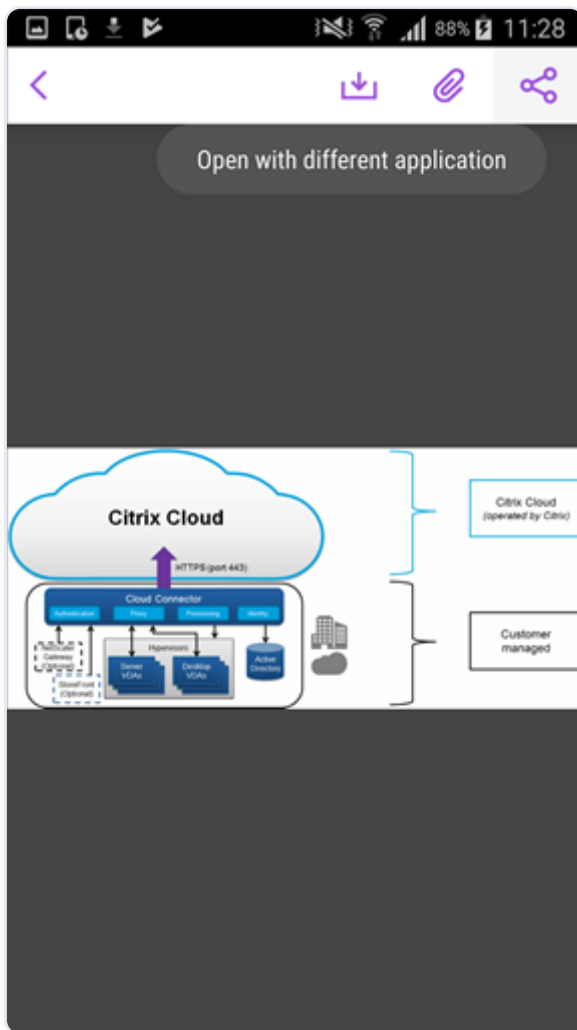
オフラインファイルから添付ファイルを削除するには

1. 添付ファイルを開きます。
2. ページの右上にある**その他**アイコンをタップし、**オフラインファイルから削除**をタップして、オフラインファイルから添付ファイルを削除します。

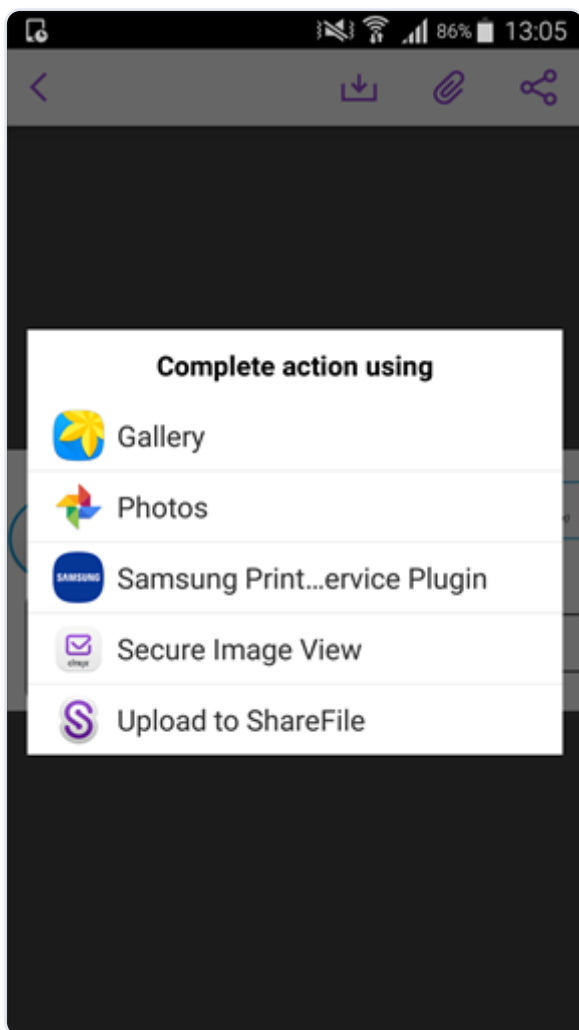


別のアプリケーションを使用して添付ファイルを開くには

1. 添付ファイルを開きます。
2. ページの右上にある**その他**アイコンをタップし、**別のアプリで開く**をタップして、別のアプリケーションを使用して添付ファイルを開きます。



3. 表示されるオプションの中から、添付ファイルを開きたいものをタップします。



添付ファイルの元のメールまたはカレンダーイベントを表示するには

1. 画面右下にある添付ファイルアイコンをタップします。
2. オフラインをタップします。

オフラインファイルの画像(/en-us/mobile-productivity-apps/media/OFFLINE-files.png)

3. 添付ファイルをタップし、画面右上のその他アイコンをタップします。

情報アイコンの画像(/en-us/mobile-productivity-apps/media/more-icon.png)

4. ソースメールが表示されます。

ソースメールの画像(/en-us/mobile-productivity-apps/media/inapp-preview.png)

ユーザー名をメールアドレス（UPN）に移行する

iOSおよびAndroid版Secure Mailでは、Exchangeのユーザー名とパスワードに基づく認証から、UPNとパスワードに基づく認証に移行できます。

この機能を有効にすると、以下の操作を行う必要がありません。

- Secure Mailを再インストールする。
- Secure Mailでアカウントを削除して追加する。
- Secure Mailでユーザー名を変更する。

前提条件

この移行を進める前に、ユーザーがSecure Mailバージョン10.7.25以降を実行していることを確認してください。この機能を使用するには、「Attempt Username Migration On Auth Failure」ポリシーを有効にする必要があります。

UPNベースの認証に移行するには

1. Endpoint Managementで「認証失敗時にユーザー名移行を試行する」ポリシーを有効にします。
2. Exchangeユーザーアカウントを、ユーザーのプライマリSMTPメールアドレスと一致する新しいUPNに移行します。これにより認証失敗がトリガーされます。Secure MailはプライマリSMTPメールアドレスを使用して認証を試行します。

認証が成功すると、ユーザーアカウントは更新されたUPNに移行されます。

移行を確認するには

iOSデバイスの場合: 設定に移動し、アカウントをタップして詳細を表示します。移行が成功すると、プライマリSMTPメールアドレスが**ACCOUNT画面のユーザー名フィールド**に表示されます。

Androidデバイスの場合: 設定に移動し、アカウントをタップして詳細を表示します。移行が成功すると、プライマリSMTPメールアドレスが**アカウントの詳細画面のユーザー名フィールド**に表示されます。

個人配布リスト

前提条件

- Exchange ServerでExchange Web Services (EWS) が有効になっていること。
- Microsoft Exchange Serverバージョン10 SP1以降。

iOSおよびAndroid版Secure Mailは、個人連絡先グループをサポートしています。Outlookデスクトップクライアントで作成した連絡先グループをSecure Mailで表示できます。作成した連絡先グループは、Secure Mailの連絡先に表示されます。

注:

Secure Mailでは、ネストされた連絡先グループのメンバーを表示することはできません。

メールを作成したり、カレンダーイベントを作成したりする際に、個人配布リストを使用できます。Exchangeを使用して個人連絡先グループ（配布リスト）を作成した場合、Secure Mailでそのリストを表示できます。

個人の配布リストを表示するには

1. Secure Mail で、**連絡先**を開きます。
2. 連絡先グループの名前を入力します。検索結果にグループが表示されます。
3. 連絡先グループをタップしてメンバーを表示します。

連絡先グループの画像(/en-us/mobile-productivity-apps/media/iOS-group-expanded.png)

注

Secure Mail では連絡先グループを編集できません。

連絡先グループにメールを作成するには

1. Secure Mail を開き、**編集**フローティングアクションボタンをタップしてメールを作成します。
2. **新規メッセージ**画面で、****宛先:****フィールドに連絡先グループの名前を入力します。
3. 表示される連絡先リストから、連絡先グループを選択します。

連絡先リストの画像(/en-us/mobile-productivity-apps/media/iOS-message-compose-PDL.png)

連絡先グループは次のアイコンで示されます。

連絡先グループアイコンの画像(/en-us/mobile-productivity-apps/media/contact-group-icon.png)

連絡先グループにカレンダー招待を送信するには

1. Secure Mailを開き、**カレンダー**に移動します。
2. *******アイコンをタップして、カレンダーイベントを作成します。
3. **新規イベント**画面で、**招待者**をタップしてメンバーを追加します。

4. 連絡先グループの名前を入力して、グループに招待を送信します。

連絡先グループ名の画像(/en-us/mobile-productivity-apps/media/iOS-calendar-invite-PDL.png)

5. 表示される連絡先リストから、連絡先グループを選択します。

フォルダーの同期

iOSおよびAndroid版Secure Mailでは、**同期**アイコンをタップしてすべてのSecure Mailコンテンツを更新できます。**同期**アイコンは、メールボックス、カレンダー、連絡先、添付ファイルなどのSecure Mailのスライドアウトに表示されます。**同期**アイコンをタップすると、メールボックス、カレンダー、連絡先など、自動更新するように構成したフォルダーが更新されます。最終同期のタイムスタンプは、**同期**アイコンの横に表示されます。

フォルダーを同期するには

1. Secure Mailを開きます。
2. フッタータブバーの使用可能なフォルダーから、同期したいフォルダーをタップします。

フッタータブの画像(/en-us/mobile-productivity-apps/media/footerbar.png)

3. 画面左上のハンバーガーアイコンをタップします。
4. 画面左下の**同期**アイコンをタップします。

フォルダー同期の画像(/en-us/mobile-productivity-apps/media/Folder-Sync.jpg)

同期の進行状況の画像(/en-us/mobile-productivity-apps/media/Sync-progress.jpg)

5. フォルダーが同期され、コンテンツが更新されます。タイムスタンプは**同期**アイコンの横に表示されます。

写真添付機能の改善

iOSおよびAndroid版Secure Mailでは、新しい**ギャラリー**アイコンをタップすることで、簡単に写真を添付できます。

メールに写真を添付するには

1. Secure Mailを開きます。
2. メールを作成するには**作成**をタップするか、メールに返信する**返信**フローティングアクションボタンをタップします。
3. 画面の右下にある**添付ファイル**アイコンの横にある**ギャラリー**アイコンをタップします。

ギャラリーアイコンの画像(/en-us/mobile-productivity-apps/media/photo-attachment-gallery-icon.jpg)

4. 画面の下部にギャラリーが表示され、**カメラアイコン**と**最近アイコン**も表示されます。
5. ギャラリーから添付したい画像に移動して選択するか、または**カメラアイコン**をタップして写真を撮ります。

画像の選択オプションの画像(/en-us/mobile-productivity-apps/media/select-images.png)

注：

添付ファイルアイコンをタップすると、次のオプションが表示されます。

- ファイル
- ShareFile (現在はCitrix Files)
- メール添付ファイルから 添付ファイルオプションの画像(/en-us/mobile-productivity-apps/media/Photo-Attachment-options.jpg)

Secure Mailはメール表示中に埋め込みリソースをレンダリングします

リソースが社内ネットワークに存在する場合（内部リンクである画像URLを含むメールなど）、Secure Mailは社内ネットワークに接続してコンテンツを取得し、レンダリングします。

最新の認証のサポート

最新の認証は、ユーザー名とパスワードを使用したOAuthトークンベースの認証です。このサポートには、社内外のActive Directory Federation Services (AD FS) またはIDプロバイダー (IdP) 向けのOffice 365のサポートが含まれます。

Secure MailのSecure WebドメインMDXポリシーを許可する

Secure Mailでは、一部の外部URLはSecure Webではなくネイティブブラウザで開く必要があります。その結果、デフォルトではすべてのURLがネイティブブラウザで開きます。ただし、Secure Webで開きたいURLのリストを作成できます。これを行うには、Citrix Endpoint Managementコンソールで「許可されたSecure Webドメイン」というMDXポリシーを構成します。

ポリシーを展開すると、コンマ区切りのURLホストドメインのリストが、アプリケーションが通常外部ハンドラに送信するURLのホスト名部分と照合されます。通常、このポリシーはSecure Webが処理する内部ドメインのリストとして構成します。

ポリシーを空白のままにした場合（これがデフォルト設定です）、URLをフィルタリングから明示的に除外するか、またはURLをリダイレクトしない限り、すべてのWebトラフィックはSecure Webに送信されます。URLをリダイレクトするには、ドメインMDXポリシーのURLフィルター除外を構成します。このポリシーは、ネイティブブラウザで開く必要があるURLを示します。このポリシーはSecure Webドメインポリシーよりも優先されます。

これらのMDXポリシーはAndroidおよびiOS向けに構成できます。

Secure Webドメインポリシーの構成例

次の手順では、Android版Secure Mailのユーザーに、ネイティブのChromeブラウザまたはSecure WebでURLを開くよう促す方法を示します。iOSでは、通常Safariブラウザで開くURLがSecure Webで自動的に開くことを示します。

Android版Secure Mailの場合

1. 「アプリインタラクション」ポリシーリストの「制限付きOpen-In例外リスト」に、
*{package=com.android.chrome}*と入力します。
2. アプリインタラクション（アウトバウンドURL）ポリシーリストの**Secure Webドメイン**を許可に、内部サイトのDNSサフィックスを追加します。

その他のサードパーティ製ブラウザの場合は、以下の形式を適宜使用してください。

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

iOS版Secure Mailの場合

1. 「アプリインタラクション（アウトバウンドURL）」ポリシーリストの**許可されたURL**に、*+
^safari:*を追加します。
2. **アプリURLスキーム**に、*safari:*を追加します。
3. **Secure Webドメイン**を許可に、内部サイトのDNSサフィックスを追加します。

Secure Mail と Slack の統合

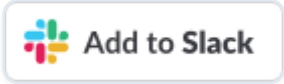
Citrix Secure Mail and its integration with Slack is not created by, affiliated with, or supported by Slack Technologies, Inc.

iOS または Android を実行しているデバイスで、メールの会話を Slack アプリに引き継ぐことができるようになりました。

この機能を有効にすると、次のことができます。

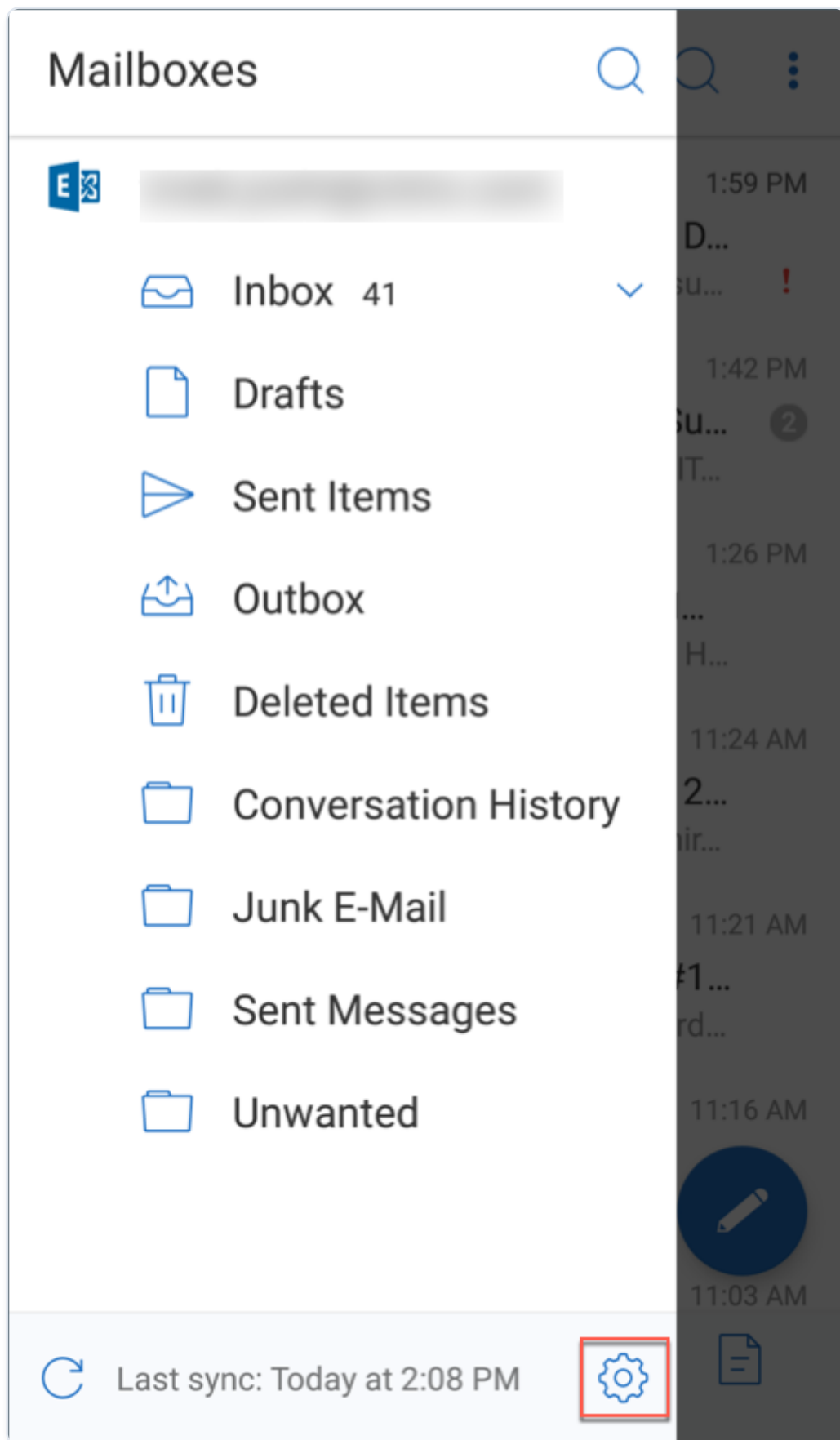
- メールから Slack の会話にシームレスに切り替える。
- メールの受信者と Slack グループ会話を作成する。
- メールの受信者と Slack でダイレクトメッセージを作成する。

前提条件

- 管理者向け:
 - Secure Mail が Slack ワークスペースにインストールされていることを確認します。以下の **Slack に追加** ボタンをクリックします。
 - **Slack を有効にする** ポリシーが **オン** になっていることを確認します。ポリシーの詳細については、以下を参照してください。
 - [iOS 用 Slack 有効化ポリシー](#)
 - [Android 用 Slack 有効化ポリシー](#)
- ユーザー向け: 続行する前に、Slack アカウントがあり、Slack アプリがデバイスにインストールされていることを確認してください。

デバイスでこの機能を有効にするには

1. Secure Mailを開き、ハンバーガーアイコンをタップします。
2. メールボックス画面で、画面右下にある設定アイコンをタップします。



3. 設定画面で、統合の下に表示されている**Slack**をタップします。

Settings

Done

ACCOUNTS



+

Add Exchange Account

INTEGRATIONS



Slack (Preview)

☐

GENERAL

Notifications

>

Auto Refresh

On

Out of Office

Off

MAIL

Ask Before Deleting

☒

Organize by Conversation

☒

Load Attachments on WiFi

☐

Show Pictures

☐

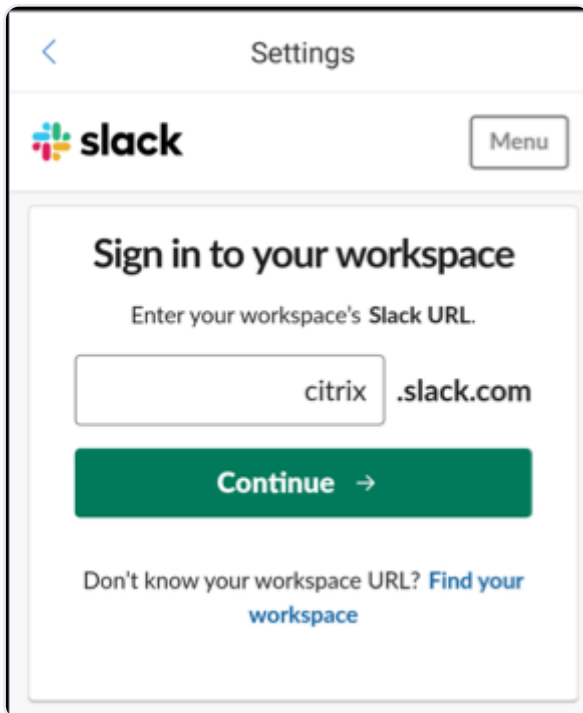
Sync Mail Period

3 days

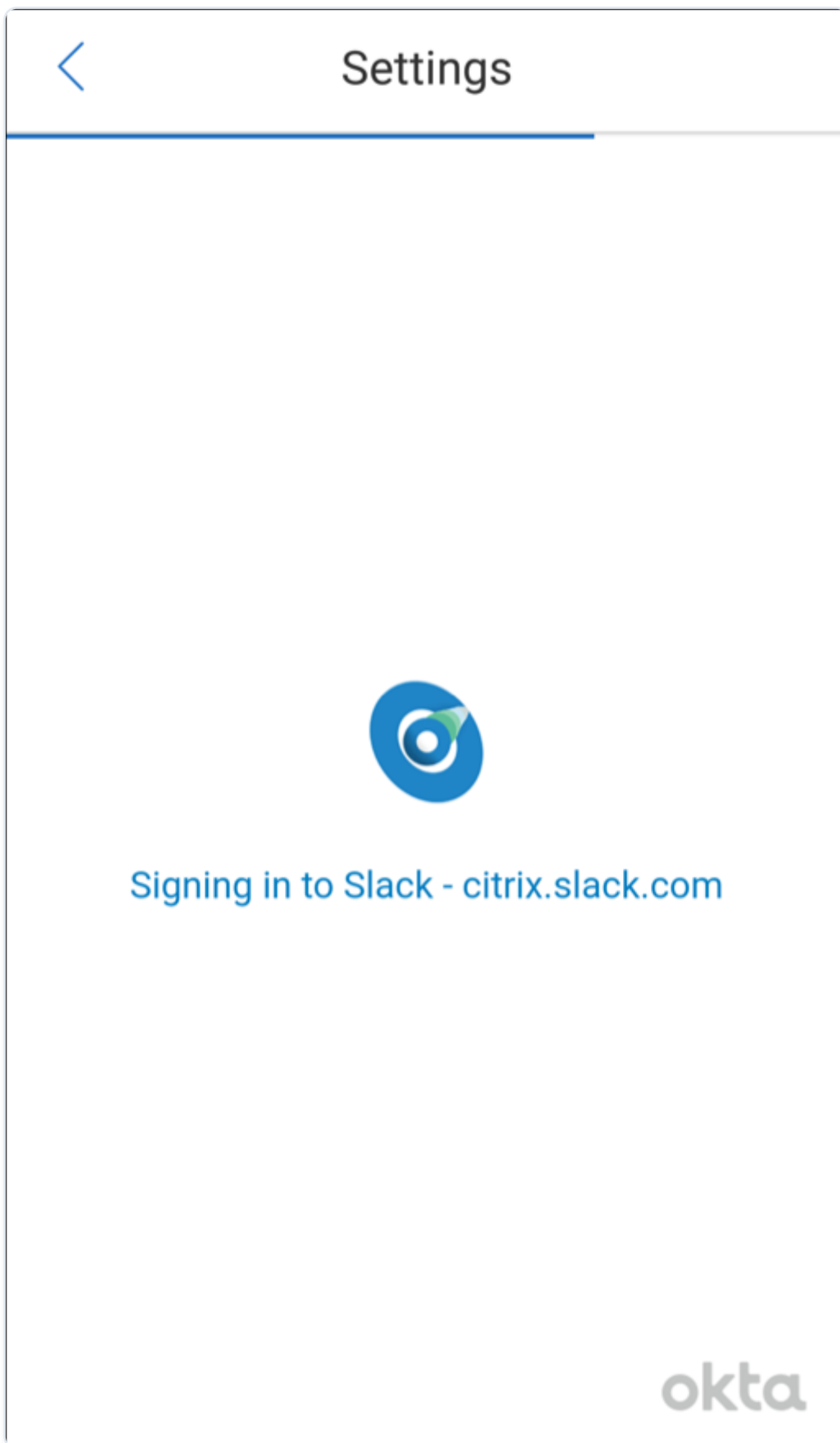
Check Spelling

☒

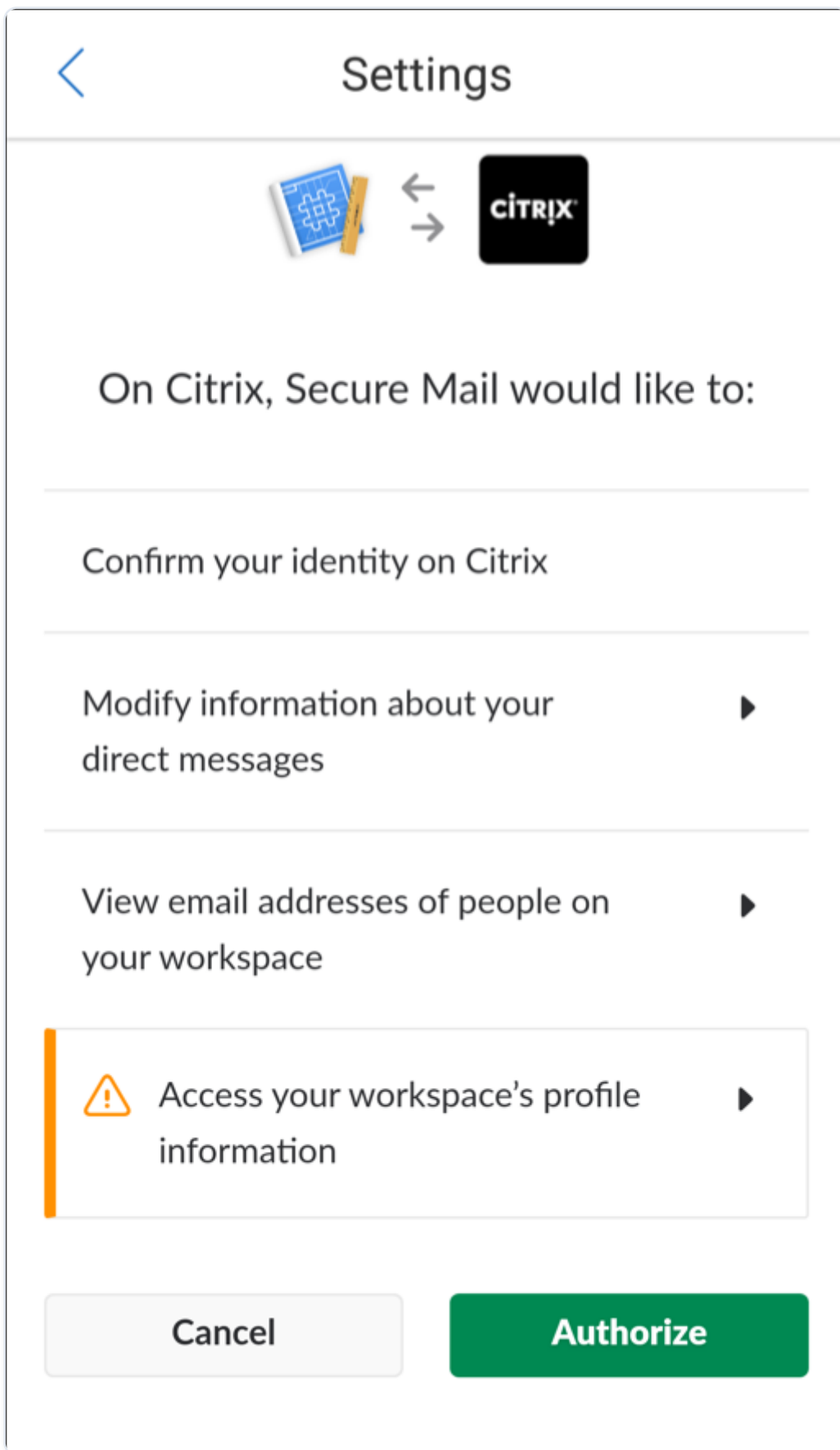
- ワークスペースのSlack URLを入力し、次に**続行**をタップします。

A screenshot of the Slack mobile app's 'Settings' screen. At the top, there's a back arrow and the word 'Settings'. Below that is the Slack logo and a 'Menu' button. The main heading is 'Sign in to your workspace'. Underneath, it says 'Enter your workspace's Slack URL.' There is a text input field containing 'citrix' followed by '.slack.com'. Below the input field is a green button with the text 'Continue →'. At the bottom, there is a link that says 'Don't know your workspace URL? Find your workspace'.

- 資格情報を入力し、次に**サインイン**をタップします。



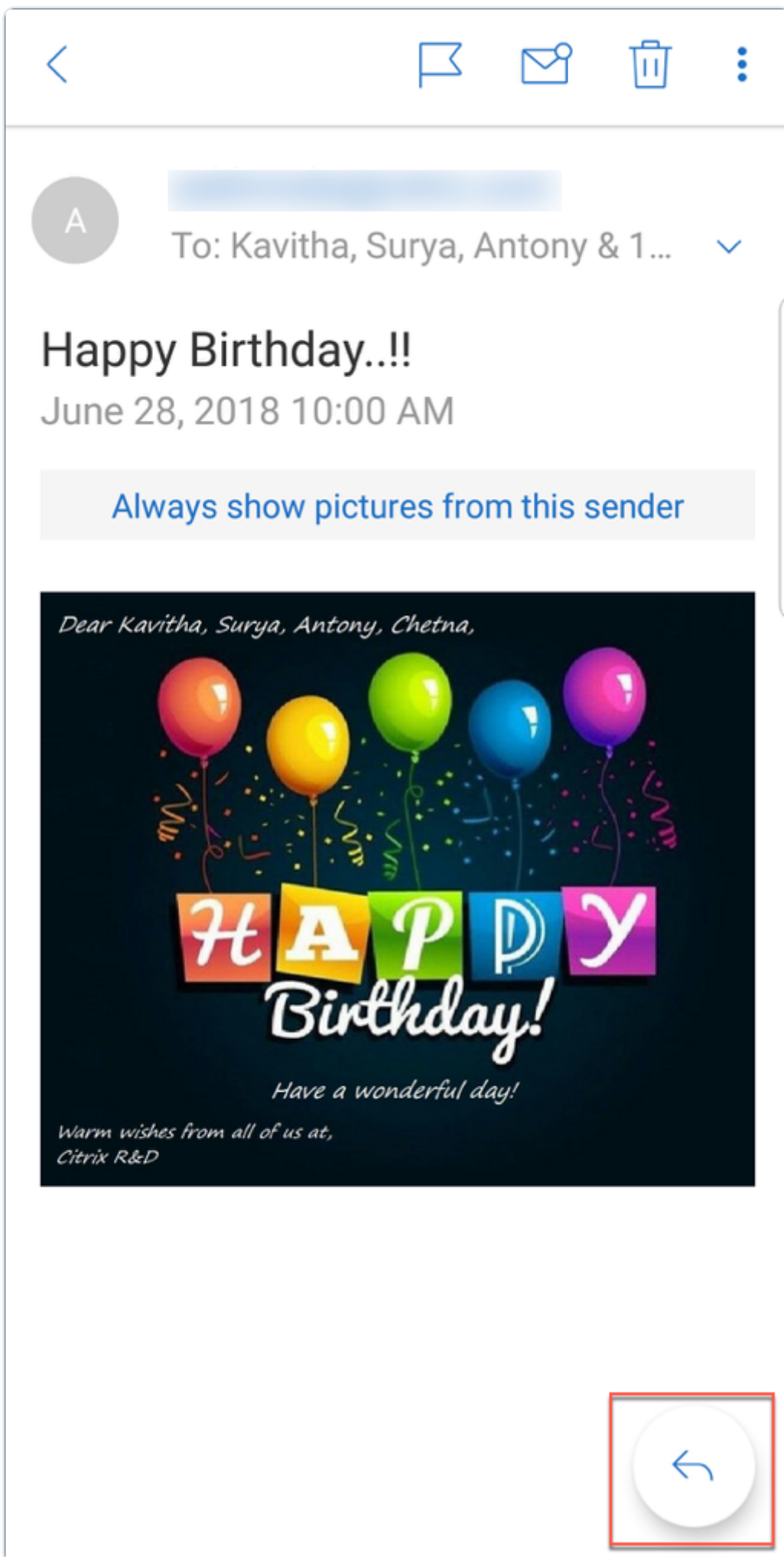
6. Secure Mailが情報へのアクセスを承認するよう求められたら、**承認**をタップします。



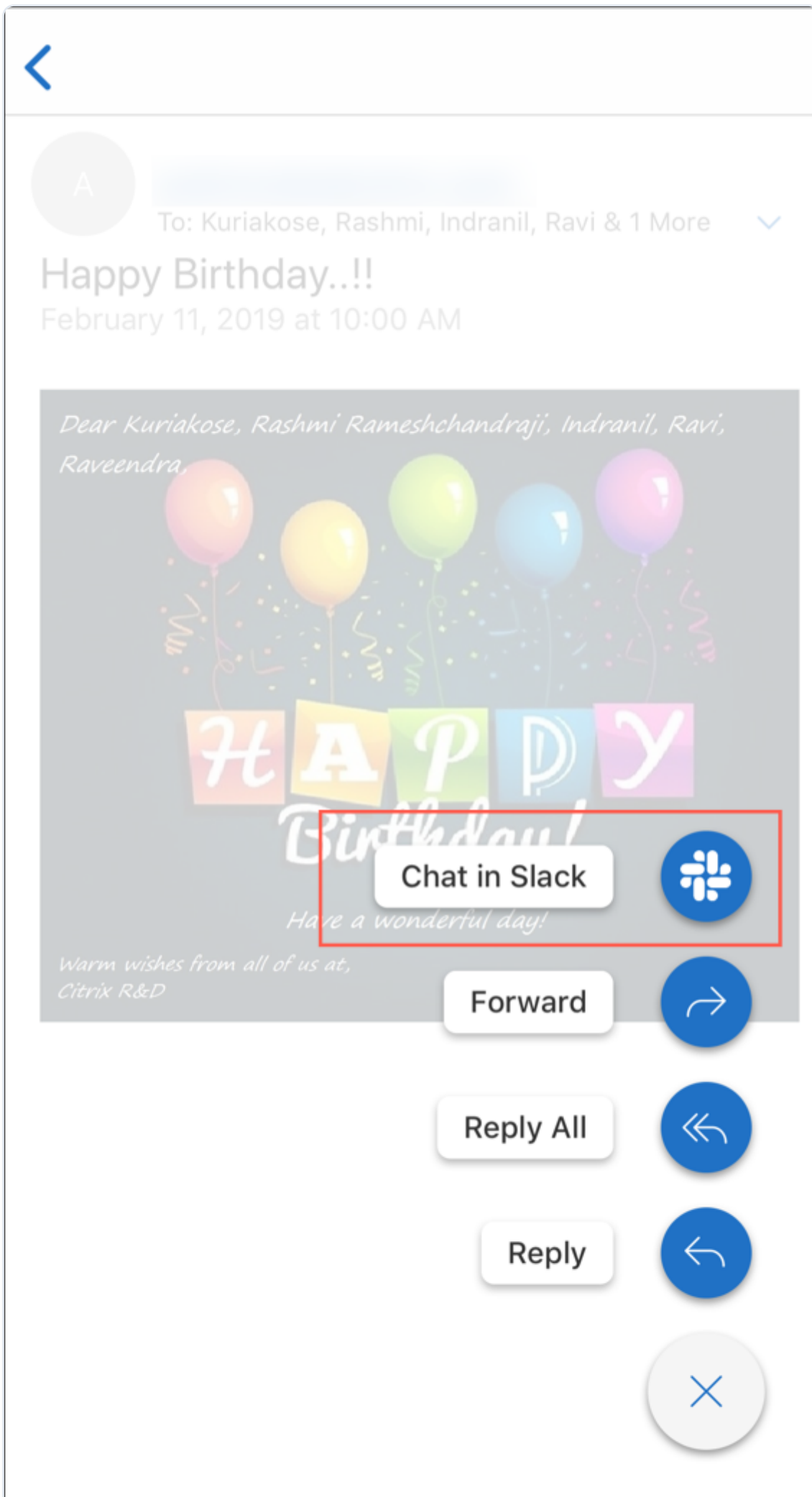
これでSlackに接続されました。

この機能を使用するには

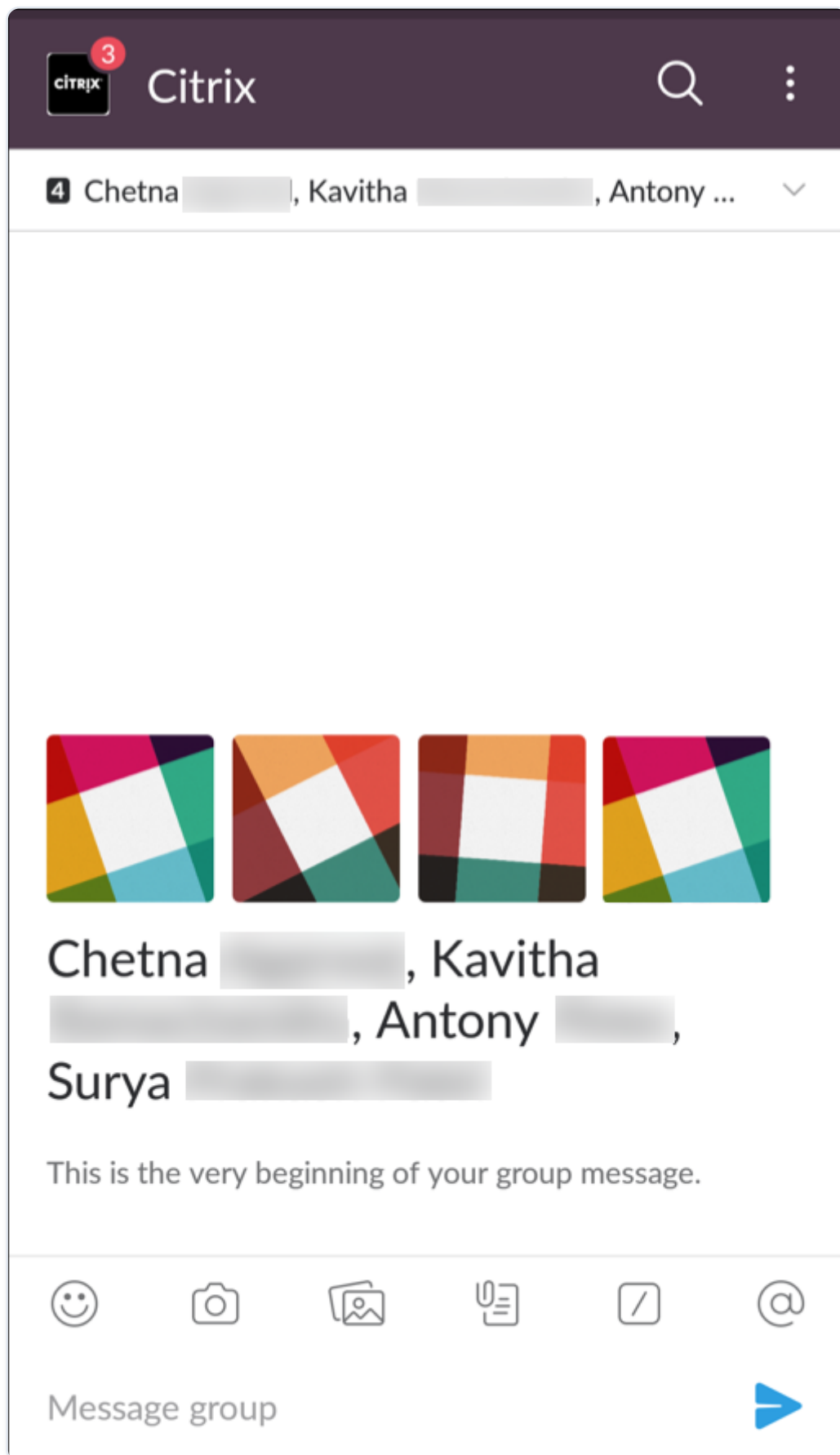
1. Secure Mailで任意のメール会話を開き、次にフローティングアクションボタンをタップします。



2. 利用可能なオプションから、**Slackでチャット**をタップします。



3. 会話は、メールの受信者とともにSlackに切り替わります。



次の点に注意してください。

- iOSまたはAndroid版Secure Mailを実行しているデバイスでは、メールから最大8人の受信者とSlackの会話を作成できます。メールに8人を超える受信者がいる場合、Secure Mailはデフォルトで、メールの会話に存在する最初の8人の受信者を選択します。

通知と同期

この記事では、Secure Mail の通知とメール同期の機能および構成について説明します。

iOS の Secure Mail のバックグラウンドアプリ更新

Secure Mail for iOS が、iOS のバックグラウンドアプリ更新（APNs ではない）を介して通知を提供するように構成されている場合、Secure Mail のメール更新は次の方法で機能します。

- ユーザーがデバイスの **設定** メニューから **App のバックグラウンド更新** を有効にし、Secure Mail がバックグラウンドで実行されている場合、メールはサーバーと同期されます。同期の頻度はさまざまな要因によって異なります。
- ユーザーが **App のバックグラウンド更新** を無効にすると、アプリはバックグラウンドで実行されている間、メールを受信することはありません。
- ユーザーが Secure Mail をバックグラウンドに移動すると、アプリは一時停止されるまでの猶予期間中、実行を継続します。
- フォアグラウンドで実行されている間、Secure Mail は **App のバックグラウンド更新** の設定に関係なく、リアルタイムのメールアクティビティを表示します。

セキュアメールとアクティブシンク

Secure Mail は、ActiveSync メッセージングプロトコルを介して Exchange Server と同期します。この機能により、ユーザーは Outlook のメール、連絡先、カレンダーイベント、自動生成されたメールボックス、およびユーザーが作成したフォルダーにリアルタイムでアクセスできます。

注:

ActiveSync は Exchange パブリックフォルダーの同期をサポートしていません。Exchange Server 2013 では、ActiveSync は下書きフォルダーを同期しません。

ユーザーが作成したフォルダーを同期するには、次の手順に従います。

iOS

1. **設定 > 自動更新** に移動します。

2. 「**自動更新**」を「**オン**」に設定します。
3. 「**オン**」をタップします。すべてのメールボックスのリストが表示されます。
4. 同期したいフォルダーをタップします。

アンドロイド

1. メールボックスリストに移動します。
2. 同期したいメールボックスをタップします。
3. 右下隅にある「その他」アイコンをタップします。
4. 「**同期オプション**」をタップします。
5. 「**確認頻度**」の下で、フォルダーを同期する頻度を選択します。

Secure Mailでの連絡先のエクスポート

Secure Mailユーザーは、連絡先を電話のアドレス帳と継続的に同期したり、個々の連絡先を電話のアドレス帳に一度だけエクスポートしたり、連絡先をvCard添付ファイルとして共有したりできます。

これらの機能を許可するには、Endpoint ManagementコンソールでSecure Mailの「連絡先のエクスポート」ポリシーを「**オン**」に設定します。

ポリシーが「**オン**」の場合、Secure Mailで次のオプションが有効になります。

- 設定の「**ローカル連絡先と同期**」
- 個々の連絡先のエクスポート
- vCard添付ファイルとして連絡先を共有する

連絡先のエクスポートポリシーがオフに設定されている場合、これらのオプションはアプリに表示されません。

ポリシーが有効になっている場合、メールサーバーから電話のアドレス帳に連絡先を継続的に同期するには、ユーザーは**ローカル連絡先と同期**を**オン**に設定する必要があります。**ローカル連絡先と同期**が**オン**である限り、ExchangeまたはSecure Mailの連絡先への更新は、ローカル連絡先の更新をトリガーします。

Androidの制限により、任意のExchangeまたはHotmailアカウントがすでにローカル連絡先と同期するように設定されている場合、Secure Mailは連絡先を同期できません。

iOSでは、Secure Mailの連絡先は電話の連絡先とエクスポートおよび同期できます。ユーザーがデバイスにHotmailまたはExchangeを設定している場合でも、連絡先をエクスポートおよび同期できます。この機能は、Endpoint ManagementでSecure Mailの「ネイティブ連絡先チェックのオーバーライド」ポリシーを通じて構成します。このポリシーは、Secure Mailがネイティブの連絡先アプリで構成されたExchange/Hotmailアカウントからの連絡先のチェックをオーバーライドするかどうかを決定します。**オン**の場合、ネイティブの連絡先アプリがExchange/Hotmailアカウントで構成されていても、アプリは連絡先をデバイスに同期します。**オフ**の場合、アプリは連絡先の同期をブロックし続けます。デフォルトは**オン**です。

制限事項:

ローカル連絡先と同期を有効にすると、デフォルトの連絡先フォルダーのみが同期されます。存在する可能性のあるサブフォルダーは、同期された連絡先には含まれません。

Secure Mailの通知

次の表に、Secure Mailがフォアグラウンドまたはバックグラウンドで実行されている場合の、サポートされているモバイルデバイスでの通知の処理方法を示します。

SECURE MAILがフォアグラウンドまたはバックグラウンドで実行されている場合	iOSでの通知の処理	ANDROIDでの通知の処理
フォアグラウンド	Secure Mailは、メールとカレンダーのアクティビティを同期するために、永続的なActiveSync接続を維持します。	Secure Mailは、メールとカレンダーのアクティビティを同期するために、永続的なActiveSync接続を維持します。
バックグラウンド (または終了)	Secure Mail は、iOS のバックグラウンドアプリ更新機能、または構成されている場合は APN を介して通知を受信します。	Secure Mail は永続的なActiveSync 接続を維持します。

構成の詳細については、「[iOS 用 Secure Mail のプッシュ通知](#)」を参照してください。

Secure Mail のプッシュ通知

iOS 版 Secure Mail と Android 版 Secure Mail は、アプリがバックグラウンドで実行されているとき、または閉じているときに、メールとカレンダーのアクティビティに関する通知を受信できま

す。iOS 版 Secure Mail は、Apple Push Notification service (APNs) を介して提供されるリモートプッシュ通知をサポートしています。Android 版 Secure Mail は、Firebase Cloud Messaging service (FCM) を介して提供される通知をサポートしています。

プッシュ通知の仕組み

iOS および Android 用のプッシュ通知を提供するために、Citrix® は Amazon Web Services (AWS) 上でリスナーサービスをホストし、以下の機能を実行します。

- 受信トレイのアクティビティがあるときに Exchange Server から送信される Exchange Web Services (EWS) プッシュ通知をリッスンします。Exchange はメールコンテンツを Citrix サービスに送信しません。

Citrix サービスによって個人を特定できる情報は保存されません。代わりに、デバイストークンとサブスクリプション ID が、Secure Mail 内で更新される特定のデバイスと受信トレイフォルダーを識別します。

- バッジカウントのみを含む APNs 通知を、iOS デバイス上の Secure Mail に送信します。
- FCM 通知を Android デバイス上の Secure Mail に送信します。

Citrix リスナーサービスは、ユーザーデバイスと Exchange Server 間で ActiveSync を介して流れ続けるメールデータトラフィックに影響を与えません。高可用性と災害復旧のために構成されたリスナーサービスは、次の3つのリージョンで利用できます。

- 米州
- ヨーロッパ、中東、アフリカ (EMEA)
- アジア太平洋 (APAC)

プッシュ通知のシステム要件

Citrix Gateway の構成に Secure Ticket Authority (STA) が含まれており、スプリットトンネリングが無効になっている場合、Citrix Gateway は、Secure Mail からトンネルされたトラフィックを以下の Citrix リスナーサービス URL に許可する必要があります。

リージョン	URL	IPアドレス
南北アメリカ	<code>https://us-east-1.pushreg.xm.citrix.com</code>	52.7.65.6; 52.7.147.0

リージョン	URL	IPアドレス
EMEA	<code>https://eu-west-1.pushreg.xm.citrix.com</code>	54.154.200.233; 54.154.204.192
APAC	<code>https://ap-southeast-1.pushreg.xm.citrix.com</code>	52.74.236.173; 52.74.25.245

プッシュ通知のためのSecure Mailの構成

アプリストア配布用のSecure MailでAppleプッシュ通知またはFCMを設定するには、Endpoint Managementコンソールで、を**ON**に設定し、地域を選択します。次の図は、iOSの設定を示しています。

Endpoint Managementのプッシュ通知設定の画像(/en-us/mobile-productivity-apps/media/public-app-store-push-notifications.png)

Androidの場合、次の図はiOSと同じ**プッシュ通知設定**を示しています。さらに、EWSがメールサーバーが存在する地域とは異なる地域でホストされている場合は、**EWSホスト名**の設定を完了してください。デフォルト設定は空です。この設定を空のままにすると、Endpoint Managementはメールサーバーのホスト名を使用します。

Endpoint ManagementにおけるAndroidのプッシュ通知設定の画像(/en-us/mobile-productivity-apps/media/android-push-notification.jpg)

トラフィックがリスナーサービスに流れるように、ExchangeとCitrix ADCを設定します。

Exchange Serverの構成

ファイアウォールから、Exchange Serverが配置されているリージョンのCitrixリスナーサービスURLへのアウトバウンドSSL（ポート443経由）を許可します。例：

リージョン	URL	IPアドレス
米州	<code>https://us-east-1.mailboxlistener.xm.citrix.com</code>	52.6.252.176; 52.4.180.132

リージョン	URL	IPアドレス
EMEA	<code>https://eu-west-1.mailboxlistener.xm.citrix.com</code>	54.77.174.172; 52.17.147.220
APAC	<code>https://ap-southeast-1.mailboxlistener.xm.citrix.com</code>	52.74.231.240; 54.169.87.20

Exchange Web Services (EWS) と Citrix リスナーデバイスの間にプロキシサーバーがある場合、次のいずれかを実行できます。

- EWS トラフィックをプロキシ経由でリスナーデバイスに送信します。
- プロキシをバイパスし、EWS トラフィックをリスナーデバイスに直接ルーティングします。

プロキシサーバー経由で EWS トラフィックを送信するには、ClientAccess\exchweb\ews フォルダーにある EWS の web.config ファイルを次のように構成します。

```
<configuration>

<system.net>

<defaultProxy>

<proxy usesystemdefault="true" bypassonlocal="true" />

</defaultProxy>

</system.net>

</configuration>
```

プロキシの構成の詳細については、「[プロキシ構成](#)」を参照してください。

Exchange 2013 環境の場合、`system.net` セクションを web.config ファイルに手動で追加する必要があります。それ以外の場合、この記事で説明されている構成は Exchange 2013 で機能するはずですが、トラブルシューティングについては、Exchange 管理者にお問い合わせください。

プロキシサーバーをバイパスするには、バイパスリストを構成して、Exchange が Citrix リスナーサービスに接続できるようにします。

Secure Hub が証明書ベースの認証で登録されている場合、Exchange Server も証明書ベースの認証用に構成する必要があります。詳細については、「[Endpoint Management Advanced Concepts](#)」の記事を参照してください。

Citrix Gateway の構成

Exchange Server はリスナーサービスへのトラフィックを許可する必要がありますが、Citrix ADC は登録サービスへのトラフィックを許可する必要があります。これにより、デバイスはプッシュ通知の登録に接続できます。

EWS サーバーと ActiveSync サーバーが異なる場合は、Citrix ADC トラフィックポリシーを構成して EWS トラフィックを許可します。Citrix Endpoint Management と Citrix Gateway の統合の詳細については、「[Citrix Gateway および Citrix ADC との統合](#)」セクションを参照してください。

トラブルシューティング

送信接続のトラブルシューティングを行うには、Exchange イベントログを確認します。これには、サブスクリプション要求またはサブスクリプションの通知が無効であるか失敗した場合のログエントリが含まれます。Exchange Server で Wireshark トレースを実行して、Citrix リスナーサービスへの送信トラフィックを追跡することもできます。

Secure Mail プッシュ通知に関する FAQ

Android は Secure Mail に通知をいつ配信しますか？

Android では、通知は常に Secure Mail に配信されます。

FCM は、ロック画面に表示されるメール通知にどのように影響しますか？

デバイスのロック画面に表示される新着メール通知は、Secure Mail によってデバイスに同期されたデータに基づいて生成されます。重要な点として、この情報はリスナーサービスから提供されるものではありません。

新着メール通知を表示するには、Secure Mail が Exchange からデータを同期できる必要があります、それによって Secure Mail が通知を作成するための情報を利用できるようになります。

新しいメールを受信すると、**新しいメッセージがあります** という FCM 通知が表示されます。バックグラウンドでメールの同期が完了すると、Secure Mail に新しいメールが表示されます。

APNs は、ロック画面に表示されるメール通知にどのように影響しますか？

デバイスのロック画面に表示される新着メール通知は、Secure Mail によってデバイスに同期されたデータに基づいて生成されます。重要な点として、この情報はリスナーサービスから提供されるものではありません。

新着メール通知を表示するには、Secure Mail が Exchange からデータを同期できる必要があり、それによって Secure Mail が通知を作成するための情報を利用できるようになります。

APNs 通知がバックグラウンドで Secure Mail に配信されない場合、Secure Mail は通知を検知せず、新しいデータを同期しません。Secure Mail で新しいデータが利用できないため、APNs 通知が配信されない場合でも、デバイスのロック画面にメール通知は生成されません。

バックグラウンドアプリの更新は Secure Mail と APNs にどのように影響しますか？

ユーザーがバックグラウンドアプリの更新をオフにすると、次の状況が発生します。

- Secure Mail がバックグラウンドアプリにある場合、Secure Mail は通知を受信しません。

注:

この状況は、リッチプッシュ通知が無効になっている場合にのみ発生します。リッチプッシュ通知の詳細については、「[iOS 用 Secure Mail のリッチプッシュ通知](#)」を参照してください。

- Secure Mail は新しいメール通知でロック画面を更新しません。

バックグラウンドアプリの更新を無効にすると、Secure Mail の動作に大きな影響があります。前述のとおり、APNs に基づくバッジの更新は引き続き行われますが、このモードではメールはデバイスに同期されません。

低電力モードは Secure Mail と APNs にどのように影響しますか？

低電力モードでの Secure Mail に関するシステムの動作は、バックグラウンドアプリの更新が無効になっている場合と同じです。低電力モードでは、デバイスは定期的な更新のためにアプリを起動せず、バックグラウンドでアプリに通知を配信しません。したがって、副作用は上記の「バックグラウンドアプリの更新」セクションに記載されているものと同じです。低電力モードでも、APNs 通知に基づいてバッジの更新は引き続き行われることに注意してください。

FCM 主導の同期がバックグラウンドで失敗する原因となるその他の問題は何ですか？

FCM 主導の同期要求が失敗する原因となるさまざまな問題があり、以下が含まれます。

- 無効な STA チケット。
- Secure Mail がドーズモードで起動された場合、アプリはサーバーからすべてのデータを同期するために 10 秒間かかります。

上記のいずれかの条件が発生した場合、Secure Mail はデータを同期できません。その結果、ロック画面の通知は表示されません。

APNs 主導の同期がバックグラウンドで失敗する原因となるその他の問題は何ですか？

APNs 主導の同期要求が失敗する原因となるいくつかの問題があり、以下が含まれます。

- 無効な STA チケット。
- ネットワーク接続が遅い場合。Secure Mail がバックグラウンドで起動された場合、アプリはサーバーからすべてのデータを同期するために 30 秒間かかります。
- データ保護ポリシーが有効になっており、Secure Mail が APNs 通知によって起動された場合、デバイスがロックされていると、Secure Mail はデータストアにアクセスできず、同期は行われません。これは、システムが Secure Mail をコールドスタートしようとしている場合にのみ当てはまることに注意してください。ユーザーがデバイスのロック解除後に Secure Mail を一度でも起動している場合、デバイスがロックされていても APNs 主導の同期は成功します。

上記のいずれかの条件が発生した場合、Secure Mail はデータを同期できず、したがってロック画面の通知を表示できません。

通知が配信されない場合やAPNsが使用されていない場合、Secure Mailは他にどのようにロック画面通知を生成しますか？

APNsが無効になっている場合でも、Secure Mailは、バックグラウンドアプリ更新が有効で、低電力モードがオフになっていることを前提として、iOSからの定期的なバックグラウンドアプリ更新イベントによって起動されます。

これらの起動イベント中に、Secure MailはExchange Serverから新しいメールを同期します。この新しいメールは、ロック画面にメール通知を生成するために使用できます。したがって、APNs通知が配信されない場合やAPNsが無効になっている場合でも、Secure Mailはバックグラウンドでデータを同期できます。

APNsが使用されている場合やAPNs通知がSecure Mailに配信される場合よりも、これがリアルタイムで発生する頻度は低いことに注意することが重要です。iOSがAPNs通知をSecure Mailにルーティングすると、アプリはすぐにサーバーからデータを同期し、ロック画面通知はリアルタイムで表示されます。

In the event that Background App Refresh wakeups are required, lock screen notifications do not occur in real time. In this case, Secure Mail is woken up at a frequency that iOS completely determines. As such, some time may elapse between these two situations:

- When an email arrives in a user's Inbox on Exchange.
- Secure Mailがそのメッセージを同期し、ロック画面通知を生成したとき。

APNsが使用されている場合でも、Secure Mailはこれらの定期的なウェイクアップを受け取ることに注意してください。Background App RefreshがSecure Mailを起動するすべての場合において、Secure MailはExchangeからデータを同期しようとします。

Secure Mailは、ロック画面にコンテンツを表示する他のアプリとどう異なりますか？

混乱を招く可能性のある重要な違いは、Secure Mailがロック画面に新しいメールを常にリアルタイムで表示するわけではないということです。この動作は、Gmail、Microsoft Outlook、およびその他のアプリとは異なります。この違いの主な理由はセキュリティです。他のアプリの動作に合わせるには、CitrixリスナーサービスがExchangeで認証するためにユーザー資格情報を必要とします。資格情報はメールコンテンツを取得するために必要です。また、このメールコンテンツをCitrixリスナーサービスを介してApple APNsサービスに渡すためにも資格情報が必要です。CitrixのAPNs通知へのアプローチでは、Citrixリスナーサービスがユーザーのパスワードを取得または保存する必要はありません。リスナーサービスはユーザーのメールボックスやパスワードにアクセスできません。

ネイティブiOSメールアプリに関する注意点：iOSは、独自のメールアプリがメールサーバーとの永続的な接続を維持することを許可しており、これにより通知が常に配信されることが保証されます。ネイティブメール以外のサードパーティアプリには、この機能は許可されていません。

Gmailアプリの動作： GoogleはGmailアプリとGmailサーバーの両方を所有および管理しています。この動作は、Googleがメッセージコンテンツを読み取り、そのメッセージコンテンツをAPNs通知ペイロードに含めることができることを意味します。iOSがGmailからこのAPNs通知を受信すると、iOSは次のことを行います。

- 通知ペイロードで指定された値にアプリケーションバッジを設定します。
- 通知ペイロードに含まれるメッセージテキストを使用して、ロック画面通知を表示します。

これは決定的な違いです。ペイロードに含まれるデータに基づいてロック画面通知を表示するのは、GmailアプリではなくiOSです。実際、通知が届いたときにiOSがSecure Mailを起動しないのと同様に、iOSはGmailアプリを起動しない場合があります。しかし、ペイロードにメッセージスニペットが含まれているため、iOSはメールデータをデバイスに同期することなくロック画面通知を表示できます。

Secure Mailでは、この状況は異なります。アプリがロック画面通知を表示する前に、Secure Mail はまずExchangeからメッセージデータを同期する必要があります。

Outlook for iOSアプリの動作: MicrosoftがOutlook for iOSを制御しています。しかし、ユーザーが所属する組織は、データが取得されるExchange Serverを制御しています。この設定にもかかわらず、OutlookはMicrosoftがAPNs通知で提供するデータに基づいてロック画面通知を表示できます。その理由は、Outlook for iOSがMicrosoftがユーザー資格情報を保存するモデルを利用しているためです。その後、Microsoftはクラウドサービスからユーザーのメールボックスに直接アクセスし、新しいメールの存在を判断します。

新しいメールが利用可能な場合、Microsoftクラウドサービスは新しいメールデータを含むAPNs通知を生成します。このモデルはGmailモデルと同様に動作します。Gmailモデルでは、iOSは単にデータを受け取り、そのデータに基づいてロック画面通知を生成します。Outlook iOSアプリはこのプロセスに関与しません。

Outlook for iOSに関する重要なセキュリティ上の注意: Outlook for iOSのアプローチには、明確なセキュリティ上の影響があります。組織は、ユーザーのパスワードをMicrosoftに信頼する必要があります。この信頼により、Microsoftはユーザーのメールボックスにアクセスできるようになり、セキュリティリスクをもたらします。

プッシュ通知に関する管理者向けのFAQについては、こちらの[サポート技術情報記事](#)を参照してください。ユーザー向けのFAQについては、こちらの[サポート技術情報記事](#)を参照してください。

Secure Mail for iOS のリッチプッシュ通知

Secure Mail for iOS はリッチプッシュ通知をサポートしています。リッチ通知により、Secure Mail がバックグラウンドで実行されていない場合でも、受信トレイのロック画面通知を受信できます。この機能は、パスワードベースの認証とクライアントベースの認証設定でサポートされています。

注:

この機能をサポートするためのアーキテクチャの変更により、VIP のみのメール通知機能は利用できなくなりました。

リッチプッシュ通知機能を有効にするには、以下の前提条件が満たされていることを確認してください。

- Endpoint Management コンソールで、プッシュ通知を **ON** に設定します。

- ネットワークアクセス ポリシーが **無制限** または **内部ネットワークへのトンネル** に設定されていること。ネットワークアクセス ポリシーが **内部ネットワークへのトンネル** に設定されている場合は、Exchange Web Services (EWS) ホストがバックグラウンドネットワークサービス ポリシーで構成されていることを確認してください。EWS ホストと ActiveSync ホストが同じ場合は、ActiveSync ホストがバックグラウンドネットワークサービス ポリシーで構成されていることを確認してください。
- ロック画面通知の制御ポリシーが **許可** または **メール送信者またはイベントタイトル** に設定されていること。
- **Secure Mail > 設定 > 通知** に移動し、**メール通知** を有効にします。

以下のいずれかの設定を実行している場合、この機能はサポートされません。

- Microsoft Office 365 を使用した最新の認証
- Microsoft Intune/EMS との Endpoint Management 統合によって管理されるアプリ
- 派生資格情報を使用して登録されたデバイス

Secure Mail iOS でプッシュ通知が機能する方法

Secure Mail は、以下の受信トレイアクティビティのプッシュ通知を受信します。

- **新規メール、会議出席依頼、会議キャンセル、会議更新**: APNsがiOS Secure Mailにリモート通知をプッシュし、Secure Mailが自動更新対象としてマークされているすべてのフォルダーを更新する場合。

注:

デフォルトでは、受信トレイ、カレンダー、連絡先フォルダーは自動更新対象としてマークされています。ユーザーは、**Secure Mail > 設定 > 自動更新**から、他のメールフォルダーを自動更新対象として選択できます。

- Secure Mailアイコンには、Exchange受信トレイフォルダー内の未読および新規メッセージの合計数のみが表示されます。ユーザーがデスクトップまたはラップトップコンピューターでメールを読んだ後、Secure Mailはアイコンを更新します。
- インストールまたはアップグレード中に、Secure Mail for iOSはプッシュ通知を許可するようにユーザーに促します。ユーザーは、iOS設定を使用して後でプッシュ通知を許可することもできます。

リッチプッシュ通知サポートなしでのプッシュ通知の動作

iOSのリッチプッシュ通知機能でサポートされていない構成の場合でも、Secure Mailは同期期間の未読受信トレイメールの数を提供します。ロック画面通知の制御ポリシーがオンの場合、iOSがSecure Mailを起動して同期を実行した後、ロックされたデバイス画面にプッシュ通知が表示されます。

Secure Mail iOSプッシュ通知に関するFAQ

iOSはいつSecure Mailに通知を配信しますか？

リッチプッシュ通知機能が有効になっている場合、iOSはSecure Mailにリモート通知を配信します。これらの通知は、アプリがバックグラウンドで実行されていない場合や、低電力モードの場合でも発生します。

注:

リッチプッシュ通知が有効になっていない場合、Secure Mailがアクティブでないときに通知がSecure Mailに配信されないことがあります。この状況は、次のような多くの理由で発生します。

- デバイスが低電力モードで、Secure Mailがバックグラウンドにある場合: これは、通知が配信されない最も一般的なケースです。
- Secure Mailのバックグラウンドアプリ更新がオフで、Secure Mailがバックグラウンドにある場合: この設定はユーザーが制御することに注意してください。
- デバイスのネットワーク接続が悪い場合: この状況はiOSデバイスに依存します。

iOSデバイスに「新着メールがあります」通知が表示される理由

Secure Mailが指定された時間内にExchange Web Services (EWS) から応答を受信しない場合、iOSデバイスに「新着メールがあります」通知が表示されます。メッセージの詳細を取得するために必要な時間は30秒です。

一般的なiOSの新着メール通知の画像(</en-us/mobile-productivity-apps/media/ios-new-email-notification-generic.png>)

Wi-Fiまたはデータ接続が不良である場合、デバイスでこの動作が発生することもあります。

EWS応答の遅延以外にも、Secure Mailは次の状況で「新着メールがあります」通知を表示します。

- Secure Mailがセキュアコンテナから必要な情報を読み取れない場合。このシナリオは通常、デバイスを再起動した後、デバイスのロックを解除する前に発生します。
- Secure MailがCitrix GatewayまたはEWSとのセキュアチャネルへの接続または設定に失敗した場合。
- 資格情報が期限切れになった場合、または資格情報を変更したがSecure Mailで更新されていない場合。次の図は、このシナリオで通知が表示される方法を示しています。

メール通知メッセージの画像(/en-us/mobile-productivity-apps/media/new-mail-notification-ios.png)

- Secure Mailからの有効な要求に対して、Exchange Serverから予期しない応答を受信した場合。EWS応答コードの詳細については、Microsoft開発者向けドキュメントを参照してください。

Secure Mail for iOSにおけるプッシュ通知の失敗メッセージ

Secure Mail for iOSでは、適切なプッシュ通知の失敗メッセージがデバイスの通知センターに表示されます。これらの通知は、通知の失敗の種類に基づいて表示されます。

さまざまな失敗シナリオに基づいて、次の通知メッセージが表示されます。

- **Secure Mailは組織のネットワークに接続できません。** この通知は、Secure MailがCitrix GatewayとのSOCKS5接続を確立できない場合に表示されます。
- **Secure Mailは組織のネットワークに接続できません。管理者にお問い合わせください。** この通知は、Citrix Gatewayに到達できない場合に表示されます。Citrix ADCが正しく構成されており、外部ネットワークから到達可能であることを確認してください。
- **Secure Mail は組織のネットワークに安全に接続できません。管理者にお問い合わせください。** この通知は、Secure Mail が Citrix Gateway との SSL 接続を確立できなかった場合に表示されます。SSL 証明書が有効であることを確認してください。
- **Secure Mail はメールサーバーに安全に接続できません。管理者にお問い合わせください。** この通知は、Secure Mail が Exchange Server との SSL 接続を確立できなかった場合に表示されます。Exchange Server の SSL 証明書が有効であることを確認してください。無効な証明書があるにもかかわらずアプリを Exchange Server に接続する場合は、MDX ポリシーを有効にしていることを確認してください。
- **メールサーバーエラーのため、Secure Mail はメッセージを取得できません。管理者にお問い合わせください。** この通知は、Secure Mail が Exchange Server からの EWS 応答を解析できない場合に表示されます。

- リクエストのタイムアウトにより、**Secure Mail** はメッセージを取得できません。この通知は、Secure Mail が 30 秒以内にサーバーからの応答を受信できなかった場合に表示されます。この通知は、デバイスのデータ接続または Wi-Fi 接続が不安定な場合に表示されることがあります。数分待ってからもう一度お試しください。
- メッセージを取得できません。**Secure Mail** を開いてください。この通知は、Secure Mail がセキュアコンテナから資格情報を読み取れない場合に表示されます。この通知は、デバイスが再起動されたがロック解除されていない場合に表示されることがあります。デバイスのロックを解除して、Secure Mail がセキュアコンテナに自動的にアクセスできるようにします。この通知が引き続き表示される場合は、Secure Mail を開いてセキュアコンテナ内の資格情報を自動的に更新してください。

Secure Mail と他のモバイル生産性アプリおよび Citrix Files との連携

Secure Mail と他のモバイル生産性アプリおよび Citrix Files との連携により、ユーザーは組織のポリシーによって設定されたセキュアな環境を離れることなく、ドキュメントにシームレスにアクセス、編集、共有、保存できます。たとえば、Secure Mail でリンクをタップすると、Secure Web でサイトが開きます。ユーザーは Endpoint Management 用の Citrix QuickEdit™ で添付ファイルを開いて編集できます。添付ファイルは、ユーザーの Endpoint Management 用 Citrix Files スペースにダウンロードされます。

各プラットフォームの Secure Mail 機能の全リストについては、「[プラットフォーム別の機能](#)」を参照してください。

注：

- Citrix Files for XenMobile は July 1, 2023 に EOL に達しました。詳細については、[EOL および非推奨のアプリ](#)を参照してください。

Secure Mailのテストとトラブルシューティング

Secure Mailが正常に動作しない場合、通常は接続の問題が原因です。この記事では、接続の問題を回避する方法について説明します。問題が発生した場合、この記事ではそのトラブルシューティング方法について説明します。

ActiveSync接続、ユーザー認証、およびAPNs構成のテスト

Endpoint Management Analyzerを使用して、Secure Mailの自動検出サービスチェックを実行できます。これにより、Endpoint Management Exchange ActiveSync Testアプリケーションのダウンロードが案内されます。メールテストオプションは、メールサーバーへの基本的な接続設定をチェックします。このツールは、ActiveSyncサーバーがEndpoint Management環境に展開できる状態であるかどうかのトラブルシューティングにも役立ちます。

Analyzerのメールテストオプションは、以下を検証します。

- Microsoft ExchangeまたはIBM TravelerサーバーとのiOSおよびAndroidデバイス接続。
- ユーザー認証。
- Exchange Server、Exchange Web Services (EWS)、Citrix Gateway、APNs証明書、Secure Mailを含むiOSのプッシュ通知構成。プッシュ通知の構成については、「[iOS用Secure Mailのプッシュ通知](#)」を参照してください。

このツールは、問題の修正に関する包括的な推奨事項リストを提供します。

注：

Mail Test App (MailTest.ipa) は非推奨です。代わりに、Endpoint Management Analyzerで同じ機能にアクセスしてください。

テストの前提条件

- ネットワークアクセスポリシーがブロックされていないことを確認します。
- メール作成のブロックポリシーをオフに設定します。

Secure Mailログを使用した接続問題のトラブルシューティング

Secure Mailのログを取得するには、次の手順を実行します。

1. **Secure Hub > ヘルプ > 問題を報告**に移動します。
2. アプリケーションの一覧から**Secure Mail**を選択します。

組織のヘルプデスク宛てのメールが開きます。

3. 件名と本文に、問題の内容を数語で記述します。
4. 問題が発生した時刻を選択します。
5. サポートチームから指示があった場合にのみ、ログ設定を変更してください。
6. **送信**をクリックします。

完了したメッセージが、圧縮されたログファイルが添付された状態で開きます。

7. もう一度**送信**をクリックします。

送信されたzipファイルには、次のログが含まれています。

CtxLog_AppInfo.txt (アイオーエス)、Device_And_AppInfo.txt (アンドロイド)、logx.txt、および WH_logx.txt (ウィンドウズ フォン)

アプリ情報ログには、デバイスとアプリに関する情報が含まれています。使用中のハードウェアモデルとプラットフォームバージョンがサポートされていることを確認してください。使用中の Secure MailとMDX Toolkitのバージョンが最新であり、互換性があることを確認してください。詳細については、「[Secure Mailのシステム要件](#)」および「[Endpoint Managementの互換性](#)」を参照してください。

- CtxLog_VPNConfig.xml (アイオーエス) およびVpnConfig.xml (アンドロイド)

VPN構成ログはSecure Hub専用です。最新のCitrix ADCリリースが使用されていることを確認するために、Citrix ADCのバージョン `ServerBuildVersion` を確認してください。 `SplitDNS` と `SplitTunnel` の設定を次のように確認してください。

- Split DNSが**Remote**、**Local**、または**Both**に設定されている場合は、DNSを介してメールサーバーのFQDNが正しく解決されていることを確認してください。(Split DNSはAndroid版Secure Hubで利用可能です。)
- Split Tunnelが**On**に設定されている場合は、メールサーバーがバックエンドでアクセス可能なインターネットアプリの1つとしてリストされていることを確認してください。
- CtxLog_AppPolicies.xml (アイオーエス)、Policy.xml (Android および Windows Phone)

ポリシーログには、ログを取得した時点でのSecure Mailに適用されたすべてのMDXポリシーの値が示されます。接続の問題については、 `<BackgroundServices>` および `<BackgroundServicesGateway>` ポリシーの値を確認してください。

- 診断ログ (diagnosticsフォルダー内)

Secure Mailの初期構成で最も一般的な問題は、「Your Company Network Is Not Currently Available.」です。接続の問題をトラブルシューティングするために診断ログを使用するには、次の手順を実行します。

診断ログの主要な列は、Timestamp、Message Class、およびMessageです。Secure Mailにエラーメッセージが表示されたら、その時刻をメモしておく、**Timestamp**列に関連するログエントリをすばやく見つけることができます。

デバイスからCitrix Gatewayへの接続が成功したかどうかを判断するには、AG Tunnelerのエントリを確認します。次のメッセージは、接続が成功したことを示します。

- AGポリシー FQDN:443をSTAトンネリング用にインターセプト
- (null):443への新しいTCPプロキシ接続が確立されました

Citrix GatewayからEndpoint Managementへの接続が成功したかどうか（したがってSTAチケットを検証できるかどうか）を判断するには、次の手順を実行します。Secure Hub診断ログに移動し、デバイスが登録された時刻のMessage Classの下にあるINFO (4)エントリを確認します。次のメッセージは、Secure HubがEndpoint ManagementからSTAチケットを取得したことを示します。

- STAチケットを取得しています。
- STAチケット応答を受信しました。
- STAチケット – アプリ -- Secure MailのSTAチケット取得に成功しました。

注:

登録中に、Secure HubはEndpoint ManagementにSTAチケットを要求します。Endpoint ManagementはSTAチケットをデバイスに送信し、デバイスに保存され、Endpoint ManagementのSTAチケットリストに追加されます。

Endpoint ManagementがユーザーにSTAチケットを発行したかどうかを確認するには、サポートバンドルに含まれるUserAuditLogFile.logを確認してください。このログには、各チケットの発行時刻、ユーザー名、ユーザーデバイス、および結果が一覧表示されます。例：

時間: 2015-06-30T 12:26:34.771-0700

ユーザー: user2

デバイス: Mozilla/5.0 (iPad; CPU OS 8_1_2 like macOS)

結果: アプリ「Secure Mail」のユーザー「user2」向けSTAチケットが正常に生成されました

Citrix Gatewayからメールサーバーへの通信を確認するには、DNSとネットワークが正しく構成されているかを確認します。これを行うには、Secure Webを使用してOutlook Web Access (OWA)にアクセスします。Secure Mailと同様に、Secure WebはマイクロVPNトンネルを使用してCitrix Gatewayへの接続を確立できます。Secure Webは、アプリがアクセスしている内部または外部リソースへのプロキシとして機能します。通常、特にExchange環境では、OWAはメールサーバー上でホストされます。

構成をテストするには、Secure Webを開き、OWAページのFQDNを入力します。このリクエストは、Citrix Gatewayとメールサーバー間の通信と同じルートとDNS解決を使用します。OWAページが開けば、Citrix Gatewayがメールサーバーと通信していることがわかります。

前述のチェックで通信が成功していることが示された場合、問題はCitrixのセットアップにはなく、ExchangeまたはTravelerサーバーにあることがわかります。

ExchangeまたはTravelerサーバーの管理者向けに情報を収集できます。まず、Secure Mailの診断ログで「Error」という単語を検索して、ExchangeまたはTravelerサーバー上のHTTPの問題を確認します。エラーにHTTPコードが含まれており、複数のExchangeまたはTravelerサーバーがある場合は、各サーバーを調査します。ExchangeとTravelerには、クライアントデバイスからのHTTPリクエストとレスポンスを示すHTTPログがあります。ExchangeのログはC:\inetpub\LogFiles\W3SVC1\U_EX.logです。TravelerのログはIBM_TECHNICAL_SUPPORT>HTTHR.logです。

iOS版Secure Mailのデバイスからクラッシュログを取得するには

1. iOSデバイスで、**設定 > プライバシー > 解析 > 解析データ** に移動します。
2. **データ リスト**で、アプリの名前と関連するタイムスタンプをクリックします。ログが表示されます。

メール、連絡先、またはカレンダーに関する問題のトラブルシューティング

Secure Mailの問題（下書きに留まっているメール、連絡先の欠落、カレンダー項目の同期ずれなど）をトラブルシューティングできます。これらの問題をトラブルシューティングするには、Exchange ActiveSyncメールボックスログを使用します。ログには、デバイスから送信された受信リクエストと、メールサーバーからの送信レスポンスが表示されます。

無制限同期のベストプラクティス

ユーザーが同期メール期間を**すべて**に設定すると、無制限同期が有効になります。無制限同期では、ユーザーがメールボックスのサイズ（受信トレイと同期されたすべてのサブフォルダー）を管理することが前提となります。最高のパフォーマンスを得るために、以下の点に留意してください。

1. メールボックスのサイズが18,000メッセージまたは合計600 MBを超えると、メール同期が遅くなる可能性があります。
2. 無制限同期で**Wi-Fiで添付ファイルを読み込む**を有効にすることはお勧めしません。このオプションは、デバイス上のメールサイズを急速に肥大化させる可能性があります。

3. ユーザーのオプションとして無制限同期を防止するには、**最大同期間隔アプリポリシー**を**すべて**以外の値に設定します。
4. ユーザーに対して**すべて**を**デフォルトの同期間隔**として設定することはお勧めしません。