Secure Mail

Contents

Secure Mail の概要

March 29, 2019

Citrix Secure Mail では、スマートフォンまたはタブレット上でメール、カレンダー、および連絡先を管理できます。Microsoft Outlook または IBM Notes アカウントからの連続性を維持するため、Secure Mail は Microsoft Exchange Server および IBM Notes Traveler Server と同期します。

シトリックス製品ファミリのアプリである Secure Mail には、Citrix Secure Hub とのシングルサインオン（SSO）互換性があります。ユーザーが Secure Hub にサインオンした後は、ユーザー名とパスワードを再入力する必要なく、シームレスに Secure Mail に移動できます。デバイスが Secure Hub に登録されるとユーザーデバイスに自動的に公開されるように Secure Mail を構成できます。または、ユーザーが Store からアプリを追加できます。

Secure Mail は次のものと互換性があります。

- 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 2016 累積更新プログラム 11
- Exchange Server 2016 累積更新プログラム 10
- Exchange Server 2016 累積更新プログラム 9
- Exchange Server 2016 累積更新プログラム 8
- Exchange Server 2013 累積更新プログラム 21
- Exchange Server 2013 累積更新プログラム 19
- Exchange Server 2010 Service Pack 3 更新プログラムのロールアップ 26
- Exchange Server 2010 Service Pack 3 の更新プログラムのロールアップ 24
- Exchange Server 2010 Service Pack 3 の更新プログラムのロールアップ 19
- Exchange Server 2010 Service Pack 3 の更新プログラムのロールアップ 22
- IBM Domino Mail Server バージョン 9.0.1 FP10 HF197
- IBM Domino Mail Server バージョン 9.0.1 FP9
- IBM Lotus Notes Traveler version 9.0.1.21
- IBM Lotus Notes Traveler versions 8.5.3 UP2 および 9.0.1.9
- Microsoft Office 365（Exchange Online）

まず、Secure Mail とその他の Endpoint Management コンポーネントをCitrix Endpoint Management のダウンロードからダウンロードします。

Secure Mail および他のモバイル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。

アプリがバックグラウンドで実行されている時、または閉じている時の Secure Mail for iOS および Android の通知については、「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 機能については、「Secure Mail 用の 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 機能については、「Secure Mail 用の 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 機能および Android 機能については、「Secure Mail の iOS 機能と Android 機能」を参照してください。

Secure Mail の新機能

May 17, 2019

以下の機能は Secure Mail の新機能です:

Secure Mail 19.5.0

Secure Mail for Android

フィードの管理

Secure Mail for Android では、フィードカードを必要に応じて整理できます。

フィードの管理について詳しくは、「フィードの管理」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。この機能は、Office 365 または Exchange Server 2016 以降を実行しているデバイスで使用できます。

> 注:
>
> 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。

以前のバージョンの新機能

Secure Mail for Android 19.4.6、19.4.5、19.3.5

これらのリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

既知の問題と解決された問題については、「既知の問題と解決された問題」を参照してください。

Secure Mail 19.3.0

このリリース以降の Secure Mail は、次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 Service Pack 3 更新プログラムのロールアップ 26

Secure Mail と互換性のあるサーバーの完全な一覧については、「Secure Mail の概要」を参照してください。

Secure Mail for iOS

フィードの管理。Secure Mail for iOS では、フィードカードを必要に応じて整理できます。

> 注:
>
> この機能は iPad では使用できません。

フィードの管理について詳しくは、「フィードの管理」を参照してください。

Secure Mail for iOS および Android

内部ドメイン。外部組織に属するメール受信者を識別および編集できます。Citrix Endpoint Management でこの機能を使用するには、［内部ドメイン］ ポリシーを有効にしたことを確認してください。

メールを作成、返信、または転送するときに、外部の受信者がメーリングリストで強調表示されます。連絡先アイコンは、画面の左下に警告として表示されます。連絡先アイコンをタップすると、メーリングリストを変更できます。

内部ドメインについて詳しくは、「内部ドメイン」を参照してください。

人間工学に基づいた機能向上。これにより、操作ボタンが画面の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。この変更は、受信トレイ、カレンダー、連絡先の画面に適用されています。

> 注:
>
> Android を実行しているデバイスの場合は、受信トレイ画面とカレンダー画面が変更されます。

人間工学に基づいた機能向上について詳しくは、「人間工学に基づいた機能向上」を参照してください。

Secure Mail 19.2.0

Secure Mail for iOS

Secure Mail 19.2.0 リリースには、バグの修正とパフォーマンスの強化機能が含まれています。

既知の問題と解決された問題については、「既知の問題と解決された問題」を参照してください。

Secure Mail for Android

- 連絡先の機能強化。Secure Mail for Android では、［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」および「同僚」など、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］ タブでは、［マネージャー］、［直属の部下］、［同僚］ の右側にある詳細アイコンをタップして、新しいメールまたは新しいカレンダーへの招待を作成できます。メールまたはカレンダーイベントの ［宛先］ フィールドに、「マネージャー」、「直属の部下」、「同僚」の詳細が自動的に入力されます。

  前提条件:

  Exchange Web サービス（EWS）が Exchange Server で有効になっていることを確認します。

  連絡先の詳細は、Active Directory から取得した組織の詳細に基づいて表示されます。正しい連絡先の詳細を表示するには、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。

- ネットワークアクセスポリシー。Secure Mail for Android では、ネットワークアクセス MDX ポリシーに［トンネル**-Web SSO**］ という新しいオプションが追加されています。このポリシーを構成すると、内部トラフィックをセキュアブラウズおよび Secure Ticket Authority（STA）を同時に使用して柔軟にトンネリングすることができます。また、NTLM、Okta、Kerberos のようなセキュアブラウズ接続も許可できます。最初に STA を構成するときには、サービスアドレスの個別の FQDN および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。［トンネル**-Web SSO**］ オプションを構成する場合は、これらを構成する必要はありません。

Citrix Endpoint Management コンソールの Secure Mail for Android でこのポリシーを構成するには:

1. Android 用の.mdx ファイルをダウンロードします。詳しくは、「モバイルおよび MDX アプリのしくみ」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**–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。

Secure Mail for iOS 19.1.6

このリリースには、バグの修正とパフォーマンスの強化機能が含まれています。

Secure Mail 19.1.5

このリリース以降の Secure Mail は、次のサーバーをサポートします:

- Exchange Server 2016 の累積更新プログラム 11
- Exchange Server 2010 Service Pack 3 の更新プログラムのロールアップ 24

Secure Mail と互換性のあるサーバーの完全な一覧については、「Secure Mail の概要」を参照してください。

Secure Mail 19.1.0

Secure Mail for iOS

- 連絡先の機能強化。Secure Mail for iOS では、［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」および「同僚」など、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］ タブでは、「マネージャー」、「直属の部下」、「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、「マネージャー」、「直属の部下」、「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することができます。

  前提条件:

  Exchange Web サービス（EWS）が Exchange Server で有効になっていることを確認します。

  連絡先の詳細は、Active Directory から取得した組織の詳細（Outlook の連絡先）に基づいて表示されます。正しい連絡先の詳細を表示するには、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。

- 会議の日時と場所をネイティブカレンダーにエクスポートします。Secure Mail for iOS では、新しい値の ［会議の時間と場所］ が ［カレンダーのエクスポート］ MDX ポリシーに追加されました。これによって、Secure Mail のカレンダーイベントにある会議の時間と場所を、ローカルのカレンダーにエクスポートすることができます。
- Secure Mail for iOS は、Microsoft Enterprise Mobility + Security (EMS)/Intune を先進認証（O365）で実行するセットアップで、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、次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［オン］に設定します。
  - ネットワークアクセスポリシーを ［制限なし］ に設定します。
  - ロック画面上の通知を制御ポリシーは、［許可］ または ［メールの送信者またはイベントのタイトル］ に設定されています。
  - ［**Secure Mail**］>［設定］>［通知］ の順に移動し、［メール通知］ を有効にします。

- Secure Mail のユーザーは、ズームアプリを使用して会議に参加できるようになりました。ズームアプリの使用に必要なポリシーの構成について詳しくは、「カレンダーからの会議への参加」を参照してください。
- このリリースでは、iPad Pro 11 インチと iPad Pro 12.9 インチがサポートされます。

Secure Mail for Android

- 添付ファイルの機能強化。Secure Mail for Android では、添付ファイルを簡単に表示できます。より良いエクスペリエンスを提供するために、不要な手順が削除されましたが、以前のリリースでの添付オプションが引き続き使用されています。

  Secure Mail アプリ内で添付ファイルを表示できます。Secure Mail で添付ファイルを表示できる場合は、添付ファイルが直接開きます。それ以外の場合は、アプリの一覧が表示されます。添付ファイルを表示するために必要なアプリを選択できます。詳しくは、「添付ファイルの表示」を参照してください。

- Secure Mail のユーザーは、ズームアプリを使用して会議に参加できるようになりました。ズームアプリの使用に必要なポリシーの構成について詳しくは、「カレンダーからの会議への参加」を参照してください。
- 会議の日時と場所をネイティブカレンダーにエクスポートします。Secure Mail for iOS では、新しい値の［会議の時間と場所］ が ［カレンダーのエクスポート］ MDX ポリシーに追加されました。これを使用すると、Secure Mail のカレンダーイベントにある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ことができます。

> 注:
>
> Android 5.x のサポートは、2018 年 12 月 31 日に終了しました。

Secure Mail 18.12.0

Secure Mail 18.12.0 リリースには、バグの修正とパフォーマンスの強化機能が含まれています。

既知の問題と解決された問題については、「既知の問題と解決された問題」を参照してください。

Secure Web 18.11.5

Secure Mail for Android

- **ActiveSync** ヘッダーでフィッシングメールを報告。Secure Mail for Android では、ユーザーがフィッシングメールについて報告すると、そのメールに関連した添付として EML ファイルが生成されます。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ている ActiveSync ヘッダーを表示できます。

この機能を有効にするには、管理者が 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、［フィッシング報告の方法］ を ［転送で報告］ に設定する必要があります。詳しくは、「添付ファイルでフィッシングメールを報告」を参照してください。

- メールおよび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のイベントを印刷できます。この印刷機能は Android 印刷フレームワークを使用します。詳しくは、「メールおよびカレンダーイベントの印刷」を参照してください。
- 差出人がマネージャーのフィード。Secure Mail for Android 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。［メールの同期期間］設定に基づいて、［差出人がマネージャー］フィードで最大 5 通のメールが表示されます。さらにマネージャーからのメールを表示するには、［すべて表示］ をタップします。

  前提条件：

  Exchange Web サービス（EWS）が Exchange Server で有効になっていることを確認します。

  Active Directory から取得した組織の詳細（Outlook の連絡先）に基づいて、マネージャーカードが表示されます。マネージャーフィードで正しい詳細を表示するには、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。

Secure Mail 18.11.1

> 重要：
>
> 次の問題は、Secure Mail for Android 18.11.1 で解決されています
>
> Secure Mail for Android で IBM Notes Traveler 9.0.1 SP 10 に接続している場合、添付ファイル付きのメールが送信されずに送信トレイに残ります。[CXM-58962]

Secure Mail 18.11.0

Secure Mail for Android

- 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信できます。詳しくは、「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の要件を満たすために、Secure Mail バックグラウンドサービスがアップグレードされました。デバイスでメールの同期と通知を中断しないためには、Firebase Cloud Messaging（FCM）サービスのプッシュ通知を有効にします。FCM ベースのリッチプッシュ通知について詳しくは、「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ます。この更新について詳しくは、Support Knowledge Center の記事を参照してください。

制限事項:

- FCM ベースのプッシュ通知を有効にしない場合、15 分ごとにバックグラウンド同期が発生します。この間隔は、アプリがバックグラウンドまたは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でこの時間を手動で更新すると、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。

Secure Mail for iOS

- **iOS 12.1** のサポート。Secure Mail for iOS は iOS バージョン 12.1 をサポートします。
- リッチプッシュ通知の失敗メッセージの強化。Secure Mail for iOS では、通知の失敗の種類に基づいてデバイスの通知センターに適切なプッシュ通知の失敗メッセージが表示されます。詳しくは、「Secure Mail for iOS のプッシュ通知の失敗メッセージ」を参照してください。
- 差出人がマネージャーのフィード。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。［メールの同期期間］ 設定に基づいて、［差出人がマネージャー］ フィードで最大 5 通のメールを表示されます。さらにマネージャーからのメールを表示するには、［すべて表示］ をタップします。

  前提条件:

  Exchange Web サービス（EWS）が Exchange Server で有効になっていることを確認します。

  Active Directory から取得した組織の詳細（Outlook の連絡先）に基づいて、マネージャーカードが表示されます。マネージャーフィードで正しい詳細を表示するには、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。

Secure Mail 18.10.5

- **Secure Mail** の **Slack** との統合（プレビュー）: iOS または Android デバイスで、メールでの会話を Slack アプリで続けられるようになりました。詳しくは、「Secure Mail と Slack との統合（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拡張: Secure Mail for iOS では、既存のフィードフォルダーの以下の機能が拡張されています:
  - 近日中の会議がフィードカードに最大 5 つ表示されます。
  - 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］ および ［明日］ のセクションに分類されます。

Secure Mail 18.10.0

- メールとカレンダーの通知用の **Secure Mail** 通知チャネル： Android O 以降が稼働するデバイスでは、通知チャネル設定を使用して、メールやカレンダーの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して管理できます。詳しくは、「通知チャネル」を参照してください。
- 転送でフィッシングメールを報告： Secure Mail for iOS では、フィッシングメールの報告機能を使用して、フィッシングの疑いがあるメールを転送で報告することができます。不審なメッセージは、管理者がポリシーに設定する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、［フィッシング報告の方法］ を ［転送で報告］ に設定する必要があります。詳しくは、「転送でフィッシングメールを報告」を参照してください。

Secure Mail 18.9.0

- 「yy.mm.version」という形式の新しいバージョン番号体系。例えば、バージョン **18.9.0** などです。
- 転送でフィッシングメールを報告： Secure Mailfor Android では、フィッシングメールの報告機能を使用して、フィッシングの疑いがあるメールを転送で報告することができます。不審なメッセージは、管理者が設定する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、［フィッシング報告の方法］を ［転送で報告］ に設定する必要があります。詳しくは、「転送でフィッシングメールを報告」を参照してください。
- フィードカードの機能拡張： Secure Mail for Android では、既存のフィードフォルダーの以下の機能が拡張されています：
  - 自動同期されたすべてのフォルダーからの会議への出席依頼がフィードカードに表示されます。
  - 近日中の会議がフィードカードに最大 5 つ表示されます。
  - 近日中の会議は、現在の時刻から 24 時間以内に開催されるものが表示されます。これらの会議への出席依頼は ［今日］ と ［明日］ に分類されます。
    以前のリリースには、当日中に開催される近日中の会議がフィードに表示されていました。
- **Secure Mail** のカレンダーイベントのエクスポート： Secure Mail for Android および Secure Mail for iOS を使用すると、Secure Mail の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］ をタップして、「カレンダーイベントをエクスポート」スライダーを右にドラッグします。詳しくは、「Secure Mail の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。

Secure Mail 10.8.65

- **iOS 12** で利用可能： Secure Mail for iOS では、グループ通知機能がサポートされています。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。

- Secure Mail for iOS では、［下書きの保存］ ボタンと ［下書きの削除］ ボタンが大きくなります。この機能拡張により、お客様がそれぞれのオプションを区別しやすくなります。
- Secure Mail for iOS 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、Secure Mail の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、着信した場合にアプリの名前が発信者 ID 付きでデバイスに表示されます。例えば「Secure Mail Caller ID: Joe Jay」などです。詳しくは、「Secure Mail 発信者 ID」を参照してください。

Secure Mail 10.8.60

- Secure Mail は Android P をサポートしています。
- Secure Mail はポーランド語での利用が可能になりました。
- Secure Mail for iOS 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。詳しくは、「iOS の機能」を参照してください。

Secure Mail 10.8.55

Secure Mail バージョン 10.8.55 には新機能はありません。解決された問題については、「既知の問題と解決された問題」を参照してください。

Secure Mail 10.8.50

写真の添付の機能強化。Secure Mail for iOS では、新しく追加された ［ギャラリー］ アイコンをタップして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て、メールに添付する写真を選択します。

Secure Mail のフィード画面。Secure Mail for iOS および Secure Mail for Android では、未読メール、対応が必要な会議出席依頼、近日中の会議がすべて ［フィード］ 画面に表示されます。

Secure Mail 10.8.45

フォルダーの同期。Secure Mail for iOS および Secure Mail for Android で ［同期］ アイコンをタップすると、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、Secure Mail の［メールボックス］、［カレンダー］、［連絡先］、［添付ファイル］などのスライドアウトパネルに表示されています。［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、自動更新が設定されているフォルダーが更新されます。［同期］ アイコンの横に、前回の同期のタイムスタンプが表示されます。

写真の添付の機能強化。Secure Mail for Android では、新しく追加された ［ギャラリー］ アイコンをタップして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て、メールに添付する写真を選択します。

Secure Mail 10.8.40

カレンダーの検索のサポート。Secure Mail for iOS のカレンダーで、イベント、出席者、または文字列を検索できます。

Secure Mail 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、会議通知に応答できます（応答オプションは［承諾］、［辞退］、［仮承諾］など）。また、メッセージ通知に応答することもできます（応答オプションは［返信］、［削除］）。
- **Secure Mail for Android** の戻るボタンの強化。Secure Mail for Android では、デバイスの戻るをタップして、フローティング操作ボタンのオプションを閉じることができます。フローティング操作ボタンが展開状態の時に、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。これにより、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、会議への出席依頼に対する応答ボタンがメールに表示されます。会議出席依頼に関するメール受信通知を受け取った時に、次のいずれかのオプションをタップして返信することができます:
  - はい
  - 仮承諾
  - いいえ

Secure Mail 10.8.25

Secure Mail for iOS は、派生資格情報として **S/MIME** をサポートするようになりました: この機能が正しく動作するようにするには、以下を行う必要があります。

- ［S/MIME 証明書のソース］で［派生資格情報］を選択します。詳しくは、「iOS の派生資格情報」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。次の情報を使用します:
  - 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たデバイスの登録方法について詳しくは、「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］ 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 プラットフォームに表示されている［S/MIME 証明書のソース］で、［派生資格情報］ を選択します。

Secure Mail for iOS および **Secure Mail for Android** の外観と操作性が刷新されました： ユーザーが、よりシンプルかつ効率的に操作できるようになっています。Secure Mail のメニューボタンと操作ボタンの配置を、ナビゲーションバー形式に変更しました。ユーザーの操作性がどのように変わったかについて、以下のビデオを参照してください：

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。

変更内容：

- グラバーハンドを廃止しました。［メール］、［カレンダー］、［連絡先］、［添付ファイル］などの Secure Mail 機能は、フッタータブバーにボタンとして表示されます。次の図は、この変更内容を示しています。

  > 注：
  >
  > Android デバイスでは、メールアイテムを開いた後はフッタータブバーが表示されません。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表示されません。

- ［設定］ メニューは、［メール］、［カレンダー］、［連絡先］、［添付ファイル］などのすべてのメニューで表示されます。［設定］ に移動するには、ハンバーガーアイコンをタップし、右下の［設定］ボタンをタップします（下図参照）。
- ［検索］ アイコンは［検索］バーに代わるもので、［受信トレイ］、［連絡先］、［添付ファイル］の各画面に表示されます。
- iOS デバイスでは、メールアイテムをタップしたまま長押しすると、そのアイテムが選択されます。
- 次の図に示すように、作成のフローティング操作ボタンをタップして新しいメールを作成できます。
- 次のメニューオプションが画面の右上に表示されるようになりました：
  - 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、［追加オプション］**>**［同期］ のオプションに移動して、同期設定を変更できます。

    > 注：
    >
    > このオプションは、Android デバイスでのみ表示されます。

  - ［検索］アイコン： タップすると、メールを検索できます。
- トリアージ表示アイコン： タップすると、会話をトリアージ表示できます。
- 応答のフローティング操作ボタン： メールの表示中に、［転送］、［全員に返信］、または［返信］ボタンをタップしてメールに応答できます（下図参照）。

- メールの表示中、次のメニューオプションが画面の右上に表示されます:
  - フラグ: タップすると、メールにフラグが付きます。
  - 未読にする: タップすると、メールを未読状態にできます。
  - 削除: タップすると、メールが削除されます。
  - 追加オプション: オーバーフローアイコンをタップすると、[移動] など、他の利用可能な操作が表示されます。

カレンダーの変更

- カレンダーで、イベントのフローティング操作ボタンをタップしてイベントを作成することができます（下図参照）。
- 次のメニューオプションが画面の右上に表示されるようになりました:
  - 今日: タップすると、今日のイベントが表示されます。
  - 検索: タップすると、イベントを検索できます。
  - 応答のフローティング操作ボタン: イベントの表示中に、[転送]、[全員に返信]、または [返信] ボタンをタップして応答できます。

イベントを表示すると、[はい]、[仮承諾]、[いいえ] などの応答操作ボタンがイベントの詳細の下に表示されるようになりました。

連絡先の変更

- [新しい連絡先を作成] フローティング操作ボタンをタップして、新しいメールを作成できます（下図参照）。
- [検索] メニューオプションは、画面の右上に表示されるようになりました。このオプションをタップすると、連絡先を検索できます。
- 連絡先の表示中、次のメニューオプションが画面の右上に表示されます:

  Android デバイスの場合:

  - 編集: タップすると、連絡先を編集できます。
  - 追加オプション: オーバーフローアイコンをタップすると、[メールに添付]、[共有]、[削除] など、他の利用可能な操作が表示されます。

  iOS デバイスの場合:

  - 編集: タップすると、連絡先を編集できます。
  - 共有: [共有] アイコンをタップすると、[連絡先の共有] や [メールに添付] など、他の利用可能な操作が表示されます。

  > 注:

> iOS デバイスで連絡先を削除するには、削除する連絡先を選択して ［編集］ をタップし、画面の下部にある ［削除］ をタップします（下図参照）。

添付ファイルの変更

次の添付ファイルメニューオプションが画面の右上に表示され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て適切なフィルタを選択すると、添付ファイルを並べ替えることができます。
- 検索: タップすると、添付ファイルを検索できます。

Secure Mail 10.8.20

- Secure Mail for iOS で、派生資格情報を使用した登録と認証がサポートされるようになりました。派生資格情報について詳しくは、「iOS の派生資格情報」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ます。リッチ通知機能により、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の通知を確実に受信できます。この機能は、パスワードベースの認証セットアップとクライアントベースの認証セットアップでサポートされています。詳しくは、「リッチプッシュ通知」を参照してください。

  > 注:
  >
  > このリッチプッシュ通知機能をサポートするアーキテクチャが変更されたため、**VIP** のみのメール通知は利用できなくなりました。

- Secure Mail for Android、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。メールの署名に画像やリンクを使用できます。詳しくは、「リッチテキスト署名」を参照してください。

Secure Mail 10.8.15

- **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。メールの署名に画像やリンクを使用できます。詳しくは、「リッチテキスト署名」を参照してください。
- **Secure Mail** は **Android Enterprise**（以前の **Android for Work**）をサポートします。Secure Mail で Android Enterprise アプリを使用することで、別の仕事用プロファイルを作成できます。詳しくは、「Secure Mail の Android Enterprise」を参照してください。
- **Secure Mail** は電子メールを表示しながら埋め込みリソースをレンダリングします。リソースが内部ネットワークにある場合（内部リンクである画像 URL が記載されたメールなど）、Secure Mail は内部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、先進認証をサポートしています。先進認証は、ユーザー名とパスワードを使用した OAuth トークンによる認証です。Office 365 の内部および外部 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）をサポートします。

- 添付リポジトリのパフォーマンスの強化。Attachments リポジトリをすばやくスクロールすることができます。

Secure Mail 10.8.10

- 添付ファイルの印刷をサポート。Secure Mail for iOS は、メールの添付ファイルの印刷をサポートしています。
- **Microsoft Office 365** の先進認証。Secure Mail for iOS は、先進認証をサポートしています。先進認証は、ユーザー名とパスワードを使用した OAuth トークンによる認証です。Office 365 の外部および内部 Active Directory フェデレーションサービス（AD FS）および ID プロバイダー（IdP）をサポートします。

  > 注:
  >
  > – このリリースでは、Endpoint Management と Microsoft Intune/EMS との統合で先進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できる場合の先進認証が含まれています。

  詳しくは、「Microsoft Office 365 を使用した先進認証」を参照してください。

既知の問題と解決された問題

May 17, 2019

バージョン **19.5.0** の既知の問題

iOS を実行しているデバイスでは、MDX ポリシーの許可された **Wi-Fi** ネットワークで定義されている許可されている WI-FI ネットワーク以外の Wi-Fi ネットワークに接続できます。この問題により、MDX ポリシーに登録されていないネットワークを介して、Secure Mail for iOS および Secure Web for iOS を開くことができます。[CXM-66730]

バージョン **19.5.0** で解決された問題

- Secure Mail for Android では、新しいメールの作成時にメールアドレスを ［宛先**:**］ または ［**CC/BCC:**］ フィールドに貼り付けることができません。ただし、メールの返信時にはメールアドレスを ［宛先**:**］ または ［**CC/BCC:**］ フィールドに貼り付けることができます。[CXM-64752]
- Secure Mail for Android では、Android Enterprise デバイスの登録時にアカウント構成設定を保存できません。[CXM-65138]

Secure Mail for Android 19.4.6 の既知の問題と解決された問題

このリリースでは既知の問題および解決された問題はありません。

以前のバージョンでの既知の問題と解決された問題

バージョン **19.4.5** 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。

バージョン **19.4.5** で解決された問題

- Secure Mail for iOS の場合、Outlook で送信された会議要求を Secure Mail で編集すると、Outlook で会議が更新されません。受信者にも更新が通知されません。この問題は、Secure Mail で会議要求を作成し、Secure Mail で編集するときにも発生します。[CXM-62511]
- Secure Mail for iOS では、カレンダーが同期せず「Couldn't sync Calendar」というエラーが表示されます。[CXM-62796]
- Secure Mail for Android では、Outlook を使用して作成した会議要求が、Secure Mail のカレンダーに反映されないことがあります。[CXM-63552]
- Secure Mail for Android では、定期的な会議が遅れた時間に表示され、会議を更新しても正しく同期されません。[CXM-65263]

バージョン **19.3.5** 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。

バージョン **19.3.5** で解決された問題

- Secure Web for iOS では、ブラウザーに bitly URL をペーストすることができません。[CXM-56276]
- Secure Mail for iOS では、受信するすべてのメールで次の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 を起動してください。[CXM-56418]
- Secure Mail for iOS 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を使用できません」というエラーメッセージが頻繁に表示されます。[CXM-59776]
- 多要素認証に切り替えた後、Secure Mail for iOS が同期に失敗します。[CXM-62176]

Secure Mail 19.3.0 の既知の問題

このバージョンには既知の問題はありません。

バージョン **19.3.0** で解決された問題

Secure Mail for iOS

Secure Mail for iOS では、無効なネットワークセッションによって要求のタイムアウトが発生した場合、メールを受信すると次の通知バナーが断続的に表示されます：要求がタイムアウトになったため、**Secure Mail** がこのメッセージを取得できません。[CXM-62561]

Secure Mail for Android

- Secure Mail for Android で、mozaiekwonen.xm.cloud.com から Firebase Cloud Messaging（FCM）通知を受信できません。[CXM-62146]
- Secure Mail for Android でカレンダーイベントを更新しても、変更内容は Outlook Office 365 と同期しません。[CXM-62227]
- Secure Mail for Android では、ネットワーク接続が不十分な場合、またはネットワーク接続がない場合、添付ファイルを含むメールは送信されません。これらのメールは、ネットワーク接続が復元された後も送信トレイに残ります。[CXM-64297]

バージョン **19.2.0** の既知の問題

Secure Mail for iOS では、証明書の透明性オプションで Online Certificate Status Protocol（OCSP）Stapling 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。

バージョン **19.2.0** で解決された問題

Secure Mail for iOS

Secure Mail for iOS 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。[CXM-61060]

Secure Mail for Android

- Secure Mail for Android では、Samsung デバイスで予測入力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。最後にスペースが挿入されていない場合、署名の最後の単語に下線が残ったまま保存され、受信者にもそのまま表示されます。[CXM-60894]
- Secure Mail for Android では、メールの要約を受信する場合に画像が表示されません。[CXM-62280]
- Intune ポータルサイトバージョン 5.0.4324.0 がインストールされている場合、Secure Mail for Android は起動時にクラッシュします。詳しくは、Support Knowledge Center の記事を参照してください。[CXM-62516]

Secure Mail for iOS バージョン **19.1.6** の既知の問題と解決された問題

バージョン 19.1.6 で既知の問題および解決された問題はありません。

以下の問題は以前のバージョンで解決されています：

バージョン **19.1.5** の既知の問題

バージョン 19.1.5 には既知の問題はありません。

バージョン **19.1.5** で解決された問題

バージョン 19.1.5 では、次の問題が解決されています。

- Secure Mail for iOS では、受信するすべてのメールで次の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** を起動してください。 [CXM-56418]
- Secure Mail for iOS 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を使用できません」というエラーメッセージが頻繁に表示されます。[CXM-59766]
- ラッピングされた Android アプリでは、ユーザーエージェント文字列が複数回追加され、ヘッダーのサイズが大きくなります。これによってエラーが発生し、ページの読み込みに失敗します。[CXM-59869]

バージョン **19.1.0** で解決された問題

Secure Mail for iOS

- Secure Mail が Exchange Server への接続に失敗すると、メールの通知バナーに次のメッセージが表示されていました：

  「セッションが期限切れになったため、このメッセージを取得できません。Secure Mail を開いてセッションを更新してください。」

  この問題の解決策として、メッセージが次のように修正されました：

  「Secure Mail が組織のネットワークに接続できません。管理者に連絡してください。」[CXM-59128]

- O365 メールボックスを使用しているユーザーの場合、はい、いいえ、どちらでもない、削除などで通知応答アクションを繰り返し実行すると、Office 365 でスロットルが発生し、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。再試行してください。」[CXM-60123]

Secure Mail for Android

- Secure Mail for Android では、トルコ語を使用している場合、アドレスに「I」という文字が含まれる宛先にメールを送信できません。[CXM-59093]

- Secure Mail for Android では、ユーザーはメールの件名を選択して強調表示することができません。[CXM-59185]
- Secure Mail for Android では、パスワードにユーロ記号（€）が含まれている場合、ログオンに失敗します。[CXM-59654]
- Secure Mail for Android では、［ローカルの連絡先と同期する］ 設定が有効になっている場合、Secure Mai のすべての連絡先がネイティブの連絡先にエクスポートされます。同期後、携帯、職場、自宅、職場 FAX、自宅 FAX などの電話番号フィールドが正しい順序で表示されません。たとえば、ネイティブの連絡先でファックス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。[CXM-57994]

バージョン **18.12.0** で解決された問題

Secure Mail for iOS

- Secure Mail for iOS でリッチテキスト形式（RTF）でメールを受信するときに、特定の種類のインライン添付ファイルおよび添付ファイルのアイコンが表示されません。[CXM-59121]
- Secure Mail for iOS でリッチプッシュ通知が有効になった状態で［メール通知］をオフ/オンにすると、［メールの種類］ オプションが表示されることがあります。[CXM-59122]

Secure Mail for Android

- お使いの環境でクライアントベースの認証を行っている場合、Secure Mail で自動同期が失敗することがあります。手動で同期を実行すると、少数のメールのみが取得されます。[CXM-59650]

バージョン **18.11.1** で解決された問題

- Secure Mail for Android で IBM Notes Traveler 9.0.1 SP 10 に接続している場合、添付ファイル付きのメールが送信されずに送信トレイに残ります。[CXM-58962]

バージョン **18.11.0** で修正された問題

- Secure Mail for Android で、メールに埋め込まれた画像を表示できません。[CXM-53556]
- Secure Mail for Android は、URL が埋め込まれた署名を含むメールを開くとクラッシュします。例: `file://C:\...jpg`. [CXM-58219]

バージョン **18.10.5** で解決された問題

Secure Mail for iOS

- ［iOS データ保護を有効化］MDX ポリシー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表示されます。[CXM-55491]

- 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。[CXM-57030]

Secure Mail for Android

- ユーザーが Exchange ActiveSync バージョン 16 以降を実行しているアカウントの定期的な会議を変更しても、Exchange Server でこの会議は更新されません。その結果、Secure Mail と Outlook の間で会議が同期されません。[CXM-57200]

Version 18.10.0 で解決された問題

- Secure Mail for Android で、Exchange サーバー以外のサーバーを指すインラインイメージを表示できません。[CXM-56736] [CXM-55843]
- Secure Mail for Android で、Webex 会議に参加している間、PIN 番号にダイヤルイン番号が付加されませんでした。手動で PIN 番号を入力する必要があります。[CXM-56002]
- 個人用カレンダーが設定されていない場合、Secure Mail for Android でカレンダーをエクスポートしようとすると、クラッシュします。[CXM-56264]
- iPhone XS 上の Secure Mail for iOS で、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。[CXM-57030]

Version 18.9.0 で解決された問題

Secure Mail for Android

- クライアントワークステーションは、NT LAN Manager（NTLM）認証要求ごとにランダムに変更されます。[CXM-55177]
- デバイスがバッテリー節約モードになると、Secure Mail と Android P の同期が断続的に動作を停止します。[CXM-55441]
- 個人カレンダーが設定されていない場合、Secure Mail カレンダーをエクスポートしようとすると、Secure Mail がクラッシュします。[CXM-56264]

バージョン **10.8.65** で解決された問題

Secure Mail for iOS

- FIP が有効な場合に iOS 11.3 デバイスで Secure Mail for iOS を実行すると、MDX ポリシーの切り取り、コピー、貼り付けが想定どおりに機能しません。[CXM-53993]
- 共有デバイスで Secure Mail for iOS を使用すると、新規ユーザーはログオフしていても以前のユーザーのメールを表示できます。新規ユーザーがフォルダをタップして表示を更新すると、以前のユーザーのメールは表示されなくなります。[CXM-55176]

バージョン **10.8.60** で解決された問題

> 注:
>
> Secure Mail バージョン 10.8.25 ～ 10.8.60 に既知の問題はありません。

- IBM Lotus Domino サーバー上で動作する Secure Mail for iOS では、受信トレイで検索アイコンを使用できません。[CXM-53782]
- Intune ポータルサイトで Secure Mail for Android を実行しているデバイスを登録すると、Secure Mail は機能しなくなります。[CXM-54178]
- FTU のフロー中に多数のメールフォルダーをサーバーから同期すると、Secure Mail for iOS がクラッシュします。[CXM-54371]
- Secure Mail for iOS で PDF の印刷プレビューが小さく表示されます。[CXM-54482]
- Secure Mail for Android で、メールに返信するときに複数のメール ID が自動的に入力されません。[CXM-54811]

バージョン **10.8.55** で解決された問題

- iPad Pro で横向きにすると、Secure Mail for iOS のカレンダーの週単位表示が正しく表示されないことがあります。[CXM-53723]

バージョン **10.8.55** で解決された **MDX** 関連の問題

- Android で Secure Hub からサインアウトしようとすると、Secure Mail がクラッシュします。[CXM-53930]
- 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。[CXM-54089]

バージョン **10.8.50** で解決された問題

- Secure Mail for iOS でビデオファイルを ShareFile に保存できません。[CXM-42238]
- Secure Mail for Android でプッシュ通知を有効にした場合、新規メールの通知を受信できません。この問題は断続的に発生します。[CXM-53135]

バージョン **10.8.45** で解決された問題

Secure Mail バージョン 10.8.45 で解決された問題はありません。

バージョン **10.8.40** で解決された問題

Secure Mail for iOS では、メールを受信するたびに通知が重複して表示されることがあります。[CXM-51473]

バージョン **10.8.35** で解決された問題

- Secure Mail for Android では、自動同期が断続的に停止します。Office 365 サーバーから受信した新しいメッセージを Secure Mail に表示するには、手動で同期する必要がある場合があります。[CXM-49354、CXM-52716]
- Secure Mail for Android では、メール受信とカレンダーイベントのメール通知を Secure Mail で無効にしても、通知が引き続き表示され、通知音が鳴ります。[CXM-50479]
- Secure Mail for Android で終日イベントを作成すると、Outlook のカレンダーに間違った日付が表示されます。[CXM-50612]
- Secure Mail for Android では、Exchange の個人用連絡先グループがアプリと同期しません。[CXM-51190]
- そのため、SSO を構成しても、Secure Mail for Android から Exchange への SSO が失敗します。ユーザーは、サインインパスワードの入力を求められます。[CXM-51343]

バージョン **10.8.25** で解決された問題

- Secure Mail for Android では、カレンダーへの招待を Office 365 と同期した場合に遅延が生じます。この問題は、カレンダーへの招待の作成または更新時に発生します。[CXM-49596]
- Secure Mail for Android では、［CC］フィールドに 1 文字だけ入力して ［送信］ をタップした場合、次の問題が発生します：よく使う連絡先リストの最初のユーザーにメッセージが送信されます。回避策として、［CC］フィールドへの入力が無効であるという通知が表示される必要があります。[CXM-50476]
- Android 7 を実行している Zebra T51 デバイスに、Citrix Launcher アプリをインストールできません。[CXM-50621]
- NetScaler Gateway が証明書ベースの認証を使用するように設定されている場合、次の問題が発生します：Secure Mail for iOS 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。回避策として、差出人の名前、件名、メッセージのプレビューを含めた通知が表示される必要があります。[CXM-51075]

バージョン **10.8.20** で解決された問題

- Intune ポータルサイトアプリが、Endpoint Management に MAM-only モードで登録された Android デバイスにインストールされている場合、Secure Mail は 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ていません。アプリを構成するには、管理者に問い合わせてください。」[CXM-48135]
- Secure Mail for Android で、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と、サインインに失敗します。[CXM-48197]
- Android デバイスで再起動すると、Secure Mail にアクセスするための認証をバイパスできます。[CXM-48444]
- Secure Mail for Android で、インラインイメージ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滞留します。この問題は、設定で ［画像を表示する］ が有効になっている場合に発生します。

[CXM-49222]

- Secure Mail for iOS で、IRM ポリシーが ［オン］ で、かつメール分類が ［保護する］ に設定されている場合、メール全体をダウンロードしたときに添付ファイルを表示することはできません。[CXM-49544]

バージョン **10.8.10** で解決された問題

Secure Mail for iOS

- Secure Mail 10.7.25 for iOS に更新後、メールヘッダー（Message-ID）からかっこ（）が削除されます。[CXM-46029] および >
- Secure Mail for iOS でユーザーが Outlook からカレンダーの招待を追加した後、断続的にアプリがクラッシュします。この問題は、カレンダーの招待に絵文字が含まれている場合に発生します。[CXM-46250]
- iOS では、業務用モバイルアプリを 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と、Secure Mail の動作が遅くなり、開いたままにするとクラッシュします。[CXM-46721]
- Secure Mail for iOS で［ロック画面上の通知を制御］ポリシーが ［件数のみ］ に設定されている場合、断続的に重複した通知が表示されます。[CXM-47461]

Secure Mail for Android

Secure Mail for Android 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して貼り付けると、アプリがクラッシュします。[CXM-46578]

バージョン **19.1.0** の既知の問題

バージョン 19.1.0 には既知の問題はありません。

Secure Mail の展開

March 11, 2019

Citrix Endpoint Management（XenMobile の新名称）と統合された Secure Mail を展開するには、次の一般的な手順に従います:

1. Secure Mail を Exchange Server または IBM Notes Traveler Server と同期するために、Secure Mail を Microsoft Exchange または IBM Notes と統合できます。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。Active Directory の資格情報を使用して、Exchange または IBM Notes Traveler サーバーで認証を受けます。詳しくは、「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 からのメールを IBM Notes Traveler（旧称：IBM Lotus Notes Traveler）と同期させることはできません。この Lotus Notes サードパーティー機能は、現在サポートされていません。そのため、応答済の会議メールを Secure Mail から削除しても、このメールは IBM Notes Traveler サーバー上では削除されません。カレンダーイベントを承諾し、その後コメント付きでイベントを辞退したり、コメント付きでアクションを実行したりしても、そのコメントは表示されません。[CXM-47936] IBM/Lotus Notes の既知の制限事項については、Citrix ブログの投稿を参照してください。

2. オプションとして、Secure Hub から SSO を有効にできます。これを行うには、Endpoint Management コンソールで Citrix Files アカウント情報を設定して、Citrix Files の SAML ID プロバイダとして Endpoint Management を有効にします。Active Directory の資格情報を使用して、Citrix Files で認証を受けます。

   Endpoint Management コンソールでの Citrix Files アカウント情報の設定は、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 回だけの設定です。詳しくは、「Endpoint Management コンソールで SSO 用の Citrix Files アカウント情報を設定するには」を参照してください。

3. Citrix ダウンロードサイトから Secure Mail の.mdx ファイルをダウンロードします。
4. Secure Mail を Endpoint Management に追加して、MDX ポリシーを構成します。詳しくは、「[アプリの追加]」を参照してください。(/ja-jp/citrix-endpoint-management/apps.html)

> 注:
>
> Secure Mail バージョン 10.6.5 では、Secure Mail for iOS および Secure Mail for Android で新しい MDX 分析ポリシーを構成できます。シトリックスは分析データを収集して製品の質を向上させます。Google Analytics レベルの詳細ポリシーにより、データを会社のドメインに関連付けするか、匿名で収集するかを指定できます。［匿名］ を選択すると、会社ドメインと収集されたデータの関連付けからユーザーが除外されます。この新しいポリシーによって、以前の Google Analytics ポリシーが置き換えられます。

ポリシーが［匿名］に設定されると、以下の種類のデータが収集されます。シトリックスがユーザーを特定できる情報を要求することはないため、このデータが個別のユーザーに関連付けられることはありません。個人を特定できる情報が Google に送信されることはありません。

- デバイス統計情報。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。
- プラットフォーム情報。ActiveSync のバージョンおよび Secure Mail サーバーのバージョンなど。
- 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、カレンダーの同期など、製品品質の障害ポイント。

ポリシーが ［完了］ に設定されると、会社ドメイン以外の識別可能な情報は収集されません。デフォルトは ［完了］ です。

Secure Mail の構成

February 11, 2019

Secure Mail で次の機能の構成および統合ができます。

- Secure Mail と Microsoft Intune/EMS との統合
- Office 365 の先進認証
- Secure Mail のバックグラウンドサービス
- Exchange Server または IBM Notes Traveler Server の統合
- Secure Mail の S/MIME
- Secure Mail の SSO

Secure Mail と Microsoft Intune/EMS との統合

February 19, 2019

この統合により、Citrix Secure Mail をより安全に管理および配信し、生産性を向上させることができます。

Secure Mail はさまざまな Intune 構成に対応します。オンプレミスの Exchange または Office 365 のメールボックスに接続できます。Endpoint Management と EMS/Intune との統合をセットアップするには、「Citrix Endpoint Management と Microsoft Intune/EMS との統合」を参照してください。

Secure Mail は以下の展開モードをサポートします:

- Intune MAM
- Intune MAM および Intune モバイルデバイス管理（MDM：Mobile Device Management）
- Intune MAM と Endpoint Management MDM-only
- Intune MAM と Endpoint Management MDM および MAM

サポートされているメールサーバー

- Exchange Online
- Exchange Server 2016
- Exchange Server 2013

制限事項

Secure Mail では、証明書ベースの認証はサポートされていません。

> 重要:
>
> MDM モードの Secure Mail を Citrix Endpoint Management（MDM および MAM モード）と使用するには、環境で Secure Hub を構成する必要があります。

Secure Mail for Intune を構成するには

環境で MDM モードの Citrix Endpoint Management が構成されている場合、Secure Mail によって自動的に FTU エクスペリエンスにユーザー名が入力されます。

この機能を有効にするには、Endpoint Management コンソールでカスタムポリシーを構成する必要があります。詳しくは、Endpoint Management のドキュメントで「Secure Mail を構成するには」を参照してください。

Intune と互換性のない機能

以下の Secure Mail 機能は、Endpoint Management と EMS/Intune との統合で使用できません:

- Secure Ticket Authority（STA）
- シングルサインオン（SSO）によるメール登録
- リッチプッシュ通知
- Citrix Files（ShareFile の新名称）
- S/MIME 署名と暗号化
- Microsoft Information Rights Management
- セキュアブラウズ + 非 KCD SSO 内部 Exchange Server

Microsoft Office 365 の先進認証

February 19, 2019

Secure Mail は、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）で Microsoft Office 365 の先進認証をサポートしています。先進認証は、ユーザー名とパスワードを使用した OAuth トークンによる認証です。iOS デバイスを使用している Secure Mail ユーザーは、Office 365 に接続するときに、証明書ベースの認証を利用できます。Secure Mail にサインインするときに、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、次の操作を行います:

1. Microsoft Office 365 の先進認証（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、ファイアウォール内の Office 365 エンドポイント、URL、IP アドレス範囲を有効にします。詳しくは、Microsoft のドキュメントでOffice 365 の URL と IP アドレスの範囲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** の認証メカニズム: このポリシーは、Office 365 でアカウントを構成する時に認証に使用する OAuth メカニズムを示します。このポリシーでは、次の値を構成する必要があります:
  - **OAuth** を使用しない: このポリシーは、アカウントの構成時に基本認証で使用します。
  - **OAuth** でユーザー名とパスワードを使用する: このポリシーは、認証時に OAuth プロトコルで使用します。ユーザーは、OAuth のフローで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: このポリシーは、証明書ベースの認証を実行するよう Office 365 が構成されている場合に使用します。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:

- **Office 365** に先進認証を使用: このポリシーは、認証時に OAuth プロトコルで使用します。
- 先進認証用のカスタムユーザーエージェント: このポリシーを使用して、先進認証でデフォルトのユーザーエージェント文字列を変更します。

iOS と **Android** 端末に共通するポリシー:

- 信頼された **Exchange Online** ホスト名: このポリシーを使用して、アカウントの構成時に、認証に OAuth メカニズムを使用する信頼できる Exchange Online のホスト名一覧を定義します。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。この一覧には、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: このポリシーを使用して、Office 365 OAuth 認証中にパスワードを入力する Web ページの、信頼できる AD FS ホスト名一覧を定義します。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。一覧が空の場合、Secure Mail はパスワードを自動入力しません。Secure Mail は、ホスト名一覧を Office 365 認証中に検出された Web ページのホスト名と照合し、そのページが HTTPS プロトコルを使用しているかを確認します。たとえば、`sts.company.com`がホスト名一覧にある場合、ユーザーが`https://sts.company.com`にアクセスすると、パスワードフィールドがあれば、Secure Mail がパスワードを入力します。デフォルト値は`login.microsoftonline.com`です。
- **Secure Mail Exchange Server**: このポリシーを使用して、Exchange Server のアドレスを定義します。

Secure Mail for iOS では、ポリシーがデバイス上で更新されると先進認証が有効になります。

制限事項

- 環境で先進認証を使用している場合、iOS のリッチプッシュ通知機能は利用できません。リッチプッシュ通知について詳しくは、「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するセットアップでは、複数アカウントはサポートされていません。

Secure Mail ポリシー

次の 2 つの表は、Exchange インフラストラクチャごとに必要な Secure Mail ポリシーです。

Exchange インフラストラクチャ	Office 365 の認証メカニズム/Office 365 に先進認証を使用	信頼された AD FS ホスト名	信頼された Exchange Online ホスト名
オンプレミス	オフ	-	-
ハイブリッド *	オン	AD FS/IDP	`Outlook.office365.com`またはバニティ URL
Exchange Online	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	Secure Mail の Exchange Server	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 の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 のホスト名	オンプレミス、Exchange のオンプレミスホスト名	オンプレミス、Exchange のオンプレミスホスト名、AD FS/IDP（内部のみ）
Exchange Online	`Outlook.office365.com`	Exchange Online のホスト名	Exchange のオンプレミスホスト名、AD FS、IDP

*Secure Mail は、ハイブリッド Exchange インフラストラクチャと移行されたメールボックスの使用をサポートします。

オンプレミスユーザーのメールボックスが Exchange Online に移行されると、Secure Mail は自動的にこの変更を検出し、先進認証を使用するよう求めるメッセージをユーザーに表示します。アカウントを再構成する必要はありません。

> 注:
>
> バックグラウンドネットワークサービスは、メールサーバーと AD FS が内部にある場合にのみ構成します。

Secure Mail での **OAuth** のサポートマトリックス

次の表は、iOS および Android デバイス上の Secure Mail に関する OAuth のサポートマトリックスです:

認証の種類	IDP/外部 AD FS	IDP/内部 AD FS	Azure AD	Intune
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

Secure Mail のバックグラウンドサービス

April 18, 2019

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。Citrix Endpoint Management（XenMobile の新名称）に Secure Mail を追加する場合、MDX アプリポリシー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. Endpoint Management コンソールに管理者資格情報を使用してサインオンします。
2. コンソールで、［構成］ タブ、［アプリ］ をクリックし、Secure Mail アプリを選択してから ［編集］ をクリックします。
3. ［**MDX** ポリシー設定］ ページの ［プラットフォーム］ セクションで、必要に応じて iOS または Android プラットフォームを選択します。
4. ［アプリ設定］ セクションで、ポリシーを構成します。

バックグラウンドサービス構成の **MDX** アプリポリシー

次の 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、メールサーバーとの通信に関連しています。

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制限なしでインターネットを経由するかを指定します。

- ネットワークアクセスポリシーが内部ネットワークへトンネル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の一覧にある URL のみが Citrix Gateway を通過します。残りのトラフィックは、制限なしでインターネットを経由します。デフォルトでは、Secure Mail のアクセスは内部ネットワークへトンネルです。
- ネットワークアクセスポリシーが制限なしに設定されている場合、Secure Mail からの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。VPN はバックグラウンドサービスへのアクセスには使用されません。

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。

バックグラウンドネットワークサービス： バックグラウンドネットワークサービスポリシーは、Citrix Gateway 経由でアクセスできるメールサーバーの一覧を指定します。ホスト名とポート番号をコンマ区切りの値で表示します。値の先頭と末尾に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が含まれます。例: mail1.example.com:443,mail2.example.com:443（コンマの間にスペースは入れないでください）。

バックグラウンドネットワークサービスゲートウェイ： 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は、メールサーバーに接続するために Secure Mail が使用する Citrix Gateway を指定します。Citrix Gateway のアドレスには、citrixgatewayFQDN:portnumberが含まれます。例: gateway3.example.com:443。

バックグラウンドサービスチケットの有効期間： 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。Citrix Gateway を介して Secure Mail がメールサーバーに接続する場合、Citrix Endpoint Management は内部メールサーバーへの接続に Secure Mail が使用するトークンを発行します。Secure Mail がこのトークンを使用できる期間は、この設定によって指定されます。トークンがアクティブな場合、認証とメールサーバーに接続するための新しいトークンは必要ありません。有効期限が切れた場合は、ユーザーは再度ログオンして新しいトークンを生成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）です。

バックグラウンドサービスの MDX アプリポリシーについて詳しくは、以下を参照してください：

- Secure Mail アプリ設定ポリシー（Android）
- Secure Mail アプリ設定ポリシー（iOS）

以下の図は、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。

以下の図は、メールサーバーに対する Secure Mail 接続の種類を示しています。それ以降の各図は、関連のポリシー設定の一覧です。

メールサーバーへの直接接続：

メールサーバーに対する直接接続のポリシー：

- ネットワークアクセス：制限なし

ネットワークアクセスが制限なしの場合、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: N/A
- バックグラウンドサービスチケットの有効期間: N/A
- バックグラウンドネットワークサービスゲートウェイ: N/A

STA 経由のメールサーバーへの接続:

STA 経由でメールサーバーに接続するポリシー:

- ネットワークアクセス: 内部ネットワークへトンネル
- 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`
- バックグラウンドサービスチケットの有効期間: **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:
>
> STA 接続は長期間のセッション接続をサポートするため、Secure Mail に STA 接続を使用することをお勧めします。

STA について詳しくは、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

February 11, 2019

Secure Mail とメールサーバーとの同期を維持するため、Secure Mail を内部ネットワーク内または Citrix Gateway の背後の Exchange Server または IBM Notes Traveler サーバーと統合します。

- 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。
- IBM Notes Traveler Server for Secure Mail 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 からのメールを IBM Notes Traveler（旧称: IBM Lotus Notes Traveler）と同期させることはできません。この Lotus Notes サードパーティー機能は、現在サポートされていません。そのため、たとえば、応答済の会議メールを Secure Mail から削除しても、このメールは IBM Notes Traveler サーバー上では削除されません。[CXM-47936]
> IBM/Lotus Notes の既知の制限事項については、Citrix ブログの投稿を参照してください。

また、Secure Notes および Secure Tasks も同期できます。ただし、Secure Notes および Secure Tasks は 2018 年 12 月 31 日に製品終了（EOL）となったことにご注意ください。詳しくは、「EOL と廃止予定のアプリ」を参照してください。

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

Citrix Endpoint Management（XenMobile の新名称）に Secure Mail、Secure Notes、Secure Tasks を追加する場合、「バックグラウンドサービス構成の MDX アプリポリシー」で説明されているように MDX ポリシーを構成します。

> 注:
>
> Secure Mail for Android および Secure Mail for iOS では Notes Traveler Server をフルパスで指定できます。例: `https://mail.example.com/traveler/Microsoft-Server-ActiveSync`。
>
> Domino Directory に Traveler サーバーの Web サイト置換規則を構成する必要はなくなりました。

Secure Mail 用の IBM Notes Traveler Server 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、この構成の環境図およびシステム要件について説明します。

> 重要:
>
> Notes Traveler サーバーが SSL 3.0 を使用する場合、SSL 3.0 には Padding Oracle On Downgraded Legacy Encryption（POODLE）攻撃と呼ばれる脆弱性があることに注意してください。これは SSL 3.0 を使用するサーバーに接続するいずれのアプリにも影響がある man-in-the-middle 攻撃です。POODLE 攻撃によってもたらされる脆弱性に対処するために、Secure Mail はデフォルトで SSL 3.0 接続を無効にし、サーバーへの接続には TLS 1.0 を使用します。これにより、Secure Mail は SSL 3.0 を使用する Notes Traveler Server には接続できません。推奨される回避策については、「Exchange Server または IBM Notes Traveler Server の統合」の「SSL/TLS のセキュリティレベルの構成」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。

以下の図は、サンプルの展開環境における IBM Notes Traveler サーバーと IBM Domino メールサーバーのネットワーク配置を示しています。

システム要件

インフラストラクチャサーバーの要件

- IBM Domino Mail Server 9.0.1
- IBM Notes Traveler 9.0.1

認証プロトコル

- Domino データベース

- Lotus Notes 認証プロトコル
- Lightweight Directory 認証プロトコル

ポート要件

- Exchange：デフォルトの SSL ポートは 443 です。
- IBM Notes：SSL はポート 443 でサポートされます。デフォルトで、非 SSL はポート 80 でサポートされます。

SSL/TLS のセキュリティレベルの構成

前の「重要」の注に記載のとおり、POODLE 攻撃によりもたらされる脆弱性に対処するため、Secure Mail に対して修正が加えられました。したがって、Notes Traveler サーバーで SSL 3.0 を使用している場合は、接続を有効にするために推奨される回避策は、IBM Notes Traveler 9.0 のサーバーで 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ツーサーバー通信における SSL 3.0 の使用を防ぐパッチを用意しています。2014 年 11 月にリリースされたパッチには、以下の Notes Traveler サーバーのバージョンに対する臨時の修正更新プログラムが含まれています：9.0.1 IF7、9.0.0.1 IF8、および 8.5.3 Upgrade Pack 2 IF8（および以降のすべてのリリースに含まれます）。パッチについて詳しくは、「LO82423: DISABLE SSLV3 FOR TRAVELER SERVER TO SERVER COMMUNICATION」を参照してください。

代替の回避策として、Secure Mail を Endpoint Management に追加するときに接続のセキュリティレベルポリシーを［**SSLv3 and TLS**］に変更します。この問題についての最新の情報は、「SSLv3 Connections Disabled by Default on Secure Mail 10.0.3」を参照してください。

以下の表に、Secure Mail でサポートされるプロトコルを、接続のセキュリティレベルポリシーの値に基づいてオペレーティングシステム別に示します。メールサーバーでプロトコルをネゴシエートできる必要もあります。

以下の表に、接続セキュリティレベルが SSLv3 および TLS の場合に Secure Mail でサポートされるプロトコルを示します。

オペレーティングシステムの種類	SSLv3	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
Android O	いいえ	はい

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

オペレーティングシステムの種類	SSLv3	TLS
iOS 9 以降	いいえ	はい
Android M より前	いいえ	はい
Android M および Android N	いいえ	はい
Android O	いいえ	はい

Notes Traveler Server の構成

次の情報は、IBM Domino Administrator 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、［Fewer name variations with higher security］に設定されています。この設定は、［UID］を LDAP 認証プロトコルの［AD User ID］にマップするために使われます。
- **NOTES.INI** 設定： **NTS_AS_ENFORCE_POLICY**=**false** を追加します。これにより、Secure Mail ポリシーを Traveler ではなく Endpoint Management で管理できます。この設定は、現在の展開と競合を引き起こす可能性がありますが、Endpoint Management 展開でのデバイスの管理が簡略化されます。
- 同期プロトコル： 現時点で、IBM Notes およびモバイルデバイスの同期に関して、SyncML は Secure Mail のサポート対象外です。Secure Mail では、Traverler サーバーに組み込まれた Microsoft ActiveSync プロトコルによりメール、カレンダー、および連絡先の情報が同期されます。SyncML がプライマリプロトコルとして強制される場合、Secure Mail を Traveler インフラストラクチャを介して接続し直すことはできません。
- **Domino** ディレクトリ構成 **- Web** インターネットサイト： /traveler に対するセッション認証をオーバーライドして、フォームベースの認証を無効にします。

Secure Mail の **S/MIME**

March 11, 2019

Secure Mail は Secure/Multipurpose Internet Mail Extensions（S/MIME）をサポートしています。これにより、ユーザーはメッセージに署名し、これを暗号化して、セキュリティを高めることができます。署名は、メッセージがいかがわしい発信元からきたものではなく、出所がはっきりした相手から送信されたものであることを受信者に保証します。暗号化は、互換性がある証明書を持つ受信者のみにメッセージを開くことを許可します。

S/MIME について詳しくは、Microsoft TechNet を参照してください。

次の表では、デバイスのオペレーティングシステム上の Secure Mail により S/MIME 機能がサポートされていることを示しています。

S/MIME の機能	iOS	Android
デジタル **ID** プロバイダー統合: Secure Mail とサポートされているサードパーティのデジタル ID プロバイダーを統合できます。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対する証明書を提供します。このアプリは、機密アプリデータ用のセキュアなストレージ領域である Endpoint Management の共有コンテナに証明書を送信します。Secure Mail はこの共有コンテナから証明書を入手します。詳しくは、「デジタル ID プロバイダーとの統合」を参照してください。	☒	
派生資格情報のサポート	Secure Mail では、証明書のソースとして派生資格情報を使用できます。派生資格情報について詳しくは、「iOS の派生資格情報」を参照してください。	
メールによる証明書の配布: メールにより証明書を配布するには、証明書テンプレートを作成してからそれを使ってユーザー証明書を求める必要があります。証明書をインストールし、検証した後で、ユーザー証明書をエクスポートしてから、ユーザーにメールで送信します。ユーザーはこのメールを Secure Mail で開き、証明書をインポートします。詳しくは、「メールによる証明書の配布」を参照してください。	☒	☒

S/MIME の機能	iOS	Android
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を目的とするものであることを検出すると、その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。証明書が両方を対象にしたものである場合は、インポートを求めるプロンプトがユーザーに表示されます。	☒	

デジタル **ID** プロバイダーとの統合

次の図は、証明書がデジタル ID プロバイダーホストから Secure Mail に到達するまでのパスを示しています。これは、Secure Mail とサポートされているサードパーティのデジタル ID プロバイダーを統合する場合に発生します。

MDX の共有コンテナは、証明書など機密アプリデータ用のセキュアなストレージ領域です。Endpoint Management で有効なアプリのみが共有コンテナにアクセスできます。

前提条件

Secure Mail では、Entrust IdentityGuard との統合がサポートされています。

統合の構成

1. ID プロバイダーアプリを準備してユーザーに提供します：
    - ラップする.ipa を取得するには、Entrust に問い合わせてください。
    - MDX Toolkit を使ってアプリをラップします。

      Endpoint Management 環境以外でこのアプリのバージョンを所有するユーザーにこのアプリを展開する場合は、このアプリに対して一意の ID を使用してください。このアプリと Secure Mail に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、それを Endpoint Management アプリストアに公開します。
    - 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ユーザーに通知します。必要に応じて、インストール後の作用に関するガイダンスを提供します。

次の手順で Secure Mail に対して S/MIME ポリシーをどのように構成するかによっては、Secure Mail によりユーザーにプロンプトが表示されて証明書のインストールを求めたり、ユーザーが Secure Mail 設定で S/MIME を有効にしたりすることがあります。これらの手順については、「Secure Mail for iOS での S/MIME の有効化」を参照してください。

2. Secure Mail を Endpoint Management に追加する場合、次のポリシーを構成する必要があります:
   - S/MIME 証明書のソースポリシーを ［共有コンテナ］ に設定します。この設定により Secure Mail は、デジタル ID プロバイダーにより共有コンテナに保存された証明書を使用します。
   - Secure Mail の初期スタートアップの間に 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。ポリシーにより、共有コンテナに証明書がある場合に Secure Mail が S/MIME を有効にしたかどうかが判別されます。使用できる証明書がない場合は、Secure Mail によりプロンプトが表示されユーザーに証明書のインポートを求めます。このポリシーが有効でない場合は、Secure Mail 設定で S/MIME を有効にできます。デフォルトでは Secure Mail で S/MIME が有効でないため、ユーザーが Secure Mail 設定を介して 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、派生資格情報を使用できるようにすることができます。

Secure Mail を Endpoint Management に追加する場合、S/MIME 証明書のソースポリシーを ［派生資格情報］ に設定します。派生資格情報について詳しくは、「iOS の派生資格情報」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する、または派生資格情報を使用する代わりに、ユーザーにメールで証明書を配布することもできます。このオプションを実行する場合は、このセクションで詳しく説明されている次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って Microsoft Certificate Services の Web 登録を有効にして、IIS で認証設定を確認します。
2. メールメッセージに署名して暗号化するための証明書テンプレートを作成します。ユーザー証明書を要求するには、これらのテンプレートを使用します。
3. 証明書をインストールして検証し、その後で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. ユーザーはこのメールを Secure Mail で開き、証明書をインポートします。したがって、この証明書は Secure Mail でのみ使用できます。これらは S/MIME の iOS プロファイルには表示されません。

前提条件

このセクションで示す手順は、次のコンポーネントを基にしています。

- XenMobile Server 10 以降
- サポートされているバージョンの Citrix Gateway（旧称 NetScaler Gateway）
- Secure Mail for iOS（10.8.10 以降）、Secure Mail for Android（10.8.10 以降）
- Microsoft Windows Server 2008 R2 以降（ルート証明機関（CA）として動作する Microsoft Certificate Services 付属）
- Microsoft Exchange:
  - Exchange Server 2016 の累積更新プログラム 4
  - Exchange Server 2013 の累積更新プログラム 15
  - Exchange Server 2010 Service Pack 3 の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:

- 手動で、または Endpoint Management の資格情報デバイスポリシーを通して、ルート証明書および中間証明書をモバイルデバイスに配信します。詳しくは、「資格情報デバイスポリシー」を参照してください。
- プライベートサーバー証明書を使用して Exchange Server への ActiveSync トラフィックを保護している場合は、ルート証明書および中間証明書をすべて、モバイルデバイスにインストールします。

Microsoft Certificate Services の **Web** 登録の有効化

1. ［管理ツール］ に移動し、［サーバーマネージャー］ をクリックします。
2. ［**Active Directory** 証明書サービス］ 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. 必要な場合は、［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］ を選択して ［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 での認証設定の確認

- ユーザー証明書の要求に使用される 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 登録サイトには HTTPS を介して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］ をクリックします。
2. **Web** サーバー（**IIS**）で、［役割サービス］ を確認します。クライアント証明書マッピング認証および 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か確認します。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 登録用に 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の認証] 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** インターネットインフォメーションサービスの既定のサイト] **>** [バインド] の順にクリックします。
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の承認] をクリックします。

新規証明書テンプレートの作成

メールメッセージに署名して暗号化するには、Microsoft Active Directory Certificate Services で証明書を作成することをお勧めします。1 つの証明書を両方の目的で使用し、暗号化証明書をアーカイブする場合は、署名証明書が復元され、偽装される可能性があります。

証明機関（CA）サーバーで証明書テンプレートを複製するには、次の手順に従います。

- Exchange Signature Only（著名用）
- Exchange User（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 Signature Only テンプレートを検索し、この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。
5. 名前を付けます。
6. [**Active Directory** の証明書を発行する] チェックボックスをオンにします。

   > 注:
   >
   > [**Active Directory** の証明書を発行する] チェックボックスをオンにしなかった場合、ユーザーはユーザー証明書（署名と暗号化用）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] **>** [メールセキュリティ] **>** [**GAL**（**Global Address List**）に公開] の順に選択して実行できます。

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
   - キーの最小サイズ： 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
   - [ユーザー入力の強制なしでサブジェクトを登録する] チェックボックス： オン

8. ［セキュリティ］ タブをクリックし、［グループまたはユーザー名］ に、認証ユーザー（または必要な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。さらに、［認証ユーザーの権限］ で、［読み取り登録］ チェックボックスで ［許可］ が選択されていることを確認します。
9. そのほかのタブや設定はすべてデフォルトのまま残します。
10. ［証明書テンプレート］ で、［**Exchange User**］ をクリックし、手順 4 ～ 9 を繰り返します。

    新しい Exchange User テンプレートでは、オリジナルのテンプレートのデフォルト設定をそのまま使用します。
11. ［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： 暗号化
    - キーの最小サイズ： 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
    - ［ユーザー入力の強制なしでサブジェクトを登録する］チェックボックス： オン
12. テンプレートが両方とも作成されたら、必ず、両方の証明書テンプレートを発行してください。［新規作成］ を選択し、［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（例: `https://ad.domain.com/certsrv/`）に移動します。この手順では、メールを保護するために、署名用と暗号化用に 2 種類のユーザー証明書を要求します。Secure Mail を介して S/MIME の使用を必要とするその他のドメインユーザーについても同じ手順を使うことができます。

署名と暗号化に使用するユーザー証明書を生成するには、Microsoft 証明書サービスの Web 登録サイト（例: `https://ad.domain.com/certsrv/`）から手動登録します。または、この機能を使用するユーザーのグループのグループポリシーを通じて自動登録を構成します。

1. Windows ベースのコンピューターでは、Internet Explorer を開き、Web 登録サイトに移動して、新しいユーザー証明書を要求します。

   > 注:
   >
   > 証明書を要求するには、必ず正しいドメインユーザーでログオンしてください。
2. ログオン後に、［証明書の要求］ をクリックします。
3. ［証明書の要求の詳細設定］ をクリックします。
4. ［この **CA** への要求を作成し送信する］ をクリックします。
5. 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てから、［要求の形式］ の隣にある ［**PKCS10**］ を選択します。

   これで要求は送信されました。

6. ［この証明書のインストール］をクリックします。
7. 証明書が正常にインストールされたことを確認します。
8. 同じ手順を繰り返しますが、今度はメールメッセージの暗号化用の証明書を生成します。Web 登録サイトにログオンしたのと同じユーザーとして、［ホーム］リンクに移動し、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。
10. 証明書が正常にインストールされたことを確認してから、同じ手順を繰り返して、もう 1 人のドメインユーザー用にユーザー証明書ペアを生成します。この例では、同じ手順に従って、”User2” のために 2 通の証明書を生成します。

> 注:
>
> この手順では、同じ Windows ベースのコンピューターを使って、「User2」のために 2 組目の証明書を要求します。

公開された証明書の検証

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た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］**>**［高度な機能］ の順に選択します。
2. ユーザー（この例では User1）のプロパティに進み、［公開された証明書］ タブをクリックします。証明書が両方とも使用可能であることを確認します。それぞれの証明書が特定の用途を持っていることも検証できます。

   この図は、証明書がメールメッセージの暗号化用であることを示しています。

   この図は、証明書がメールメッセージの署名用であることを示しています。

   ユーザーに正しい暗号化証明書が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］**>**［ユーザープロパティ］ で検証できます。

   Secure Mail は動作の際、LDAP クエリ経由で userCertificate ユーザーオブジェクトの属性を確認します。この値は ［属性エディタ］ タブに表示されます。このフィールドが空か、または間違った暗号化用ユーザー証明書が表示されている場合、Secure Mail はメッセージを暗号化（または復号化）できません。

ユーザー証明書のエクスポート

この手順では、”User1” および”User2” 両方の証明書ペアを.PFX（PKCS#12）形式で秘密キーとともにエクスポートします。エクスポートした証明書は、Outlook Web Access（OWA）を使用して、ユーザーにメールで送信されます。

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」の両方の証明書ペアが表示されます。
2. 証明書を右クリックし、［すべてのタスク］**>**［エクスポート］ の順にクリックします。

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. ［証明のパスにある証明書を可能であればすべて含む］ 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。
5. 1 つ目の証明書をエクスポートしたら、残りの証明書についても同じ手順を繰り返します。

> 注:
>
> どちらの証明書が署名証明書で、どちらが暗号化証明書であるかを名前からはっきり区別できるようにします。この例では、証明書に”userX-sign.pfx” と”userX-enc.pfx” という名前を付けています。

メールを使った証明書の送信

すべての証明書を PFX 形式でエクスポートしたら、次は、Outlook Web Access（OWA）を使ってメールで送信します。この例で使用するログオン名は User1 で、送信するメールには両方の証明書が含まれています。

User2 をはじめとして、同じドメインにいる他のユーザーすべてに同じ手順を繰り返します。

Secure Mail for iOS および **Android** での **S/MIME** の有効化

メールの送信が完了したら、次に、Secure Mail を使ってメッセージを開き、署名と暗号化に適した証明書を使って S/MIME を有効化します。

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. Secure Mail を起動して、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、ダウンロードしてインポートします。
3. サーバーから署名証明書をエクスポートしたときに秘密キーに割り当てられたパスワードを入力します。

   証明書がインポートされました。
4. ［署名を有効にする］ をタップ
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有効にします。
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。
7. メールに戻って、暗号化証明書をタップし、ダウンロードしてインポートします。
8. サーバーから暗号化証明書をエクスポートしたときに秘密キーに割り当てられたパスワードを入力します。

   証明書がインポートされました。
9. ［暗号化を有効にする］ をタップ
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］を有効にします。

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。

> 注:
>
> a) メールが S/MIME でデジタル署名され、ファイルが添付されていて、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 の制限事項です。効率的に S/MIME メッセージを受信するには、Secure Mail 設定で S/MIME をオンにします。
>
> b) ［デフォルトで暗号化］ オプションを使用すると、メールの暗号化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、メールは作成中に暗号化された状態になります。
> この機能がオフの場合、メールは作成中に暗号化されていない状態になるため、［ロック］ アイコンをタップして暗号化する必要があります。

1 つ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. Secure Mail を起動して、S/MIME 証明書を含むメールに移動します。
2. S/SMIME 証明書をタップして、ダウンロードしてインポートします。
3. サーバーから証明書をエクスポートしたときに秘密キーに割り当てられたパスワードを入力します。
4. 表示された証明書オプションから、適切なオプションをタップして、署名証明書または暗号化証明書をインポートします。
   ［証明書を開く］ をタップすると、証明書の詳細が表示されます。

   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**］ に移動すると表示できます。

iOS および **Android** での **S/MIME** のテスト

上記の手順を実行すると、受信者は署名され暗号化されたメールを読むことができます。

次の図は、受信者に読まれる暗号化されたメッセージを示しています。

次の図は、信頼されている署名済み証明書の検証例です。

Secure Mail は Active Directory ドメインで受信者の公開暗号証明書を検索します。ユーザーが、有効な公開暗号化キーを持っていない受信者に暗号化したメッセージを送信した場合は、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で、1 人の受信者が有効なキーを持っていない場合は、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。

パブリック証明書のソースの構成

S/MIME パブリック証明書を使用するには、S/MIME パブリック証明書ソース、LDAP サーバーアドレス、LDAP ベース DN、および［LDAP に匿名でアクセスする］ポリシーを構成します。

アプリのポリシーのほかに、以下を実行します。

- LDAP サーバーがパブリックの場合、トラフィックが直接 LDAP サーバーに向かっていることを確認してください。これを行うには、Secure Mail のネットワークポリシーを ［内部ネットワークへトンネル］ に設定し、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にある場合、以下を実行します。
  - iOS の場合は、バックグラウンドネットワーク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。このポリシーを構成すると、ユーザーが頻繁に認証を求められるようになります。
  - Android の場合は、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一覧に **LDAP** サーバー **URL** を追加してください。

Secure Mail の SSO

April 18, 2019

ユーザーを Secure Hub に登録すると Secure Mail にも自動的に登録されるように Endpoint Management を構成できます。これは、ユーザーが追加情報を入力する必要がないか、Secure Mail に登録する追加手順を実行する必要がないことを意味します。メールの資格情報で Secure Hub に登録するユーザーは、この機能のために Autodiscovery を有効にする必要があります。Autodiscovery が有効になっていない場合、次の登録方法でこの機能を有効にできます。

- Endpoint Management アドレスを Secure Hub から Secure Mail に渡す。
- Secure Hub への登録時に Endpoint Management アドレスを入力する。

Secure Mail で自動登録を有効にするには

1. Endpoint Management クライアントのプロパティの ［設定］ ページで、以下を実行します:

   a. 次の値を **true** に設定します:

   - ENABLE_PASSCODE_AUTH
   - ENABLE_PASSWORD_CACHING
   - ENABLE_CREDENTIAL_STORE

   b. 次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

3. Secure Mail プロパティを構成します。
    - ［最初の認証メカニズム］をユーザーのメールアドレスに設定します。
    - ［最初の認証資格情報］を **userPrincipalName** に設定します。
4. ユーザーの Exchange Server メールボックスのメールに基づいて Autodiscovery サービスを構成します。サポートについては、Microsoft Exchange 管理者に連絡してください。ここでは、DNS に SRV レコードを照会して Autodiscovery サービス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 アプリの設定を構成します：

1. ［最初の認証メカニズム］でユーザーのメールアドレスをクリックします。
2. ［最初の認証資格情報］で **userPrincipalName** または **sAMAccountName** をクリックします。ユーザーの Exchange メールサーバーに対して構成された認証の種類に基づいて選択します。
3. Secure Mail Exchange Server と Secure Mail ユーザードメインフィールドは空のままにします。
4. 必要に応じて Secure Mail アプリの他のポリシーを構成し、必要なデリバリーグループを割り当てます。

自動プロビジョニングを使用した **Secure Mail** の **SSO** のユーザー操作手順

次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 ストア（Android）から Secure Hub をインストールします。
2. Secure Hub を起動して、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 ストア（Android）から Secure Mail をインストールします。
4. Secure Mail を開いて ［**OK**］ をタップします。この手順によって、Secure Hub は Secure Mail を管理できるようになります。Secure Mail を起動すると、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 サービスから取得されます。DNS の SRV レコード照会は、Secure Hub から取得し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 から取得します。

アカウントが構成されると、ユーザーは、デバイスの ［**Secure Mail**］ > ［設定］ > ［アカウント］ で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、次の手順を実行してください。

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 サービス用に構成され、ユーザー登録がメールアドレスを使用するように構成されていることを確認します。
3. Exchange Server ドメインが Autodiscovery で構成されていることを確認します。SRV レコードの照会が ActiveSync メールクライアントに関して予想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、以下の情報を収集し、シトリックス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。
    - ログレベルが最も高い Secure Mail 診断ログを収集します。
    - Autodiscovery サービスをホストしている Exchange Server の C:\inetpub\logs\LogFiles\W3SVC1 ディレクトリから IIS ログを収集します。Microsoft Autodiscovery サービスについては、Autodiscover service in Exchange Serverを参照してください。

セキュリティに関する注意事項

March 11, 2019

ここでは、Secure Mail のセキュリティに関する注意事項と、データセキュリティを強化するために有効にできる特定の設定について説明します。

Microsoft IRM および **AIP** によるメール情報保護のサポート

Secure Mail for Android と Secure Mail for iOS では、構成済みの IRM ポリシーに合わせて、Microsoft IRM（Information Rights Management）および AIP（Azure Information Protection）ソリューションで保護されたメッセージがサポートされています。このサポートには、Citrix Endpoint Management で構成された IRM ポリシーが適用されます。

この機能により、IRM を使用している組織は、送信するメッセージのコンテンツに対して保護を適用できます。また、この機能を使用すると、モバイルデバイスのユーザーは、権利が保護されたコンテンツを作成および利用できます。デフォルトでは、IRM のサポートは ［オフ］ になっています。これを有効にするには、Information Rights Management ポリシーを ［オン］ に設定します。

Secure Mail で **Information Rights Management** を有効化するには

1. Endpoint Management にログオンして ［構成］>［アプリ］ に移動し、［追加］ をクリックします。
2. ［アプリの追加］ 画面で、［**MDX**］ をクリックします。
3. ［アプリケーション情報］ 画面でアプリの詳細を入力し、［次へ］ 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、アップロードします。
5. ［アプリ設定］ 画面で［Information Rights Management］をオンにします。

> 注:
>
> iOS と Android の両方で Information Rights Management を有効にします。

権利が保護されたメールを受信したとき

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:

このユーザーが付与されている使用権の詳細を表示するには、［詳細］ をタップします。

権利が保護されたメールを作成するとき

ユーザーがメールを作成するときに、制限プロファイルを設定してメールを保護することができます。

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。
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、戻るアイコンをクリックします。

   適用された制限は、「件名」フィールドの下に表示されます。

組織によっては、IRM ポリシーを厳しく順守することが必要な場合があります。Secure Mail へのアクセス権を持つユーザーが、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することで、IRM ポリシーを回避しようとするかもしれません。

Endpoint Management はこのような攻撃の一部を検出できますが、次のような予防措置を検討することでより高いセキュリティを提供できます:

- 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する。
- Endpoint Management の機能やその他の機能を使って、デバイスを適切に構成する。
- Secure Mail などの IRM 機能を適切に使用するように、ユーザーにガイダンスを提供する。
- このような攻撃に備えて、サードパーティのセキュリティソフトウェアを追加で展開する。

メールセキュリティの分類

Secure Mail for iOS および Secure Mail for Android ではメール分類マーキングがサポートされており、ユーザーはメールの送信時に SEC（security）および DLM（dissemination limiting markers）を指定できます。SEC マーキングには Protected、Confidential、Secret などがあります。DLM には Sensitive、Legal、Personal などがあります。メールを作成する時に、Secure Mail のユーザーは次の図で示すようにマーキングを選択してメールの分類レベルを指定することができます。

受信者はメールの件名でその分類マーキングを確認できます。次に例を示します：

- 件名：計画 [SEC = PROTECTED、DLM = Sensitive]
- 件名：計画 [DLM = Sensitive]
- 件名：計画 [SEC = UNCLASSIFIED]

メールヘッダーに、この例において太文字で表示されているインターネットメッセージヘッダー拡張としての分類マーキングが含まれています。

日付：2015 年 5 月 1 日（金）12:34:50 +530

件名：計画 [SEC = PROTECTED、DLM = Sensitive]

優先度：標準

X 優先度：標準 **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 は分類マーキングを表示するだけです。マーキングに基づいて何かしらの操作が行われることはありません。

分類マーキングが付いたメールに返信またはそれを転送する場合、デフォルトでは SEC および DLM 値は元のメールのままとなります。ユーザーは別のマーキングを選択することができます。Secure Mail は元のメールと比較してこれらの変更を検証しません。

メール分類マーキングは、次の MDX ポリシーを介して構成します。

- 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”X-Protective-Marking” 値としてメールヘッダーに表示されます。関連するメール分類ポリシーを構成する必要があります。デフォルト値は ［オフ］ です。
- メール分類の名前空間： 使用される分類の標準によりメールヘッダー内で必要とされる分類名前空間を指定します。たとえば、名前空間”gov.au” はヘッダーには”NS=gov.au” と表示されます。デフォルト値は空です。

- メール分類のバージョン: 使用される分類の標準によりメールヘッダー内で必要と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” はヘッダーには”VS=2012.3” と表示されます。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、［メール分類のマーキング］ポリシーの一覧にある必要があります。デフォルトの値は ［**UNOFFICIAL**］ です。
- メール分類のマーキング: 分類マーキングを指定してユーザーが使用できるようにします。一覧が空の場合、Secure Mail は保護マーキングの一覧を含めません。マーキングの一覧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 のメールの件名とヘッダーに付随された文字列であるマーキング値が含まれます。たとえば、マーキングペアの「UNOFFICIAL,SEC=UNOFFICIAL」の場合、リスト値は「UNOFFICIAL」、マーキング値は「SEC=UNOFFICIAL」となります。

デフォルト値は変更できる分類マーキングの一覧です。次のマーキングが Secure Mail により提供されます。

- UNOFFICIAL,SEC=UNOFFICIAL
- UNCLASSIFIED,SEC=UNCLASSIFIED
- For Official Use Only,DLM=For-Official-Use-Only
- Sensitive,DLM=Sensitive
- Sensitive:Legal,DLM=Sensitive:Legal
- Sensitive:Personal,DLM=Sensitive:Personal
- PROTECTED,SEC=PROTECTED
- PROTECTED+Sensitive,SEC=PROTECTED
- PROTECTED+Sensitive:Legal,SEC=PROTECTED DLM=Sensitive:Legal
- PROTECTED+Sensitive:Personal,SEC=PROTECTED DLM=Sensitive:Personal
- PROTECTED+Sensitive:Cabinet,SEC=PROTECTED,DLM=Sensitive:Cabinet
- CONFIDENTIAL,SEC=CONFIDENTIAL
- CONFIDENTIAL+Sensitive,SEC=CONFIDENTIAL,DLM=Sensitive
- CONFIDENTIAL+Sensitive:Legal,SEC=CONFIDENTIAL DLM=Sensitive:Legal
- CONFIDENTIAL+Sensitive:Personal,SEC=CONFIDENTIAL,DLM=Sensitive:Personal
- CONFIDENTIAL+Sensitive:Cabinet,SEC=CONFIDENTIAL DLM=Sensitive:Cabinet
- SECRET,SEC=SECRET
- SECRET+Sensitive,SEC=SECRET,DLM=Sensitive
- SECRET+Sensitive:Legal,SEC=SECRET,DLM=Sensitive:Legal
- SECRET+Sensitive:Personal,SEC=SECRET,DLM=Sensitive:Personal
- SECRET+Sensitive:Cabinet,SEC=SECRET,DLM=Sensitive:Cabinet
- TOP-SECRET,SEC=TOP-SECRET
- TOP-SECRET+Sensitive,SEC=TOP-SECRET,DLM=Sensitive
- TOP-SECRET+Sensitive:Legal,SEC=TOP-SECRETDLM=Sensitive:Legal
- TOP-SECRET+Sensitive:Personal,SEC=TOP-SECRETDLM=Sensitive:Personal

- TOP-SECRET+Sensitive:Cabinet,SEC=TOP-SECRETDLM=Sensitive:Cabinet

iOS データ保護

ASD（Australian Signals Directorate：オーストラリア通信電子局）のデータ保護要件を満たす必要がある企業では、Secure Mail および Secure Web の ［**iOS** データ保護を有効化］ ポリシーを使用できます。デフォルトでは、このポリシーは ［オフ］ になっています。

Secure Web の ［**iOS** データ保護を有効化］ ポリシーが ［オン］ のとき、Secure Web ではサンドボックス内のすべてのファイルに対してクラス A の保護レベルが適用されます。Secure Mail のデータ保護について詳しくは、「オーストラリア通信電子局のデータ保護」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ので、**Minimum data protection class** ポリシーも指定する必要はありません。

Enable iOS data protection 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 に読み込みます：新しいアプリの場合、［構成］ **>** ［アプリ］ **>** ［追加］ の順に選択して ［**MDX**］ をクリックします。アップグレードについては、「MDX またはエンタープライズアプリケーションのアップグレード」を参照してください。
2. Secure Mail の場合、［アプリ］ 設定に移動して ［**iOS** データ保護を有効化］ ポリシーを見つけ、［オン］ に設定します。古いバージョンのオペレーティングシステムが動作するデバイスは、このポリシーを有効にしても影響を受けません。
3. Secure Web の場合、［アプリ］ 設定に移動して ［**iOS** データ保護を有効化ポリシー］ を見つけ、［オン］ に設定します。古いバージョンのオペレーティングシステムが動作するデバイスは、このポリシーを有効にしても影響を受けません。
4. 通常通りアプリのポリシーを構成して設定を保存し、Endpoint Management アプリストアにアプリを展開します。

オーストラリア通信電子局のデータ保護

Secure Mail では ASD（Australian Signals Directorate：オーストラリア通信電子局）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を対象に、ASD のデータ保護をサポートします。デフォルトでは、［iOS データ保護を有効化］ポリシーは ［オフ］ に設定されており、Secure Mail ではクラス C のデータ保護が提供される、つまりプロビジョニングプロファイルに設定されているデータ保護が使用されます。

ポリシーが ［オン］ の場合、アプリのサンドボックスでファイルを作成し開くときに Secure Mail によって保護レベルが指定されます。Secure Mail は以下のアイテムにクラス A の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

- ほかのアプリから貼り付けられた画像
- ダウンロードした添付ファイル

Secure Mail は以下のアイテムにクラス B の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
- アドレス帳
- ActiveSync ポリシーファイル

クラス B の保護により、ロックされたデバイスでの同期が可能になります。また、ダウンロードを開始してからデバイスをロックした場合は、ダウンロードの完了が可能になります。

データ保護が有効な場合、デバイスのロック中はファイルが開けないため、キューにある送信トレイアイテムは送信されません。デバイスのロック中に Secure Mail が終了されその後再起動された場合、デバイスのロックを解除して Secure Mail を起動するまで、Secure Mail で同期することができません。

このポリシーを有効にする場合は、クラス C のデータ保護を適用してログファイルを作成しないように、必要な時にのみ Secure Mail ログを有効にすることをお勧めします。

Android の機能

May 17, 2019

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。

フィードの管理

Secure Mail for Android では、フィードカードを必要に応じて整理できます。

フィード機能の強化には、以下のオプションが含まれています:

- 最大 3 つのメールフォルダーを追加できます。
- 同僚や直属の部下のカードを追加したり、VIP やフラグ付きなどのフォルダーを追加したりできます。
- カードまたはフォルダーを検索できます。
- 既存のカードを並べ替えることができます。
- 既存のカードを削除することができます。

［フィード］ ビューで ［フィードの管理］ ボタンをタップして、カードを管理できます。

または、設定画面の ［メール］ で ［フィードの管理］ オプションをタップして、カードを管理することもできます。

必要に応じて、カードを追加したり、並べ替えたり、削除したりできます。

カードを追加する

1. ［すべてのカード］ タブまたは ［すべてのフォルダー］ タブをタップします。
2. 画面右上の追加アイコン（+）をタップして、対象のカードを選択します。
3. ［完了］ をタップします。

選択したカードが追加され、フィードに表示されます。

カードを並べ替える

1. ［フィードの管理］ ボタンをタップします。
2. 利用可能なカードから選択するカードをタップして、長押しします。
3. カードを目的の場所に移動します。

カードを削除する

1. ［フィードの管理］ ボタンをタップします。
2. カードの横にある ［-］ アイコンをタップします。
3. ［完了］ をタップします。

カードがフィードから削除されます。

添付ファイルの表示

Secure Mail for Android では、メールおよびカレンダーに添付されたファイルを簡単に表示できます。添付ファイルがアプリ内で直接開くか、サポートされているアプリの一覧が表示されます。添付ファイルを表示するために必要なアプリを選択できます。

Secure Mail での表示がサポートされているのは、.txt、Word、オーディオ、ビデオ、html、.zip ファイル、画像、.eml ファイル、.vcf 形式の連絡先ファイルです。

前提条件

Citrix Endpoint Management コンソールで管理者が、以下の MDX ポリシーを構成するようにしてください:

- ［ドキュメント交換（このアプリケーションで開く）］ポリシーを ［制限なし］ に設定します。
- ［オフラインドキュメントを許可］ポリシーを ［無制限］ に設定します。

これらの MDX ポリシーについて詳しくは、MDX Toolkit ドキュメントの「アプリ相互作用」を参照してください。

添付ファイル表示中の操作

添付ファイルの表示中、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添付ファイルとして選択する。
- ファイルを添付する新しいメッセージを作成する。
- オフラインでのアクセス用に添付ファイルを保存する。
- オフラインファイルから添付ファイルを削除する。
- 画面の指示に従って、別のアプリケーションを使用して添付ファイルを開く。
- 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。

次の操作を実行中、添付ファイルのプレビュー表示ができます:

- メッセージを表示する。
- 新しいメッセージを作成する。
- メッセージを転送する。

次の場所から添付ファイルをプレビュー表示することもできます:

- [添付ファイル] フォルダー。
- カレンダーイベント。

既存のメールまたは新しいメールにファイルを添付する

既存のメールにファイルを添付するか、またはメールを作成してファイルを添付することができます。

1. [添付ファイル] フォルダーをタップし、長押しで複数の添付ファイルを選択するか、タップで 1 つの添付ファイルを選択します。
2. 画面上の [添付] アイコンをタップします。メールボックスが表示されます。
3. 次のいずれかを実行します:
    - 既存のメールにファイルを添付するには、既存のメッセージを選択します。
    - 新しいメールにファイルを添付するには、[新しいメッセージ] をタップします。

添付ファイルをオフラインアクセス用に保存するには

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] をタップします。

別のアプリ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、［プログラムから開く］ をタップします。
3. 表示されるオプションで、添付ファイルを開くアプリをタップします。
4. または、左にスワイプして、添付ファイル操作の一覧を表示することもできます。

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するには

1. 画面右下の ［添付ファイル］ アイコンをタップします。
2. 添付ファイルをタップしてから、画面の右上にある ［その他］ アイコンをタップします。
3. ［元のメールを表示］ または ［元のカレンダーを表示］ をタップして、メールまたはカレンダーイベントの場所を表示します。

メールおよび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のイベントを印刷できます。この印刷機能は Android 印刷フレームワークを使用します。

前提条件

- Citrix Endpoint Management コンソールで管理者が印刷を禁止ポリシーを ［オフ］ に設定するようにしてください。Android のこのポリシーについて詳しくは、「印刷を禁止ポリシー」を参照してください。
- メールが IRM で保護されている場合、メールの ［閲覧者に印刷を許可する］ オプションを有効にしてください。

これらのポリシーが適切に設定されていない場合、メールまたはカレンダーイベントを印刷できません。

> 注:
>
> この印刷機能には、次の既知の制限があります:
>
> - インラインイメージは、［画像を表示する］ 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。［画像を表示する］ をタップしないと、画像のプレースホルダーだけが印刷されます。
> - Secure Mail では、サイズの大きいメールが省略表示されるため、印刷前に、［メッセージ全体のダウンロード］ をタップしてメール全体を印刷します。メッセージ全体をダウンロードしない場合、省略表示されたメールが印刷されます。
> - これらのアイテムの印刷時に、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. 印刷するメールを開きます。
2. 画面の左上にある［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:
>
> タブレットでメールを印刷する場合、画面の左上にある印刷アイコンを直接使用できます。

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. 一覧をタップすると、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
3. ［**PDF** として保存］ をタップしてメールを PDF 形式で保存します。
4. ［すべてのプリンター］ をタップします。要件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、［プリンターの選択］ をタップしてプリンターを選択します。［プリンター］ 画面が開きます。

    > 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。以下は Canon E480 プリンターの画像であり、一例にすぎません。

6. 印刷するプリンタを選択します。次の印刷オプションを使用します:
    - 印刷する部数を手動で入力します。
    - 一覧から用紙サイズを選択します。
    - 一覧から色を選択します。
    - 必要に応じて印刷の向きを選択します。
    - 1 ページまたは複数のページを印刷するには、ページの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、画面の［印刷］アイコンをタップします。

インラインイメージを印刷するには

- メールで ［画像を表示する］ をタップし、上記の「メールを印刷するには」に記載されている手順に従ってください。

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、上記の「メールを印刷するには」に記載されている内容と同じ手順に従ってください。

ActiveSync ヘッダーでフィッシングメールを報告

Secure Mail for Android では、ユーザーがフィッシングメールについて報告すると、そのメールに関連した添付として EML ファイルが生成されます。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ている ActiveSync ヘッダーを表示できます。

この機能を有効にするには、管理者が 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設定し、フィッシング報告の方法を ［添付ファイルで報告］ に設定する必要があります。詳しくは、「添付ファイルでフィッシングメールを報告」を参照してください。

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信できます。

> 注:
>
> - 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、サブフォルダーの通知を取得します。FCM ベースのプッシュ通知の構成について詳しくは、「Secure Mail のプッシュ通知」を参照してください。
> - サブフォルダーの通知機能は、Lotus Notes サーバーでは使用できません。

サブフォルダーの通知を有効にするには

1. ［設定］ に移動して、 ［全般］ で ［通知］ をタップします。
2. ［通知］ 画面で［メールフォルダー］ をタップします。受信トレイにサブフォルダーの一覧が表示されます。
3. 通知を受信する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。

サブフォルダーの通知を無効にするには、通知を受信し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 以降が稼働するデバイスでは、通知チャネル設定を使用して、メールやカレンダーの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して管理できます。

メールまたはカレンダーの通知を設定するには、Secure Mail を起動して ［設定］**>**［通知］ に移動し、対象の通知オプションを選択します。

その後、［メール通知の管理］ または ［カレンダー通知の管理］ のいずれかに移動すると、メール通知またはカレンダー通知をそれぞれ管理できます。

または、デバイス上の Secure Mail アプリアイコンを長押しして［アプリ情報］を選択し、［通知］をタップします。

バイブレーション設定が事前にマナーモード時のみに設定されている場合、この機能によりデフォルトのバイブレーション設定（オフ）に変わります。

> 注:
>
> ロック画面上の通知は、管理者が設定したロック画面上の通知を制御 MDX ポリシーの内容に従って通知されます。

Android の添付ファイル

Secure Maill バージョン 10.3.5 以降では、受信ドキュメント交換（このアプリケーションで開く）ポリシーが ［制限］ に設定されている場合、ギャラリーアプリから直接画像を添付できません。このポリシー設定を ［制限］ のままにして、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場合は、Endpoint Management コンソールで次の手順に従います。

1. ［ギャラリーを禁止］ 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:
   - **LG Nexus 5**:
     com.google.android.gallery3d, com.google.android.apps.photos
   - **Samsung Galaxy Note 3**:
     com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.p
   - **Sony Expire**:
     com.sonyericsson.album, com.google.android.apps.photos
   - **HTC**:
     com.google.android.apps.photos, com.htc.album
   - **Huawei**:
     com.android.gallery3d, com.google.android.apps.photos
3. 非表示の InboundDocumentExchangeWhitelist ポリシーを表示に変更します。
   - WorxMail APK ファイルをダウンロードして、そのファイルを MDX Toolkit でラップします。
   - コンピューター上で.mdx ファイルを検索し、ファイルの拡張子を.zip に変更します。
   - ZIP ファイルを開いて、policy_metadata.xml ファイルを検索します。

- InboundDocumentExchangeWhitelist を検索して`PolicyHidden>**true**</PolicyHidden`>を<`PolicyHidden`>**`false`**</`PolicyHidden`>に変更します。
- policy_metadata.xml ファイルを保存します。
- そのフォルダー内のファイルをすべて選択して圧縮し、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。フォルダー内のファイルをすべて選択して、選択されているファイルを圧縮してください。

- 圧縮されたファイルをクリックします。
- ［情報を取得］ を選択してファイルの拡張子を.mdx に戻します。

4. 修正済みの.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 の一覧を、表示されるようになった受信ドキュメント交換のホワイトリストポリシーに追加します。

   パッケージ ID がコンマで区切られていることを確認します:

   com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photo
5. Secure Mail を保存して展開します。

これで 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す。

サポートされるファイル形式

次の表は、Secure Mail での添付および表示がサポートされるファイル形式の一覧です。

形式	iOS	Android
ビデオ: H.263 AMR NB codec_Mp4		X
ビデオ: H.263 AMR NB codec_3gp		X
ビデオ: H.264 AAC codec_3gp	X	X
ビデオ: H.264 AAC codec_mp4	X	X
ビデオ: H.264 Acclc codec_mp4	X	X
GTM recorded_wmv		X
AVI		X
WAV	X	X
MP4	X	X

形式	iOS	Android
3GP	X	X
Flac		X
AAC	X	X
M4A	X	X
3GP（AMR-NB）	X	X
MP3	X	X
WAV	X	X
OGG		X
ICO	X	X
JPEG	X	X
PNG	X	X
TIF（単一ページのみ）	X	
BMP	X	X
GIF	X	X
WebP		X
.dot	X	X
PDF	X	
PPT	X	X
PPTX	X	X
DOC	X	X
DOCX	X	X
XLS	X	X
XLSM	X	X
XLSX	X	X
TXT	X	X
POT	X	X
HTM	X	X
HTML	X	X
ZIP	X	X

形式	iOS	Android
EML	X	X

Android での複数の **Exchange** アカウント

Secure Mail 内の ［設定］ 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。

前提条件

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須です。自動登録または資格情報ストアの構成は、アプリでの最初のアカウントセットアップ時にのみ適用されます。追加アカウントにはすべて、ユーザー名とパスワードを入力します。

- 作成する最初のアカウントが証明書ベースの場合、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。
- 追加アカウントを外部ネットワークのドメインや Exchange Server に接続できるようにするには、Citrix ADC で分割トンネリングを ［オン］ に設定する必要があります。
- Secure Mail for iOS では、Exchange および Office 365 のメールサーバーのみがサポートされます。

Android で **Exchange** メールアカウントを追加するには、以下を行います

1. Secure Mail を起動し、ハンバーガーアイコンをタップしてから、［設定］ アイコンをタップします。
2. ［アカウント］ で ［アカウントの追加］ をタップします。
3. ［アカウントの追加］ 画面で新規アカウントの資格情報を入力します。

   オプションで、以下のパラメーターの値を設定できます:

   - メールの同期期間: タップしてメールの同期期間の値を選択します。設定した値により、Secure Mail で同期されるメールの同期日数が指定されます。管理者はデフォルト値を設定しています。
   - これをデフォルトアカウントにする: タップして、新規アカウントを自身のデフォルトアカウントとして設定します。この値はデフォルトでは ［オフ］ に設定されています。
4. ［サインイン］ をタップして、アカウントを作成します。

   ［アカウント］ メニューの ［設定］ 画面で新規アカウントを表示できます。

> 注:
>
> 追加アカウントでは Active Directory ベースの認証を使用する必要があります。Secure Mail では、複数のアカウントを構成する場合の証明書ベースの認証はサポートされていません。

アカウントを編集するには

Android でパスワードとメールアカウントの説明を編集できます。

1. Secure Mail を起動し、ハンバーガーアイコンをタップしてから、［設定］ アイコンをタップします。
2. ［アカウント］ で、編集するアカウントをタップします。
3. ［アカウント］ 画面で各フィールドを編集します。
4. ［保存］ をタップして操作を確定するか、［キャンセル］ をタップして ［設定］ 画面に戻ります。

Android でアカウントを削除するには

1. Secure Mail を起動し、ハンバーガーアイコンをタップしてから、［設定］ アイコンをタップします。
2. ［アカウント］ で、削除するアカウントをタップします。
3. ［アカウントの詳細］ 画面で、画面最下部の ［アカウントの削除］ をタップするか、［キャンセル］ をタップして ［設定］ 画面に戻ります。
4. ［削除］ をタップして操作を確定します。

> 注:
>
> デフォルトアカウントを削除すると、次のアカウントがデフォルトアカウントになります。

Android でデフォルトアカウントを設定するには

Secure Mail では、以下の場合にデフォルトアカウントが使用されます:

- メールの作成時: ［差出人:］ フィールドに、デフォルトアカウントのメール ID が自動的に入力されます。
- カレンダーイベントの作成時: ［主催者］ フィールドに、デフォルトアカウントのメール ID が自動的に入力されます。

1 つ以上のメールアカウントを追加する場合、作成する最初のアカウントがデフォルトアカウントとなります。デフォルトアカウントを変更するには、［設定］ に移動して、［全般］ で ［デフォルト］ をタップします。

［デフォルトアカウント］ 画面で、デフォルトに設定するアカウントをタップします。

Android での複数の **Exchange** アカウントの設定

複数の Exchange アカウントが構成されている場合、一部の Secure Mail 設定は各 Exchange アカウントに個別に適用できますが、グローバルに適用される設定もあります。以下の設定はアカウント固有です:

- デフォルト値
- 通知
- 不在

- 受信トレイの同期頻度
- メールの同期期間
- メールを同期する
- S/MIME
- オフラインファイル
- 署名
- クイック返信
- カレンダーを同期する
- 連絡先を同期する
- ローカルの連絡先と同期する
- 設定のエクスポート

これらの設定は［>］アイコンと共に表示されます。[>］アイコンをタップすると、デバイス上にアカウントが表示されます。

特定のアカウントに設定を適用するには、**>** をタップして設定アイテムを展開し、メールアカウントを選択します。

メールボックス画面

［メールボックス］ 画面には、構成されているすべてのアカウントが表示されます。この画面には以下のビューが含まれます。

- すべてのアカウント： 構成されているすべての Exchange アカウントのメールが含まれます。
- 個別のアカウント： 個別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。

メールボックスを表示するには、Secure Mail を起動して、ハンバーガーアイコンをタップします。［メールボックス］ 画面で、アカウントをタップしてオプションを展開します。

［すべてのアカウント］ ビューには複数のアカウントのメールがまとめて表示されますが、以下の操作では、デフォルトアカウン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：

- 新しいメッセージ
- 新しいイベント

［すべてのアカウント］ビューから新規メールを作成する場合に、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て、表示されるメールアカウントから異なる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：］ フィールドに会話の宛先のメールアドレスが自動的に入力されます。

個別のアカウント

デフォルトアカウントとプライマリアカウントは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続きます。

個別のアカウントごとに、作成済みのサブフォルダーが表示されます。

以下の操作は、個別のアカウントのみに制限されています:

- アイテムの移動。
- ［会話］ビューからのメールの作成。
- 連絡先の保存。

アドレス帳

タブバーの ［連絡先］ アイコンをタップして、画面の右上にあるハンバーガーアイコンをタップします。［連絡先］画面に以下のアイテムが表示されます:

- すべての連絡先: 複数のメールアカウントのすべての連絡先が表示されます。このオプションは、複数のメールアカウントが設定されている場合にのみ表示されます。
- 個別のメールアカウント: 構成されている個別のメールアカウントに関連する連絡先が表示されます。
- カテゴリ: 定義済み一覧から作成または選択した連絡先をグループ化した、連絡先カテゴリが表示されます。

連絡先フォルダーを表示するには

> 注:
>
> 連絡先サブフォルダーは、Secure Mail for Android ではサポートされていません。Microsoft Outlook を使用して連絡先のフォルダーまたはサブフォルダーを作成した場合、Secure Mail でこれらのフォルダーを表示できません。

1. 連絡先の画面で、次の操作を行います:
    - 複数のメールアカウントのすべての連絡先を表示するには、［すべての連絡先］をタップします。
    - 特定のメールアカウントの連絡先を表示するには、個別の連絡先をタップします。
2. 特定のカテゴリでグループ化された連絡先を表示するには、カテゴリをタップします。作成したカテゴリに基づいて連絡先をグループ化するか、定義済みの一覧のカテゴリでグループ化するかを選択できます。

個別のアカウントに関連する連絡先をローカルの連絡先と同期することができます。

ローカルの連絡先と同期するには

1. Secure Mail を起動します。

2. ［設定］アイコンをタップして ［連絡先］**>**［ローカルの連絡先と同期する］ の順に移動し、［>］をタップしてメニューを展開します。
3. ［ローカルの連絡先と同期する］ 画面で、同期する連絡先のアカウントを有効にします。
4. ［**OK**］ をタップします。
5. Secure Mail から連絡先へのアクセスを許可するかを求めるプロンプトが表示されたら、［**OK**］ をタップします。

これでこのアカウントの連絡先を正常にエクスポートできました。
この操作を元に戻すには、［設定］**>**［連絡先］**>**［ローカルの連絡先と同期する］ に移動し、アカウントの横にあるスイッチをタップしてこの機能を無効にします。［**OK**］ をタップして操作を確定します。

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色を設定して、個別のアカウントに関連するカレンダーイベントを識別することができます。

> 注:
>
> 個人用カレンダーの機能は、プライマリアカウントまたはデフォルトアカウントに常に関連付けられています（有効な場合）。

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、構成されているすべてのアカウントが表示されます。
2. Exchange アカウントの右に表示されるデフォルトの色をタップします。
   “色” 画面に、アカウントに使用できる色が表示されます。
3. 好きな色を選び、［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。
   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、選択した色が設定されます。

カレンダーの招待状またはイベントを作成すると、［主催者］ フィールドにデフォルトアカウントのメールアドレスが自動的に入力されます。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。

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。この操作を行うと、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検索では、そのアカウントに関する結果のみが表示されます。

Secure Mail の Android Enterprise

Secure Mail および Secure Web for Android は、Android Enterprise（以前の Android for Work）と互換性があります。

前提条件

- この機能を使用するには、デバイスで Android 5.0 以降が動作していることを確認してください。
- オンプレミス環境では、Endpoint Management プロパティ **afw.accounts** を **TRUE** に設定する必要があります。

Endpoint Management で Android Enterprise をセットアップすると、デバイスで業務用モバイルアプリを利用できます。アプリは、次の画像で示されているように Android Enterprise アイコンで識別できます。

Android Enterprise と互換性のある機能

次の表は、Android Enterprise と互換性のある Secure Mail 機能の一覧です。

機能	サポート
Exchange Server の自動検出	X
Secure Ticket Authority（STA）	X
連絡先のエクスポート	X
Microsoft Information Rights Management	X
ロック画面での通知	X
メール同期	X
メール分類	X
S/MIME 署名と暗号化	X
Firebase Cloud Messaging（FCM）サービス	X
先進認証（OAuth）	
複数の Exchange アカウント	X
個人用カレンダー	
メール設定のエクスポート	X
共有デバイス	
Endpoint Management と Microsoft Intune/EMS との統合	

機能	サポート
Office 365	X
LDAP Exchange Server 2010、2013、2016	X
証明書ベースの認証（CBA）	
Go ToMeeting	X
Skype for Business	
個人用配布リスト	X
Citrix Files との互換性	X
シングルサインオンによるメール登録	X

次の表は、Android Enterprise と互換性のある Secure Web 機能の一覧です。

機能	サポート
セキュアブラウズモード	X
完全 VPN モード	X
すべてのアプリの機能	X
Secure Mail との互換性	X

制限事項

- 仕事用プロファイルモードの Android Enterprise で ［ステータスバーの使用を許可］ デバイス制限ポリシーが ［オン］ に設定されている場合、Secure Mail for Android のステータスバーにカレンダーのエクスポートの進行状況およびプッシュ通知が表示されません。ただし、許可されている場合、これらの通知はロック画面には表示されます。詳しくは、「Android Enterprise の設定」を参照してください。

Secure Mail と Slack との統合（プレビュー）

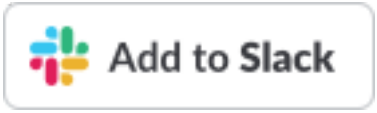
March 29, 2019

iOS または Android デバイスで、メールでの会話を Slack アプリで続けられるようになりました。

この機能を有効にすると、次のような操作を実行できます：

- メールから Slack に、会話をシームレスに切り替えます。
- Slack でグループを作成して、複数のメール受信者と会話します。
- Slack でメール受信者との DM を作成します。

前提条件

- 管理者の場合:
  - Slack ワークスペースに Secure Mail がインストールされていることを確認してください。以下の 

［**Slack** に追加］ ボタンをクリックします。
  - **Slack** の有効化ポリシーが ［オン］ になっていることを確認してください。ポリシーについて詳しくは、以下を参照してください:
    * iOS の Slack ポリシーを有効にする
    * Android の Slack ポリシーを有効にする
- ユーザーの場合: 手順を実行する前に、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 を起動し、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、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］ に表示されている ［**Slack**］ をタップします。
4. ワークスペースに Slack の URL を入力し、 ［続行］ をタップします。
5. 資格情報を入力し、 ［サインイン］ をタップします。
6. Secure Mail による情報へのアクセスを許可するように要求された場合は、 ［許可する］ をタップします。

これで Slack に接続しました。

この機能を利用するには

1. Secure Mail でメールの会話を開き、フローティング操作ボタンをタップします。
2. 表示されるオプションから、 ［**Slack** でチャットする］ をタップします。
3. メールの受信者との会話が Slack に切り替わります。

次の点に注意してください:

- Secure Mail を実行している iOS または Android デバイスでは、メールから最大 8 人の受信者が参加する会話を Slack で作成できます。メールに 8 人以上の受信者がいる場合、デフォルト設定では、メールの受信者のうち最初の 8 人が選択されます。

通知と同期

March 11, 2019

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。

Secure Mail for iOS のアプリのバックグラウンド更新

(APNs ではなく) iOS バックグラウンドアプリ更新を介して通知を提供するように Secure Mail for iOS が構成されると、Secure Mail メール更新は次のように機能します。

- デバイスで［設定］メニューから［**App** のバックグラウンド更新］をオンにしてあり、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。同期間隔はさまざまな要素に従って変化します。
- **App** のバックグラウンド更新機能が無効な場合、WorxMail がバックグラウンドで動作している間はメールを受信しません。
- ユーザーが Secure Mail をバックグラウンドにすると、アプリが一時停止する前に猶予期間内で引き続き実行されます。
- Secure Mail がフォアグラウンドで動作している間は、［**App** のバックグラウンド更新］の設定にかかわらずリアルタイムでメールのアクティビティが表示されます。

Secure Mail と **ActiveSync**

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 メール、連絡先、カレンダーイベント、自動的に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ません。Exchange Server 2013 では、ActiveSync は［下書き］フォルダーと同期しません。

ユーザーの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一覧が表示されます。
4. 同期するフォルダーをタップします。

Android

1. メールボックス一覧に移動します。
2. 同期するメールボックスをタップします。
3. 右下隅にある More の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］ で、フォルダーの同期頻度を選択します。

Secure Mail での連絡先のエクスポート

Secure Mail ユーザーは、連絡先を携帯のアドレス帳と継続して同期したり、個別の連絡先を携帯のアドレス帳に 1 回のみエクスポートしたり、vCard 添付ファイルとして連絡先を共有したりできます。

この機能を有効にするには、Endpoint Management コンソールで Secure Mail 用の連絡先のエクスポートポリシーを ［オン］ に設定します。

このポリシーが ［オン］ になっていると、Secure Mail で次のオプションを使用できます:

- ［設定］の ［ローカルの連絡先と同期する］
- 個別の連絡先のエクスポート
- 連絡先を vCard 添付ファイルとして共有する

連絡先のエクスポートポリシーが ［オフ］ の場合、これらのオプションはアプリに表示されません。

ポリシーが有効な場合に、継続的にメールサーバーから携帯のアドレス帳に連絡先を同期するには、［ローカルの連絡先と同期する］を［オン］にする必要があります。［ローカルの連絡先と同期する］が［オン］の場合、Exchange または Secure Mail で連絡先が更新されると、ローカルの連絡先も更新されます。

Android の制限のため、Exchange または Hotmail のアカウントがローカルの連絡先に同期するように既に設定されている場合、Secure Mail で連絡先を同期することはできません。

iOS では、デバイスで Hotmail または Exchange が設定されていても、Secure Mail の連絡先をエクスポートして電話の連絡先と同期できます。この機能は、Endpoint Management で、Secure Mail のネイティブ連絡先の確認を上書きするポリシーで設定します。このポリシーによって、ネイティブの連絡先アプリに構成された Exchamge/Hotmail アカウントからの連絡先の確認を Secure Mail によって上書きするかどうかが決定されます。これが ［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る場合でも、アプリによって連絡先がデバイスに同期されます。［オフ］ の場合、アプリは連絡先同期のブロックを継続します。デフォルトは ［オン］ です。

Secure Mail の通知

次の表は、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中の場合に、サポートされているモバイルデバイスに対して通知がどのように処理されるかを説明するものです。

フォアグラウンドまたはバックグラウンドで Secure Mail を実行している場合:	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 は永続的 ActiveSync 接続を維持し、メールおよびカレンダーのアクティビティを同期します。	Secure Mail は永続的 ActiveSync 接続を維持し、メールおよびカレンダーのアクティビティを同期します。
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 APNs を介して通知を受信します。	Secure Mail は永続的 ActiveSync 接続を維持します。

構成について詳しくは、「Secure Mail for iOS のプッシュ通知」を参照してください。

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ます。リッチ通知機能により、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の通知を確実に受信できます。この機能は、パスワードベースの認証セットアップとクライアントベースの認証セットアップでサポートされています。

> 注:
>
> この機能をサポートするアーキテクチャが変更されたため、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、次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 ［オン］ に設定します。
- ネットワークアクセスポリシーは、［制限なし］ または ［内部ネットワークへトンネル］ に設定されています。ネットワークアクセスポリシーが ［内部ネットワークへトンネル］ に設定されている場合は、バックグラウンドネットワークサービスポリシーで Exchange Web サービス（EWS）ホストが設定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設定されていることを確認します。
- ロック画面上の通知を制御ポリシーは、［許可］ または ［メールの送信者またはイベントのタイトル］ に設定されています。
- ［**Secure Mail**］ **>** ［設定］ **>** ［通知］ の順に移動し、［メール通知］ を有効にします。

この機能は、次のいずれかの設定を実行している場合はサポートされていません。

- Microsoft Office 365 の先進認証（Oauth）
- Endpoint Management と Microsoft Intune/EMS との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

iOS デバイスに「新しいメールがあります」という通知が表示される理由

メッセージ詳細の取得に必要な指定時間である 30 秒以内に Secure Mail が Exchange Web サービス（EWS）から応答を受信しなかった場合、iOS デバイスに「新しいメールがあります」という通知が表示されます。

Wi-Fi またはデータ接続の質が低い場合に、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、Secure Mail では、次の場合にも「新しいメールがあります」という通知が表示されます:

- 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。この事象は通常、デバイスの再起動後、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 との接続やセキュアチャネル設定に失敗した場合。
- 資格情報の有効期限が切れたとき、または資格情報を変更したがまだ Secure Mail で更新されていないとき。次の図は、このような事象で通知がどのように表示されるかを示しています。
- Secure Mail が、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け取ったとき。EWS 応答コードについて詳しくは、Microsoft 社の開発者ドキュメントを参照してください。

Secure Mail for iOS のプッシュ通知の失敗メッセージ

Secure Mail for iOS では、デバイスの通知センターに適切なプッシュ通知の失敗メッセージが表示されます。これらの通知は、失敗した通知の種類に基づいて表示されます。

次のようにそれぞれの失敗内容ごとに通知メッセージが表示されます:

- **Secure Mail** が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 SOCKS5 接続を確立できない場合に表示されます。
- **Secure Mail** が組織のネットワークに接続できません。管理者に連絡してください。この通知は Citrix Gateway にアクセスできない場合に表示されます。Citrix ADC が正しく構成され、外部ネットワークから通信できることを確認してください。
- **Secure Mail** が組織のネットワークに安全に接続できません。管理者に連絡してください。この通知は、Secure Mail が Citrix Gateway と SSL 接続を確立できない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** がメールサーバーに安全に接続できません。管理者に連絡してください。この通知は、Secure Mail が Exchange Server と SSL 接続を確立できない場合に表示されます。Exchange Server で SSL 証

明書が有効であることを確認してください。有効な証明書がないアプリを Exchange Server に接続する場合、「すべての SSL 証明書を承認する」MDX ポリシーを承諾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** がメッセージを取得できません。管理者に連絡してください。Secure Mail が Exchange Server からの EWS 応答を解析できない場合、この通知が表示されます。
- 要求がタイムアウトになったため、**Secure Mail** がメッセージを取得できません。Secure Mail が 30 秒以内にサーバーから応答を受信できない場合、この通知が表示されます。デバイスのデータや Wi-Fi 接続が不十分な場合に、この通知が表示されることがあります。数分待ってから再試行してください。
- メッセージを取得できません。**Secure Mail** を起動してください。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、この通知が表示されます。デバイスが再起動されたときにロック解除されていない場合、この通知が表示されることがあります。デバイスをロック解除すると、Secure Mail が自動的にセキュアコンテナにアクセスできます。この通知を受信し続ける場合、Secure Mail を起動してセキュアコンテナの資格情報を自動的に更新します。

Secure Mail のプッシュ通知

March 11, 2019

Secure Mail for iOS および Secure Mail for Android では、アプリがバックグラウンドで実行中、または終了しても、メールおよびカレンダーのアクティビティに関する通知を受け取ることができます。Secure Mail for iOS は、［App のバックグラウンド更新］による通知、または Apple Push Notification service（APNs）によるプッシュ通知をサポートします。Secure Mail for Android は、Firebase Cloud Messaging Service（FCM）による通知をサポートします。

プッシュ通知の動作

Secure Mail は次の受信トレイでのアクティビティについて、プッシュ通知を送信します。

- 新しいメール、会議要求、会議キャンセル、会議更新： APNs により受信ボックスに通知がプッシュされると、Secure Mail によりカレンダーを含むすべてのフォルダーが更新されます。これにより、会議の変更がユーザーのカレンダーに直ちに反映されます。
- **iOS** の場合、メールの状態を既読から未読に、または未読から既読に変更。Secure Mail アイコンは、Exchange の受信トレイのフォルダー内の未読メッセージと新規メッセージの合計のみを表示します。ユーザーがデスクトップまたはノートブックコンピューターでメールを開いた後、Secure Mail はアイコンを更新します。

  iOS では、同期期間中、受信トレイの未読メッセージ数は表示されたままになります。ロック画面上の通知を制御ポリシーが ［オン］ の場合、iOS が Secure Mail をウェイクアップして同期を実行した後プッシュ通知がロックされたデバイス画面に表示されます。

インストールまたはアップグレード中、Secure Mail for iOS によりプッシュ通知を許可するプロンプトがユーザーに表示されます。また、iOS の設定を使ってプッシュ通知を後から許可することもできます。

iOS および Android にプッシュ通知を提供するため、Amazon Web Services（AWS）のリスナーサービスがホストされ、次の機能が実行できるようになります。

- 受信トレイにアクティビティがある場合に Exchange Server により送信された Exchange Web Services（EWS）プッシュ通知をリスンします。Exchange はメールコンテンツを Citrix サービスに送信しません。

  Citrix サービスは、個人を識別可能な情報を保存しません。代わりに、デバイストークンおよびサブスクリプション ID により特定のデバイスおよび受信トレイのフォルダーが識別され、Secure Mail 内で更新されます。
- iOS デバイス上の Secure Mail にバッジ数のみを含む APNs 通知を送信します。
- Android デバイス上の Secure Mail に FCM 通知を送信します。

Citrix リスナーサービスは、ユーザーデバイスと Exchange Server 間で ActiveSync を介して引き続きフローするメールデータトラフィックには影響を与えません。高可用性および障害復旧用に構成されるリスナーサービスは、次の 3 つの地域で利用できます。

- 南北アメリカ
- ヨーロッパおよび中近東およびアフリカ（EMEA）
- アジア太平洋（APAC）

プッシュ通知のシステム要件

Citrix Gateway 構成に Secure Ticket Authority（STA）が含まれていて分割トンネリングがオフの場合、Citrix Gateway は（Secure Mail からトンネル処理される場合は）次の Citrix リスナーサービス URL へのトラフィックを許可する必要があります。

Region（リージョン）	URL	IP アドレス
南北アメリカ	https://us-east-1.pushreg.xm.citrix.com	52.7.65.6; 52.7.147.0
EMEA（欧州、中東、アフリカ）	https://eu-west-1.pushreg.xm.citrix.com	54.154.200.233; 54.154.204.192
アジア太平洋	https://ap-southeast-1.pushreg.xm.citrix.com	52.74.236.173; 52.74.25.245

プッシュ通知のための **Secure Mail** の設定

アプリストア配信用の Secure Mail で Apple プッシュ通知または FCM をセットアップするには、Endpoint Management コンソールでプッシュ通知を ［オン］ に設定してからリージョンを選択します。次の図は、iOS での設定です。

次の図は、iOS と同様の Android のプッシュ通知設定です。さらに、EWS がメールサーバーとは異なるリージョンでホストされている場合、［**EWS** ホスト名］ 設定に入力します。デフォルト値は空です。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。

Exchange と Citrix ADC がトラフィックをリスナーサービスにフローできるように設定します。

Exchange Server 構成

ファイアウォールから Exchange Server があるリージョンの Citrix リスナーサービス URL に SSL を送信できます（ポート 443）。次に例を示します:

Region（リージョン）	URL	IP アドレス
南北アメリカ	https://us-east-1.mailboxlistener.xm.citrix.com	52.6.252.176; 52.4.180.132
EMEA（欧州、中東、アフリカ）	https://eu-west-1.mailboxlistener.xm.citrix.com	54.77.174.172; 52.17.147.220
アジア太平洋	https://ap-southeast-1.mailboxlistener.xm.citrix.com	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は、次のうちいずれか選択できます。

- 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する。
- プロキシをバイパスして 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する。

EWS トラフィックをプロキシサーバー経由で送信するには、ClientAccess\exchweb\ews フォルダーの EWS 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>
```

プロキシの構成について詳しくは、「プロキシ構成」を参照してください。

Exchange 2013 環境では、`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。追加しない場合、ここで説明した構成を使用します。トラブルシューティングに関しては、Exchange の管理担当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、バイパスの一覧を構成して 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。詳しくは、「Endpoint Management の高度な設定」の記事を参照してください。

Citrix Gateway 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、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。これによってデバイスが接続してプッシュ通知を登録できます。

EWS および ActiveSync サーバーが異なる場合、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。

トラブルシューティング

発信接続をトラブルシューティングするには、Exchange のイベントログをチェックします。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あるいはエラーだった時のログエントリが含まれています。また、Exchange Server で Wireshark トレースを実行して、Citrix ライセンスサービスへの発信トラフィックを追跡できます。

その他の問題については、「Secure Mail Test Tool」を参照してください。

Secure Mail のプッシュ通知に関するよくある質問

iOS は、どのタイミングで Secure Mail に通知を配信しますか

Secure Mail がフォアグラウンドで実行されている場合、通知は常に Secure Mail に配信されます。これは、通知の配信を保証できる唯一の状況です。Secure Mail がバックグラウンドに移動すると、アプリケーションのバッジ数は常に更新されます。ただし、ロック画面およびバナー通知などの通知は、[App のバックグラウンド更新] に依存するため、通知は確実ではありません（特に iOS がアプリを中断または停止する場合）。以下の要因は、制御できません。

以下の場合は、通知の配信に影響を与えることがあります：

- バッテリー残量が低下している。
- Secure Mail が頻繁に使用されない（フォアグラウンドで起動されることが少ない）。
- アプリがバックグラウンドで長時間中断されていて、メールをコア使用時間外（例：真夜中から午前 6 時の間）に受信する。

通知は、以下の場合に Secure Mail に配信されません：

- ユーザーが Secure Mail を終了した（それ以降、ユーザーが手動でアプリを再起動するまでの間）。
- Secure Mail が強制終了し、アプリが自動的に再起動されていない。
- Secure Mail がアクティブではない。

> 重要：
>
> Secure Mail が、以下のようなさまざまな理由でアクティブではない場合、Secure Mail に通知が配信されないことがあります：
>
> - デバイスが省電力モードで、Secure Mail がバックグラウンドで動作している。これは、通知が送信されない最も一般的なケースです。
> - Secure Mail の［App のバックグラウンド更新］がオフか、Secure Mail がバックグラウンドで動作している。ユーザーは、この設定を制御できます。
> - デバイスのネットワーク接続状態が不十分である。この状況は、完全に iOS デバイスに依存します。

Secure Mail が通知を受信しない場合、Secure Mail は、新しいデータをデバイスと同期しません。その結果、以下のような状況になります：

- Secure Mail は、ユーザーがアプリをバックグラウンドに移動したときのみデータと同期する。
- ロック画面の新しいメールの通知が停止する。カレンダー通知は、引き続き表示されます。

Android は、どのタイミングで **Secure Mail** に通知を配信しますか

Android では、常に通知が Secure Mail に配信されます。

FCM はロック画面でのメール通知の表示にどのような影響を与えますか

デバイスのロック画面に表示される新しいメールの通知は、Secure Mail がデバイスに同期したデータに基づいて生成されます。この情報は、リスナーサービスによるものではないことにご注意ください。

新しいメール通知を表示するには、Secure Mail は、Exchange からのデータを同期する必要があります。これによって、Secure Mail が通知を作成するための情報を使用できます。

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。メールの同期がバックグラウンドで完了すると、Secure Mail に新しいメールが表示されます。

［**App** のバックグラウンド更新］は、**Secure Mail** および **APNs** にどのような影響を与えますか

ユーザーが、［App のバックグラウンド更新］をオフにすると、以下のような状況になります：

- Secure Mail がバックグラウンドアプリではない場合、Secure Mail は通知を受信しない。
- Secure Mail は、ロック画面で新しいメールの通知を表示しない。

［App のバックグラウンド更新］を無効にすると、Secure Mail の動作に大幅に影響を及ぼします。前述のとおり、APNs に基づくバッジは依然として更新されますが、メールはこのモードのデバイスと同期しません。

省電力モードにすると、**Secure Mail** および **APNs** はどのような影響を受けますか

［App のバックグラウンド更新］が無効な場合、Secure Mail に関連したシステムは、省電力モードのときと同様の動作をします。省電力モードでは、デバイスは定期的な更新のためにアプリを起動したり、バックグラウンドでアプリに通知を配信したりしません。そのため、前述の「App のバックグラウンド更新」部分に記載されている場合と同様の影響があります。省電力モードでは、システムは APNs 通知に基づいてアプリのバッジを表示し続けます。

APNs はロック画面でのメール通知の表示にどのような影響を与えますか

デバイスのロック画面に表示される新しいメールの通知は、Secure Mail がデバイスに同期したデータに基づいて生成されます。この情報は、リスナーサービスによるものではないことにご注意ください。

新しいメール通知を表示するには、Secure Mail は、Exchange からのデータを同期する必要があります。これによって、Secure Mail が通知を作成するための情報を使用できます。

バックグラウンドで、APNs 通知が Secure Mail に配信されない場合、Secure Mail は通知を検出せず、新しいデータと同期しません。Secure Mail で使用できる新しいデータがないため、APNs 通知が配信されない場合、デバイスのロック画面でメール通知が生成されません。

FCM による同期がバックグラウンドで失敗するのは、どのような問題によるものですか

以下を含むさまざまな問題によって、FCM による同期の要求が失敗します：

- 無効な STA チケット。
- Secure Mail が Doze モードで起動すると、アプリがサーバーのすべてのデータと同期するのに 30 秒かかります。

上のいずれかの状況が発生した場合、Secure Mail はデータを同期できません。その結果、通知がロック画面に表示されないことがあります。

APNs による同期がバックグラウンドで失敗するのは、どのような問題によるものですか

以下を含むさまざまな問題によって、APNs による同期の要求が失敗します：

- 無効な STA チケット。
- 遅いネットワーク接続。Secure Mail がバックグラウンドで起動すると、アプリがサーバーのすべてのデータと同期するのに 30 秒かかります。
- データ保護ポリシーが有効で、APNs 通知によって Secure Mail が起動される場合、デバイスがロックされると Secure Mail はデータストアにアクセスできず、同期も発生しない。これは、システムが、Secure Mail をコールドスタート（再起動）しようとする場合のみです。ユーザーがデバイスのロック解除後に既に Secure Mail を起動している場合、デバイスがロックされていても APNs による同期は成功します。

上記のいずれかの状況が発生すると、Secure Mail はデータを同期して、ロック画面に通知を表示することはできません。

通知が配信されない、または **APNs** が使用されていない場合、**Secure Mail** がロック画面に通知を表示するにはどうすればよいですか

APNs が無効な場合でも、iOS の［App のバックグラウンド更新］が有効で、省電力モードがオフになっている場合、Secure Mail は定期的な［App のバックグラウンド更新］イベントによって起動されます。

起動イベント中、Secure Mail は Exchange Server の新しいメールと同期します。この新しいメールを使用して、ロック画面でメール通知を生成できます。そのため、APNs 通知が配信されない、または APNs が無効な場合でも、Secure Mail はバックグラウンドでデータを同期できます。

APNs を使用中で、APNs 通知が Secure Mail に配信される場合に比べると、リアルタイムで通知されないことが多くなることにご注意ください。iOS が APNs 通知を Secure Mail にルーティングすると、アプリは即座にサーバーのデータと同期して、ロック画面の通知がリアルタイムで表示されます。

［App のバックグラウンド更新］による起動が必要なイベントでは、ロック画面の通知はリアルタイムで発生しません。この場合、iOS の判断する頻度のみで Secure Mail が起動されます。このため、メールが Exchange の受信トレイに到着する時間と、Secure Mail がメッセージと同期して、ロック画面の通知を生成する時間にずれが生じることがあります。

また、APNs が使用中であっても、Secure Mail がこのような定期的な起動を受信することにご注意ください。［App のバックグラウンド更新］が Secure Mail を起動するあらゆる状況で、Secure Mail は Exchange のデータと同期しようとします。

Secure Mail とロック画面にコンテンツを表示する他のアプリとの違いはどのようなものですか

重要な違いがあり、これが混乱を招くことがあります。Secure Mail は、Gmail、Microsoft Outlook、その他のアプリと違い、常にロック画面にリアルタイムで新しいメールを表示するわけではありません。この違いの主な理由は、セキュリティによるものです。他のアプリの動作に合わせるために、Citrix リスナーサービスには資格情報が必要です。この資格情報で、メールの内容を取得するために Exchange に認証し、Citrix リスナーサービスや Apple APNs サービスを通してこのメールの内容を渡すことができます。APNs 通知に対するシトリックスのアプローチでは、Citrix リスナーサービスがユーザーのパスワードを取得して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することはありません。

一方、ネイティブの iOS メールアプリでは、メールサーバーへの一貫した接続を維持し、通知が常に配信されるようにします。ネイティブのメールアプリではないサードパーティ製のアプリでは、この機能は許可されません。

Gmail アプリの動作: Google は、Gmail アプリおよび Gmail サーバーの両方を所有し、制御します。このため、Google はメッセージの内容を読み取り、APNs 通知ペイロードにメッセージの内容を含めることができます。iOS は Gmail からこの APNs 通知を受信すると、以下を実行します:

- 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の内容を使用して、ロック画面の通知を表示します。

これは、重要な違いです。ペイロードに含まれるデータに基づいてロック画面に通知を表示するのは、iOS であって Gmail アプリではありません。実際、通知を受信した場合、iOS は Gmail アプリを起動しません。これは、iOS が Secure Mail を起動しないのと同様です。しかし、メッセージスニペット（冒頭部分）を含むペイロードによって、iOS はデバイスにメールデータを同期せずにロック画面の通知を表示できます。

Secure Mail の場合は違います。ロック画面に通知を表示するには、最初に Exchange の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 は Outlook for iOS を制御します。しかし、データを取得する Exchange Server を制御するのは、ユーザーが所属する組織です。こうしたセットアップにもかかわらず、Outlook は Microsoft が APNs 通知で提供するデータに基づいて、ロック画面の通知を表示できます。これは、Outlook for iOS が、Microsoft によるユーザー資格情報を保存するモデルを利用するためです。次に、Microsoft は、クラウドサービスから直接ユーザーのメールボックスにアクセスし、新しいメールを確認します。

新しいメールがあれば、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 モデルと同じ方法で動作します。Gmail モデルでは、iOS は単純にデータを取得してデータに基づいてロック画面の通知を生成します。Outlook iOS アプリは、このプロセスに関係していません。

Outlook for iOS の重要なセキュリティメモ: Outlook for iOS アプローチには、明確に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に関して Microsoft を信頼する必要があり、これによって Microsoft はユーザーのメールボックスにアクセスできるため、セキュリティリスクにつながります。Microsoft がユーザーのパスワードを管理する方法について詳しくは、Microsoft TechNetを参照してください。

プッシュ通知の管理者に関連したよくある質問については、Support Knowledge Center のこの記事を参照してください。ユーザー向けのよくある質問については、Support Knowledge Center のこの記事を参照してください。

Secure Mail と他の業務用モバイルアプリおよび **Citrix Files** との相互作用

February 11, 2019

Secure Mail は他の業務用モバイルアプリや Citrix Files と連係できるため、組織のポリシーにより設定されたセキュアな環境から出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、および保存できます。たとえば、Secure Mail 内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、Citrix QuickEdit

for Endpoint Management 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 Citrix Files for Endpoint Management の領域にダウンロードされます。

プラットフォームごとの Secure Mail 機能の詳細な一覧については、「プラットフォームごとの機能」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

March 11, 2019

Secure Mail が正常に動作しない場合、原因は一般的に接続の問題です。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は、この記事に問題のトラブルシューティングが記載されています。

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 Autodiscovery Service のチェックを行うことができます。Endpoint Management Analyzer が、Endpoint Management Exchange ActiveSync Test アプリケーションのダウンロード方法をガイドします。メールテストオプションは、メールサーバーの基本的な接続設定を確認します。このツールは、Endpoint Management 環境での ActiveSync サーバーの展開の準備に関するトラブルシューティングにも役立ちます。詳しくは、「Endpoint Management Analyzer ツール」を参照してください。

Endpoint Management Analyzer のメールテストオプションは、次のことを確認します:

- iOS および Android デバイスが Microsoft Exchange または IBM Traveler サーバーと接続しているか。
- ユーザー認証。
- Exchange Server、Exchange Web Services (EWS)、Citrix Gateway、APN 証明書、および 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詳しくは、「Secure Mail for iOS のプッシュ通知」を参照してください。

ツールにより、問題の修正についての包括的な推奨事項の一覧が提供されます。

> 注:
>
> Mail Test アプリである MailTest.ipa は推奨されていません。代わりに、Endpoint Management Analyzer で同じ機能にアクセスします。

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。
- [メール作成を禁止] ポリシーを [オフ] に設定します。

Secure Mail ログを使った接続の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、以下を実行します。

1. ［**Secure Hub**］**>**［ヘルプ］**>**［問題の報告］ の順に選択します。
2. アプリの一覧から［**Secure Mail**］を選択します。

   組織のヘルプデスク宛の電子メールが開きます。
3. 件名行と、問題を簡単に説明する本文を入力します。
4. 発生した時間を選択します。
5. ログの設定は、サポートチームからそうするように指示があった場合にのみ、変更します。
6. ［送信］ をクリックします。

   完成したメッセージが開きます。圧縮されたログファイルが添付されています。
7. ［送信］ をもう一度クリックします。

   送信される圧縮ファイルには、次のログが含まれています:

   CtxLog_AppInfo.txt（iOS）、Device_And_AppInfo.txt（Android）、logx.txt and WH_logx.txt（Windows Phone）

アプリ情報のログにはデバイスおよびアプリに関する情報が含まれます。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互換性があるか確認します。詳しくは、「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（iOS）および VpnConfig.xml（Android）

VPN 構成ログは Secure Hub に対してのみ提供されます。最新の Citrix ADC リリースが使用されているか Citrix ADC のバージョン（`ServerBuildVersion`）をチェックします。以下のように`SplitDNS`および`SplitTunnel`の設定を確認してください:

- Split DNS が［**Remote**］、［**Local**］、または［**Both**］に設定されている場合、DNS を介してメールサーバー FQDN を正しく解決しているか確認します（Split DNS は Android 上の Secure Hub で使用できます）。
- Split Tunnel が ［オン］ に設定されている場合、バックエンド上でアクセスできるインターネットアプリの 1 つとしてメールサーバーが一覧表示されていることを確認してください。
- CtxLog_AppPolicies.xml（iOS）、Policy.xml（Android および Windows Phone）

ポリシーのログは、ログを取得した時点で Secure Mail に適用されるすべての MDX ポリシーの値を提供します。接続の問題の場合、<`BackgroundServices`>および<`BackgroundServicesGateway`>ポリシーの値を確認します。

- 診断ログ（diagnostics フォルダー内）

Secure Mail の初期構成において最も一般的な問題は、「現在会社のネットワークを使用できない」という場合です。診断ログを使って接続の問題をトラブルシューティングするには、次の手順に従います。

診断ログのキーの列は Timestamp、Message Class、Message です。Secure Mail にエラーメッセージが表示されたら、その時間をメモしておくと **Timestamp** 列で関連のログエントリをすぐに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別するには、AG Tunneler のエントリを確認します。次のメッセージは接続に成功したことを示しています:

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

Citrix Gateway から Endpoint Management への接続が成功した（およびそれによって STA チケットを検証できる）かどうかを判別するには、以下を行います: Secure Hub の診断ログを開き、デバイスが登録された時間の Message Class の INFO (4) の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ています:

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

> 注:
>
> 登録中に、Secure Hub は STA チケットの要求を Endpoint Management に送信します。Endpoint Management は STA チケットをデバイスに送信し、チケットはデバイスに保存され、Endpoint Management STA チケット一覧に追加されます。

Endpoint Management が STA チケットを発行したかどうか判別するには、サポートバンドルに含まれている UserAuditLogFile.log をチェックします。そこには、各チケット、発行時間、ユーザー名、ユーザーデバイス、および結果の一覧があります。次に例を示します:

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

User: user2

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

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

Citrix Gateway からメールサーバーへの通信をチェックするには、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。この確認を行うには、Secure Web を使って Outlook Web Access（OWA）にアクセスします。Secure Mail のように、Secure Web はマイクロ VPN トンネルを使って Citrix Gateway への接続を確立します。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動作します。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 を開いて OWA ページの FQDN を入力します。要求は、Citrix Gateway とメールサーバー間の通信と同じルートおよび DNS となります。OWA ページが開いたら、Citrix Gateway がメールサーバーと通信していることになります。

チェックが通信に成功したことを示す場合、Citrix セットアップは問題ありません。ただし、Exchange または Traveler サーバーに問題があることになります。

Exchange または Traveler サーバー管理者のため情報を収集できます。最初に、Secure Mail の診断ログで「Error」という用語を検索して Exchange または Traveler サーバーで HTTP の問題をチェックします。エラーに HTTP コードが含まれていて複数の Exchange または Traveler サーバーを実行している場合は、各サーバーで調査を実行します。Exchange および Traveler には、クライアントデバイスからの HTTP 要求や応答を示す 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。

Secure Mail for iOS のクラッシュログをデバイスから取得するには

1. iOS デバイスで、［設定］>［プライバシー］>［解析］>［解析データ］ の順に移動します。
2. ［データ］ 一覧で、対象アプリの名前と対象の日付の組み合わせをクリックします。ログが表示されます。

メール、連絡先、カレンダーの問題のトラブルシューティング

メールが下書きのままとなる、連絡先が消失する、カレンダーアイテムを同期できないなどの Secure Mail の問題をトラブルシューティングできます。このような問題をトラブルシューティングするには、Exchange ActiveSync メールボックスのログを使用します。このログは、デバイスから送信された受信要求やメールサーバーからの送信応答を示しています。

詳しくは、TechNet のブログ記事Under the Hood: Exchange ActiveSync Mailbox Log Analysisを参照してください。

無制限同期のベストプラクティス

ユーザーがメール同期期間を ［すべて］ に設定すると、同期が無制限になります。無制限の同期では、受信トレイおよび同期されるすべてのサブフォルダーが含まれるメールボックスサイズをユーザーが管理するものとみなされます。最善のパフォーマンスを得るために、次のような項目が挙げられます。

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サイズ 600 MB を超過すると、メールの同期速度が遅くなることがあります。
2. ［**Wi-Fi** 接続時に添付ファイルを読み込む］ を無制限の同期で有効にすることはお勧めしません。このオプションによって、デバイスのメールサイズがすぐに膨張する可能性があります。
3. ユーザーが無制限同期を選択できないようにするには、［最大同期間隔］ アプリポリシーを ［すべて］ 以外に設定します。
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。

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