



CHAPTER 1

Cisco Business Class Email for Android の設定と使用

- [概要 \(1-1 ページ\)](#)
- [最新情報 \(1-2 ページ\)](#)
- [ライセンス バージョンおよびコンフィギュレーション モード \(1-2 ページ\)](#)
- [サポートされるオペレーティング システム \(1-2 ページ\)](#)
- [Cisco Business Class Email アプリケーションのダウンロードおよびインストール \(1-3 ページ\)](#)
- [Cisco Business Class Email for Android アプリケーションの起動 \(1-3 ページ\)](#)
- [Cisco Business Class Email の設定ファイルの起動 \(1-4 ページ\)](#)
- [Cisco Business Class Email の設定 \(1-5 ページ\)](#)
- [コンフィギュレーション モードごとの使用可能な電子メール暗号化オプション \(1-7 ページ\)](#)
- [Message Security \(1-16 ページ\)](#)
- [キャッシュ管理 \(1-16 ページ\)](#)
- [診断ツールを使用したトラブルシューティング \(1-17 ページ\)](#)
- [Cisco Business Class Email アプリケーションのアップグレード \(1-18 ページ\)](#)
- [Cisco Business Class Email アプリケーションのアンインストール \(1-18 ページ\)](#)
- [カスタマー サポート \(1-18 ページ\)](#)

概要

Cisco Business Class Email (BCE) モバイル アプリケーションは、暗号化された電子メール メッセージの送受信を Google Android デバイス上で直接行う機能を提供します。Cisco BCE モバイル アプリケーションのコンフィギュレーション モードに応じて、次のタスクを実行できます。

- Cisco BCE を使用して、暗号化された電子メールを Android デバイス上で開く
- Cisco BCE を使用して、暗号化された電子メールを Android デバイスから送信する
- Cisco BCE を使用して、Android デバイスから送信した安全な電子メールを管理する
- Cisco BCE を使用して、暗号化して Android デバイスから送信した電子メールをロックまたはロック解除する

- Cisco BCE を使用して、暗号化して Android デバイスから送信した電子メールの有効期限を設定または変更する
- Cisco BCE を使用して、暗号化して Android デバイスから送信した電子メールに対する開封確認を受信する
- 暗号化された電子メールのオプションを Android デバイスで確認または変更する

最新情報

このリリースには、次の新機能が含まれています。

- 登録済みエンベロープに受信者言語を選択できるようになりました。この新しいオプションでは、受信者に設定されたロケールに応じてどの言語をメッセージ本文に使用するかを指定することができます。詳細については、「[アカウント設定](#)」セクション(1-6 ページ)を参照してください。

ライセンス バージョンおよびコンフィギュレーションモード

Cisco Business Class Email アプリケーションでは、導入できるライセンス バージョンが2種類あり、そのバージョンによってアプリケーションのコンフィギュレーション モードが決まります。Cisco BCE アプリケーションのデフォルトのコンフィギュレーション モードは Decrypt Only です。

2 種類のライセンス バージョンとコンフィギュレーション モードは次のとおりです。

- **Decrypt Only:** 受信した安全な電子メール メッセージを復号化したり、受信メッセージに転送して応答することができます。復号化アカウントを作成するには、ネイティブの電子メールシステムを使用して安全な電子メールを開きます。
- **Decrypt and Encrypt:** 安全な電子メール メッセージを暗号化および復号化できます。暗号化されたアカウントを作成するには、「[Cisco Business Class Email の設定ファイルの起動](#)」セクション(1-4 ページ)の説明に従って、管理者から受信したコンフィギュレーション ファイルを適用します。

サポートされるオペレーティング システム

Cisco 暗号化互換性マトリクスには、Cisco BCE でサポートされているオペレーティング システムが掲載されており、以下の URL からアクセスできます。

http://www.cisco.com/en/US/docs/security/iea/Compatibility_Matrix/IEA_Compatibility_Matrix.pdf

Cisco Business Class Email アプリケーションのダウンロードおよびインストール

Cisco BCE アプリケーションをインストールするには、Android デバイスで [Google Play](#) にアクセスして [Cisco BCE](#) アプリケーションを検索します。アプリケーションをダウンロードし、目的のデバイス上でインストールを開始します。暗号化されたアカウントを作成するには、「[Cisco Business Class Email の設定ファイルの起動](#)」セクション(1-4 ページ)の説明に従って、管理者から受信したコンフィギュレーション ファイルを適用する必要があります。BCE アカウントのタイプの詳細については、[ライセンス バージョンおよびコンフィギュレーション モード](#) (1-2 ページ)を参照してください。

Cisco Business Class Email for Android アプリケーションの起動

Android デバイスに Cisco BCE アプリケーションを正常にインストールすると、新しく *Cisco BCE* アプリケーションのアイコンが表示されます。このアプリケーションを起動するには、Android ホーム画面にある **Cisco BCE** のアイコンをタップします。



注

同じデバイスで BCE の電子メールを開く場合でも複数の CRES または IEA のアカウントを使用できます。複数のアカウントを作成するには、アカウントが異なるサーバに関連付けられるように設定します。これらのアカウントにはそれぞれ独自のアカウント設定があります。また、別のアカウントはオフライン メッセージを開いたときに作成されます。

電話機用アプリケーションのランディング画面

Cisco BCE のアイコンをタップするとアプリケーションのランディング画面が開きます。

次の表は、アプリケーションのランディング画面にあるオプションをまとめたものです。

オプション	説明
[account name] > General Settings	一般的な設定を行う設定画面を開きます。 Cisco Business Class Email の設定 (1-5 ページ) を参照してください。
[account name] > [account name] (account settings)	アカウント設定の設定画面を開きます。 Cisco Business Class Email の設定 (1-5 ページ) を参照してください。
[account name] > [Inbox]	選択したアカウントで開いている暗号化された電子メールのリストが表示されます。
[account name] > [Manage]	自分のデバイスおよび他のデバイスから送信された電子メール メッセージを管理できます。アカウントを選択して、現在のデバイスから送信されていないメッセージをサーバからロードできます。自分の電子メール アカウントから暗号化して送信した電子メールのリストを表示できます。
[Search] アイコン	受信箱または送信したメッセージを検索できます。

オプション	説明
[Secure Compose] アイコン	安全なメッセージを作成するための画面を開きます。 暗号化した電子メールの送信 (1-14 ページ) を参照してください。
Android の [Menu] ボタン > [Settings]	BCE アプリケーションの設定画面を開きます。 Cisco Business Class Email の設定 (1-5 ページ) を参照してください。

タブレット用アプリケーションのランディング画面

Cisco BCE のアイコンをタップするとアプリケーションのランディング画面が開きます。次の表は、アプリケーションのランディング画面にあるオプションをまとめたものです。

オプション	説明
[account name] > General Settings	一般的な設定を行う設定画面を開きます。 Cisco Business Class Email の設定 (1-5 ページ) を参照してください。
[account name] > [account name] (account settings)	アカウント設定の設定画面を開きます。 Cisco Business Class Email の設定 (1-5 ページ) を参照してください。
Inbox	選択したアカウントで開いている暗号化された電子メールのリストが表示されます。
Manage	自分のデバイスおよび他のデバイスから送信された電子メールメッセージを管理できます。アカウントを選択して、現在のデバイスから送信されていないメッセージをサーバからロードできます。自分の電子メールアカウントから暗号化して送信した電子メールのリストを表示できます。
[Secure Compose] アイコン	安全なメッセージを作成するための画面を開きます。 暗号化した電子メールの送信 (1-14 ページ) を参照してください。
Android の [Menu] ボタン > [Settings]	BCE アプリケーションの設定画面を開きます。 Cisco Business Class Email の設定 (1-5 ページ) を参照してください。

Cisco Business Class Email の設定ファイルの起動

暗号化されたアカウントを作成するには、次に示すように、Cisco BCE アプリケーションのインストール後に管理者から受信したコンフィギュレーションファイルを適用する必要があります。暗号化されたアカウントの BCE アプリケーションを有効化し、設定するには、次の作業を行います。

- ステップ 1** Android デバイスに提供されているネイティブの電子メールアプリケーションを開きます。
- ステップ 2** Android デバイス上で電子メールの *securedoc.html* 添付ファイルを開きます。これにより、Android デバイスにインストールされている Cisco BCE アプリケーションが自動的に設定されます。



注 暗号化された電子メールが受信トレイにない場合は、スパム メールまたは迷惑メールのフォルダを調べます。

Cisco CRES 登録アカウントがない場合は、アカウントの登録を求めるプロンプトが表示されます。

- [New User Registration] フォームの所要事項を入力して [Register] をクリックします。受信トレイにアカウントのアクティベーション電子メールが届いていないか確認します。
- アカウントのアクティベーション電子メールで [Click here to activate this account] リンクをクリックします。アカウントのアクティベーションが確認され、登録した電子メール アドレスに暗号化されて送信された電子メールを表示できるようになったことを通知するメッセージが表示されます。
- HTML ファイルが添付された元の電子メールに戻ります。 *securedoc.html* 添付ファイルの [Open] をタップします。続いて [Cisco BCE] をタップします。

ステップ 3 プロンプトが表示されたら設定を確定し、この手順を完了します。

Cisco Business Class Email の設定

次の表に、Cisco BCE に設定できる 2 種類の設定を表示します。

- General Settings
- [Account Settings]

General Settings

一般設定を設定するには、[Settings]、[General Settings] の順にタップします。使用しているコンフィギュレーション モードによっては、設定で使用できないオプションがあります。[ライセンス バージョンおよびコンフィギュレーション モード \(1-2 ページ\)](#)を参照してください。

[General Settings] 画面で使用できる電子メールのセキュリティ オプションは次のとおりです。

一般設定のオプション	説明
Default Account	デフォルトの Cisco BCE 登録アカウントとして使用する電子メール アカウントのアドレスを指定します。
Diagnostic Log Level	ログ レベルを定義することにより、アプリケーションで維持するログのタイプを設定します。 ログ レベルの設定 (1-18 ページ) を参照してください。
Show Tutorial	チュートリアルを一般設定から起動できるかどうかを決定します。
About	アプリケーションのバージョン番号、サードパーティのライセンスおよび通知、使用状況データの詳細、利用規約、およびユーザ ガイドなどの BCE アプリケーションに関する情報を表示します。
Send Usage Data	BCE アプリケーションを改善するために匿名の使用状況データをシスコに送信するかどうかを決定します。
Reset Identifier	使用状況データを送信するのに使用する ID をリセットするかどうかを決定します。

アカウント設定

アカウント設定を設定するには、[Settings]、[account name] の順にタップします。使用しているコンフィギュレーション モードによっては、設定で使用できないオプションがあります。[ライセンス バージョンおよびコンフィギュレーション モード \(1-2 ページ\)](#) を参照してください。

[Account Settings] 画面で使用できる電子メール セキュリティのオプションは次のとおりです。

アカウント設定のオプションおよび処理	説明
ログイン	使用するアカウントの電子メール アドレスを設定します。
[サーバ]	電子メール アカウントの電子メール サーバ名を設定します。
Alias Name	使用するアカウントの代行名を設定します。
Remove Account	現在使用している電子メールアカウントを削除します。
Remember Password	暗号化されたパスワードをキャッシュする時間を設定します。キャッシュをクリアすると、次回ログイン時にパスワードを再入力する必要があります。
Clear Password	キャッシュのパスワードをただちにクリアするためにタップします。キャッシュはパスワード キャッシュ時間の期間が過ぎると自動的にクリアされます。
Default Expiration	デフォルトの有効期限を日単位で設定します。このオプションは、暗号化された電子メール メッセージを有効な状態で維持できる期間を指定します。メッセージ有効期限が切れると、受信者がそのメッセージを開くことはできません。 電子メールの有効期限の設定 (1-11 ページ) を参照してください。
Read Receipt	受信者が暗号化されたメッセージを開いたときにデフォルトの開封確認通知を送信者に要求するかどうかを決定します。デフォルトでは有効に設定されています。 送信した安全なメッセージの管理 (1-13 ページ) を参照してください。
Reply	メッセージ設定でも許可する場合、返信する暗号化されたメッセージを自動的に暗号化するかどうかを決定します。デフォルトでは有効に設定されています。 電子メールへの返信、全員への返信、および転送 (1-9 ページ) を参照してください。
Reply All	メッセージ設定でも許可する場合、受信者のすべてに返信するとき、暗号化されたメッセージを自動的に暗号化するかどうかを決定します。デフォルトで、このオプションは有効になっています。
Forward	メッセージ設定でも許可する場合、転送する暗号化されたメッセージを自動的に暗号化するかどうかを決定します。デフォルトで、このオプションは有効になっています。
Message Security	メッセージのセキュリティ レベルを Low、Medium、または High に設定するかどうかを決定します。デフォルトではメッセージのセキュリティ レベルは High に設定されています。 Message Security (1-16 ページ) を参照してください。
Cache Envelope Size	ダウンロードされた安全なエンベロープを初めて開いた後のキャッシュ サイズ (MB 単位) を定義します。デフォルト値は 6 MB です。

アカウント設定のオプションおよび処理	説明
Cache Envelope Duration	キャッシュがクリアされるまでの時間を指定します。ダウンロードした安全なエンベロープは、初めて開いた後、デバイス上でキャッシュされます。デフォルトは、30 日です。
Recipient Language	受信者に設定されているロケールに応じて、どの言語をメッセージ本文に使用するかをアプリケーションで決定できるようにします。暗号化されたメッセージを同じロケールを持つ受信者に送信する場合は、このオプションを使用します。受信者がさまざまなロケールを持つ場合、メッセージ本文には、通常次のオプションから選択するデフォルトの言語を使用します。 <ul style="list-style-type: none"> • サーバのデフォルト • 英語 • フランス語 • ドイツ語 • スペイン語 • ポルトガル語 • 日本語 • イタリア語
Diagnostic Subject	診断メールの件名行に使用されるテキストを定義します。
Send Diagnostic Message	トラブルシューティングの目的で送信される診断メールの受信者、件名、コンテンツを指定できます。アプリケーションで維持するログのタイプを、ログレベルで定義されているように設定するには、 ログレベルの設定(1-18 ページ) を参照してください。

コンフィギュレーション モードごとの使用可能な電子メール暗号化オプション

Cisco BCE アプリケーションでは、導入できるライセンスバージョンが 2 種類あり、そのバージョンにより、使用できる電子メール暗号化オプションとアプリケーションのコンフィギュレーション モードが決まります。それぞれのコンフィギュレーション モードの導入の詳細については、[ライセンスバージョンおよびコンフィギュレーション モード\(1-2 ページ\)](#)を参照してください。暗号化された電子メールを開くオプションは、両方のコンフィギュレーション モードで使用できます。

2 種類のコンフィギュレーション モードそれぞれの電子メール暗号化オプションについて、次の各項で説明します。

- [Decrypt と Encrypt モードの両方で使用できるオプション\(1-8 ページ\)](#)
 - [暗号化された電子メールを開く - 新しいメッセージ\(1-8 ページ\)](#)
 - [暗号化された電子メールを開く - すでに開いたことがあるメッセージ\(1-9 ページ\)](#)
 - [電子メールへの返信、全員への返信、および転送\(1-9 ページ\)](#)
 - [暗号化した電子メールのロックまたはロック解除\(1-10 ページ\)](#)

■ コンフィギュレーション モードごとの使用可能な電子メール暗号化オプション

- 電子メールの有効期限の設定 (1-11 ページ)
- 送信した安全なメッセージの管理 (1-13 ページ)
- 暗号化モードのみで利用できるオプション (1-14 ページ)
 - 暗号化した電子メールの送信 (1-14 ページ)
 - 開封確認の要求 (1-15 ページ)
 - メッセージ設定 (1-15 ページ)



注

Cisco BCE は Android デバイスで利用できる多数のメール アプリケーションすべてをサポートします。

Decrypt と Encrypt モードの両方で使用できるオプション

Cisco BCE アプリケーションのデフォルトのコンフィギュレーション モードは **Decrypt Only** です。Decrypt Only モードでは、暗号化されたメッセージを受信して開くことはできますが、暗号化したメッセージを送信することはできません。

統合された Decrypt and Encrypt モードでは、安全な電子メール メッセージの暗号化と復号化が可能です。

いずれかのモードを有効にする方法の詳細については、[ライセンス バージョンおよびコンフィギュレーション モード \(1-2 ページ\)](#) を参照してください。

暗号化された電子メールを開く - 新しいメッセージ

Cisco BCE アプリケーションでは、暗号化された電子メール メッセージを Android 電子メール クライアントで直接開くことができます。

- Cisco BCE は、メッセージが暗号化されていることを検出し、そのメッセージを復号化するために、Cisco BCE 登録アカウントのクレデンシャルの入力を要求します。
- 正しいユーザ名とパスワードを入力すると、Cisco BCE によってエンベロープがダウンロードされ、暗号化されたメッセージが Android デバイス上に表示されます。

暗号化された新しいメッセージを開くには、次の作業を実行します。

-
- ステップ 1** Android デバイス上で電子メール クライアントを起動します。
- ステップ 2** 暗号化された電子メールを電子メール リストのビューでタップして開きます。



注

暗号化された電子メールが受信トレイにない場合は、スパム メールまたは迷惑メールのフォルダを調べます。

- ステップ 3** 電子メールで HTML 添付ファイルを参照します。*securedoc.html* 添付ファイルの [Open] をタップします。続いて [Cisco BCE] をタップします。
- Cisco CRES 登録アカウントがない場合は、アカウントの登録を求めるプロンプトが表示されます。
 - [New User Registration] フォームの所要事項を入力して [Register] をクリックします。受信トレイにアカウントのアクティベーション電子メールが届いていないか確認します。

- アカウントのアクティベーション電子メールで [Click here to activate this account] リンクをクリックします。アカウントのアクティベーションが確認され、登録した電子メールアドレスに暗号化されて送信された電子メールを表示できるようになったことを通知するメッセージが表示されます。
- HTML ファイルが添付された元の電子メールに戻ります。*Securedoc.html* 添付ファイルを押し続けます。続いて [Cisco BCE] をタップします。
- 複数の電子メール アドレスが存在する場合は、次の作業を実行します。
 - ドロップダウン リストで該当の電子メール アドレスを選択し、Cisco BCE 登録アカウントのパスワードを入力して、[Submit] をタップします。

安全な電子メールが復号化され、そのメッセージが表示されます。



注

Android デバイスにダウンロードできる添付ファイルのデフォルトの最大サイズは、使用するメール サーバとデバイスのハードウェアに応じて異なります。

暗号化された電子メールを開く - すでに開いたことがあるメッセージ

メッセージを開くと、その電子メールは Cisco BCE アプリケーションの受信トレイに追加されるので、Cisco BCE の受信トレイから再び開くことができます。

暗号化されたメッセージを再び開くには、次の作業を実行します。

- ステップ 1** [account name]、[Inbox] の順にタップして、受信箱の電子メール アカウント画面を開きます。選択したアカウントの暗号化された電子メールのリストが表示されます。
- ステップ 2** 電子メールのリストで、暗号化された電子メールをタップして開きます。パスワードがキャッシュされない場合、Cisco BCE 登録アカウントのパスワードを入力し、[Submit] をタップします。復号化したメッセージが表示されます。

電子メールへの返信、全員への返信、および転送

返信または転送の対象となる暗号化された電子メールは、デフォルトで自動的に暗号化されません。セキュア メッセージの設定は次のゼロまたはそれ以上を実行できるかどうかを決定します。

- 安全な返信
- 全員への安全な返信
- 安全な転送

暗号化された電子メールに対して [Settings] 画面で定義された権限に基づき、該当のメニュー オプションが Android デバイスに追加されます。たとえば、暗号化された電子メールに転送のみを許可する権限が設定されている場合は、[Forward] メニュー オプションのみが使用できるようになります。[Cisco Business Class Email の設定 \(1-5 ページ\)](#) を参照してください。

■ コンフィギュレーション モードごとの使用可能な電子メール暗号化オプション

暗号化された電子メールへの返信またはその転送をするには、次の作業を実行します。

-
- ステップ 1** 暗号化された電子メールを開く - 新しいメッセージ(1-8 ページ) または暗号化された電子メールを開く - すでに開いたことがあるメッセージ(1-9 ページ)の手順を実行します。
- ステップ 2** 安全な返信、全員への安全な返信、または安全な転送を実行できるかどうかを確認するには、Android の [Menu] ボタン、[Message Settings] の順にタップして、このメッセージの設定を表示します。
- 新しいメッセージを作成する画面に、元のメッセージが追加されます。応答を追加し、元のメッセージの内容を編集します。
- ステップ 3** メッセージの作成を完了したところで [Send Secure] をタップします。メニューのオプションから、サードパーティの電子メール システムを選択して作業を完了します。たとえば [Android email] を選択します。
- ステップ 4** [Send] をタップします。メッセージが暗号化され、送信する電子メールに HTML ファイルとして添付されて送信されます。
-

暗号化した電子メールのロックまたはロック解除

暗号化した電子メールを送信した後、その電子メールをロックして受信者が電子メールを開くことができないようにすることが可能です。誤った受信者に電子メールを送信した場合や電子メールの送信後に情報の更新が発生した場合などに、このオプションを使用できます。



注

これらの機能をサポートしていないキー サーバでは、[Lock/Unlock Email Messages] メニュー オプションと [Edit Lock Reason] メニュー オプションは使用できません。

暗号化した電子メールをロックするには、次の作業を実行します。

-
- ステップ 1** [account name]、[Manage Messages] の順にタップします。
- 選択したアカウントから送信した、暗号化された電子メール メッセージのリストを表示するには、プルダウン ジェスチャーを実行します。
- ステップ 2** ロックする電子メール リストの暗号化された電子メール メッセージを確認します。
- これによりロックおよび期限切れアイコンが有効化されます。
- ステップ 3** 鍵マークのアイコンをタップします。
- ステップ 4** 必要に応じて、メッセージをロックする理由を入力します。受信者がエンベロープを表示すると、このロックした理由が示されます。
- ステップ 5** [Lock] をタップします。指定の電子メール メッセージを正常にロックしたことが確認されます。ロックした電子メールには、錠が付いたエンベロープのアイコンが表示されます。



注

電子メールをロックした後は、ロックした電子メールを確認し、鍵マークのアイコンをタップし、ロックの原因を編集して、[Update] をタップすることでロックの原因の編集を完了できます。

暗号化した電子メールのロックを解除するには、次の作業を実行します。

-
- ステップ 1** [account name]、[Manage Messages] の順にタップします。
- 選択したアカウントから送信した、暗号化された電子メール メッセージのリストを表示するには、プルダウン ジェスチャーを実行します。
- ステップ 2** ロック解除する電子メール リストの暗号化された電子メール メッセージを確認します。
- これによりロックおよび期限切れアイコンが有効化されます。
- ステップ 3** 鍵マークのアイコンをタップします。
- ステップ 4** 受信者をタップします。
- ステップ 5** [Unlock] をタップします。
-

電子メールの有効期限の設定

暗号化した電子メールに有効期限を設定できます。暗号化した電子メールが有効性を維持できる期間の指定が可能です。この期限が経過するとメッセージは期限切れとなり、受信者がそのメッセージを開くことはできなくなります。有効期限を設定する際に、次の各オプションを使用できます。

- すべての安全な電子メールにデフォルトの有効期限を設定できます。
- 特定の電子メールに、デフォルトの有効期限とは異なる有効期限を設定できます。
- 電子メールの送信後に有効期限を変更できます。

デフォルト設定

デフォルトの有効期限を設定するには、次の作業を実行します。

-
- ステップ 1** スマートフォンで、[Settings]、[account name] をタップします。または、タブレットで、[account name]、[account name] をタップします。
- ステップ 2** [Default Expiration] をタップし、電子メールが期限切れになるまでの日数を指定します。
- ステップ 3** 終了して変更を保存するには [Done] をタップします。
-

メッセージごとの設定

特定の電子メールに有効期限を設定するには、次の作業を実行します。

-
- ステップ 1** [Secure Compose] アイコンをタップして、[Secure Compose] 画面を開きます。
- ステップ 2** 次の各フィールドに適切に入力します。
- Address (To、CC、および BCC)
 - Subject
- ステップ 3** メッセージのテキストを入力します。
- ステップ 4** Android の [Menu] ボタンをタップしてから、[Message Settings] をタップします。
- ステップ 5** [Expiration] をタップします。[New Expiry Date] 画面が表示されます。

■ コンフィギュレーション モードごとの使用可能な電子メール暗号化オプション

- ステップ 6 [Set Expiration] スイッチをオンに設定します。
- ステップ 7 電子メールが期限切れになる日時を選択します。
- ステップ 8 [Done] をタップして変更を保存します。
- ステップ 9 [back] ボタンをタップして [Message Settings] 画面を終了し、安全な電子メールに戻ります。
- ステップ 10 メッセージの作成を完了したところで [Send Secure] をタップします。メニューのオプションから、サードパーティの電子メールシステムを選択して作業を完了します。たとえば [Android email] を選択します。
- ステップ 11 [Send] をタップします。メッセージが暗号化され、送信する電子メールに HTML ファイルとして添付されて送信されます。

メッセージ送信後の操作

電子メールを送信した後で、それに有効期限を設定するには、次の作業を実行します。

- ステップ 1 [account name]、[Manage Messages] の順にタップします。
選択したアカウントから送信した、暗号化された電子メール メッセージのリストを表示するには、プルダウン ジェスチャーを実行します。
- ステップ 2 有効期限を設定する電子メール リストの暗号化された電子メール メッセージを確認します。
これによりロックおよび期限切れアイコンが有効化されます。
- ステップ 3 Android の [Menu] ボタンをタップしてから、[Message Settings] をタップします。
- ステップ 4 [Expiration] をタップします。[New Expiry Date] 画面が表示されます。すでにメッセージに有効期限が設定されている場合は、現在の有効期限が表示されます。
- ステップ 5 電子メールが期限切れになる日時を選択します。
- ステップ 6 [Set] をタップして、変更を保存します。メッセージが有効期限切れになる日時を確定したことを示す通知が表示されます。

有効期限のクリア

電子メールを送信した後で、その有効期限をクリアするには、次の作業を実行します。

- ステップ 1 [account name]、[Manage Messages] の順にタップします。
選択したアカウントから送信した、暗号化された電子メール メッセージのリストを表示するには、プルダウン ジェスチャーを実行します。
- ステップ 2 有効期限をクリアする電子メール リストの暗号化された電子メール メッセージを確認します。
これによりロックおよび期限切れアイコンが有効化されます。
- ステップ 3 Android の [Menu] ボタンをタップしてから、[Message Settings] をタップします。
- ステップ 4 [Expiration] をタップします。[New Expiry Date] 画面が開き、現在の有効期限が表示されます。
- ステップ 5 [Set Expiration] スイッチをオンに設定します。
- ステップ 6 [Done] をタップして変更を保存します。

送信した安全なメッセージの管理

Android デバイスから送信済みの暗号化された電子メールのリストを表示するには、[account name]、[Manage Messages] の順にタップします。送信済みの暗号化された電子メールのリストから表示する電子メール メッセージを確認します。選択したメッセージをタップして、次の情報を表示します。

- [Subject]: メッセージの件名。
- [Date]: メッセージが送信された日付。
- [To]: 受信者の電子メール アドレス。
- [From]: 送信者の電子メール アドレス。

プルダウン ジェスチャーを作成して、サーバからすべてのメッセージと受信者を更新できます。

[Manage Messages] 画面を使用して、自分のデバイスおよび他のデバイスの両方から送信されたメッセージを確認し、管理できます。デバイスから送信されたメッセージは [Sent from this device] アイコンでマークされます。[Manage Messages] 画面では、メッセージを削除、ロック、または期限切れにしたり、詳細を表示したりすることもできます。

[Filter] ボタンをタップして、デバイスから送信されたそれらのメッセージだけを表示できます。フィルタを削除するには、[Android menu Remove Filter] 項目を選択します。すべてのフィルタ処理されたメッセージが送信された日付でソートされます。

デバイスから送信されたメッセージを削除すると、メッセージは「Sent from this device」としてマークされなくなります。ただし、送信したメッセージを削除しても、いくつかのメッセージ情報は表示されたままです(件名、受信者、および送信された日付など)。メッセージが削除されると、別のデバイスから送信されたかのように、つまり Web インターフェイスを使用して開かれず、削除済みメッセージのメッセージの詳細をロックしたり、期限切れにしたり、参照することができますが、メッセージ本文と添付ファイルは表示できません。

送信済みの暗号化された電子メールで次のアクションを実行できます。

- [Lock]: 暗号化した電子メールを送信した後、その電子メールをロックして受信者が電子メールを開くことができないようにすることが可能です。電子メールをロックすると、この画面から [Edit Lock Reason] オプションと [Unlock] オプションを使用できます。[暗号化した電子メールのロックまたはロック解除\(1-10 ページ\)](#)を参照してください。
- [Set Expiration]: 暗号化した電子メールに有効期限を設定できます。[電子メールの有効期限の設定\(1-11 ページ\)](#)を参照してください。

次の情報を設定するには、[Lock] または [Expire] アイコンをタップします。

- [Open Date]: 暗号化されたメッセージを該当の受信者が開いた日付。これは Android のタブレットにのみ表示されます。
- [Expiration Date]: 暗号化した電子メールの有効期限。
- [Locked Status]: 暗号化した電子メールがロックされている場合は、錠のアイコンが表示されます。ロックされていない場合は、ロック解除のアイコンが表示されます。
- [Locked Reason]: 暗号化した電子メールをロックしたときに入力したコメントが表示されます。

暗号化モードのみで使用できるオプション

統合された Decrypt and Encrypt モードでは、安全な電子メール メッセージの暗号化と復号化が可能です。

このモードを有効にする方法の詳細については、[ライセンス バージョン および コンフィギュレーション モード \(1-2 ページ\)](#) を参照してください。

暗号化した電子メールの送信

暗号化したメッセージを送信すると、そのメッセージはすべての受信者に対して暗号化されます。暗号化した電子メールを送信するには、次の作業を実行します。

ステップ 1 [Secure Compose] アイコンをタップして、[Secure Compose] 画面を開きます。[Secure Compose] アイコンは、「暗号化」タイプのエディションが BCE コンフィギュレーション ファイルに適用された場合のみ使用可能です。

ステップ 2 次の各フィールドに適切に入力します。

- Address (To、CC、および BCC)
- Subject

設定された電子メール アカウントが 1 つだけの場合、そのアカウントは新しいメッセージの [Encrypt with] フィールドに追加されます。設定された電子メール アカウントが複数ある場合、ドロップダウン リストからアカウントを選択できます。[Encrypt with] フィールドでデフォルトのアカウントとして使用するアカウントを設定するには、Android の [Menu] ボタン、[Settings]、[General Settings]、[Default Account] の順にタップします。

ステップ 3 メッセージのテキストを入力します。

ステップ 4 安全なメッセージを作成するとき、必要に応じ、送信するメッセージのメッセージ設定を [Envelope Settings] 画面で変更できます。メッセージ設定にアクセスするには、Android の [Menu] ボタンをタップします。続いて [Message Settings] をタップします。



注 Android デバイスで安全なメッセージを作成するとき、添付ファイルを追加できます。

ステップ 5 メッセージの作成を完了したところで [Send Secure] をタップします。メニューのオプションから、サードパーティの電子メール システムを選択して作業を完了します。たとえば [Android email] を選択します。

ステップ 6 [Send] をタップします。メッセージが暗号化され、送信する電子メールに HTML ファイルとして添付されて送信されます。

開封確認の要求

送信した電子メールを受信者が開いたときに、Android デバイス上でその受信者に対して開封確認の送信を直接要求できます。

デフォルト設定

開封確認を要求(デフォルト設定)するには、次の作業を実行します。

-
- ステップ 1** スマートフォンで、[Settings]、[account name] をタップします。または、タブレットで、[account name]、[account name] をタップします。
- ステップ 2** [Read Receipt] スイッチをオンに設定します。この設定はデフォルトでイネーブルになっています。
-

メッセージごとの設定

このオプションが該当するのは、デフォルト設定を有効にせず、個別の電子メール単位で開封確認を要求する場合です。

特定の電子メールの開封確認を要求するには、次の作業を実行します。

-
- ステップ 1** [Secure Compose] アイコンをタップして、[Secure Compose] 画面を開きます。
- ステップ 2** 次の各フィールドに適切に入力します。
- Address (To、CC、および BCC)
 - Subject
- ステップ 3** メッセージのテキストを入力します。
- ステップ 4** Android の [Menu] ボタンをタップしてから、[Message Settings] をタップします。
- ステップ 5** [Read Receipt] スイッチをオンに設定します。
- ステップ 6** [back] ボタンをタップして [Message Settings] 画面を終了し、安全な電子メールに戻ります。
-

メッセージ設定

安全な電子メールの作成では、作成中の電子メールのメッセージ設定を変更できます。

メッセージ設定を変更するには、次の作業を実行します。

-
- ステップ 1** [Secure Compose] アイコンをタップして、[Secure Compose] 画面を開きます。
- ステップ 2** 次の各フィールドに適切に入力します。
- Address (To、CC、および BCC)
 - Subject
- ステップ 3** メッセージのテキストを入力します。
- ステップ 4** [Message Settings] にアクセスするには、Android の [Menu] ボタンをタップし、[Message Settings] をタップします。

ステップ 5 次をタップして、該当のメッセージ オプションを有効または無効にします。

- Expiration
- Read Receipt
- Reply
- Reply All
- Forward
- Message Security

ステップ 6 変更が自動的に保存されます。

Message Security

送信済みの暗号化された電子メールのセキュリティ レベルを指定するには、Android デバイスの [Settings]、[account name] をタップします。または、タブレットの [account name]、[account name] をタップします。

設定できるメッセージのセキュリティ レベルは次のとおりです。

- [High]: メッセージに高度のセキュリティを指定すると、暗号化されたメッセージを復号化するたびに認証用のパスワードが要求されます。
- [Medium]: メッセージに中程度のセキュリティを指定すると、受信者のパスワードがキャッシュされていれば、暗号化されたメッセージを復号化するときにパスワードは要求されません。
- [Low]: メッセージに低いセキュリティを指定した場合、送信は安全に行われますが、暗号化されたメッセージを復号化するときにパスワードが要求されません。

すべてのメッセージにはデフォルトで [High] のセキュリティ レベルが設定されます。特定のメッセージについて [Message Settings] で値を変更することで、このデフォルトの設定を変更できます。[暗号化モードのみで使用できるオプション\(1-14 ページ\)](#)を参照してください。

キャッシュ管理

パスワードのキャッシュ

Cisco BCE 登録アカウントのパスワードは、[Settings]、[account name]、[Remember Password] の順にタップして、設定できる期間にキャッシュされます。デフォルトのキャッシュ時間は、1,440 分 (24 時間) です。パスワードのキャッシュは、デフォルトではオフですが、[Medium Security messages] 画面または [Manage Messages] 画面にある [Remember Password] スイッチを使用してオンにできます。

パスワードのキャッシュは、[Settings]、[account name]、[Clear Password] の順にタップしてクリアできます。暗号化アカウントの場合は、パスワード キャッシュ期間を設定することもできます。

安全なエンベロープのキャッシュ

ダウンロードした安全なエンベロープは、初めて開いた後、デバイス上でキャッシュされます。これにより、同じ安全なエンベロープを次回開くときに、そのエンベロープが再度ダウンロードされることがありません。

キャッシュ処理は時間とサイズの組み合わせに基づいて実行されます。キャッシュするエンベロープの最大サイズは管理者が設定します。デフォルトでは、キャッシュできるエンベロープのサイズは 6 MB までです。エンベロープは、エンベロープの有効なキャッシュ サイズ (MB) と期間 (時間) を超えていると、受信箱と管理メッセージフォルダを再び開いたときに、受信箱と管理メッセージフォルダから削除されます。

診断ツールを使用したトラブルシューティング

Cisco BCE アプリケーションには、問題のトラブルシューティングに効果的な診断ツールが付属しています。エラーを受け取った場合や Cisco BCE アプリケーションに問題が発生した場合は、この診断ツールを使用できます。

この診断ツールでは、収集したデータを電子メールに添付します。診断のための電子メールには、暗号化アプリケーションとの対話操作の際にデバイスについて生成されたデータが記述されます。

**注**

最大 2,000 行はログに保存できます。ログが 2,000 行を超えると、最も古いログが削除されます。

診断ツールの実行

**注**

診断のための電子メールには、受け取ったあらゆるエラーまたは Cisco BCE アプリケーションで発生したあらゆる問題の説明を記述することが重要です。トラブルシューティングおよび問題解決で、これらの情報が役に立ちます。

診断ツールを実行して診断のための電子メールを送信するには、次の作業を実行します。

- ステップ 1** スマートフォンで、[Settings]、[account name] をタップします。または、タブレットで、[account name]、[account name] をタップします。
- ステップ 2** 診断メールの件名行として表示されるテキストを入力し、[OK] をクリックします。
- ステップ 3** アクションを完了するには、電子メール システムをメッセージの送信に使用することを選択します。たとえば [Android email] を選択します。
診断出力が添付された [Email Compose] 画面が表示されます。この診断出力は、*device.txt*、*BCE.txt*、および *config.txt* の 3 つのファイルで構成されています。
- ステップ 4** 送信先アドレスを [To] に入力して、メッセージの内容を作成します。管理者による [Subject] フィールドと [To] フィールドの設定に応じて、これらのフィールドには事前に情報を入力済みとすることができます。これらを編集できるようにすることも可能です。
- ステップ 5** [Send] をタップします。

ログレベルの設定

[Advanced Settings] 画面でログレベルを定義することで、アプリケーションに保持するログの種類を設定できます。スマートフォンで、[Settings]、[General Settings] の順にタップします。または、タブレットで、[account name]、[General Settings] の順にタップします。[Diagnostic Log Level] をタップして、ログレベルを表示または設定します。使用しているコンフィギュレーションモードによっては、このオプションを設定に使用できないことがあります。

設定できるログレベルは次のとおりです。

- [Error]: Cisco BCE で生成されたエラーメッセージがログに記録されます。
- [Warning]: アプリケーションで生成された警告とエラーメッセージがログに記録されます。
- [Info]: アプリケーションで生成されたエラー、警告および情報メッセージをログに記録します。これは、アプリケーションフローを監視するのに使用できます。これがデフォルトのオプションです。
- [Debug]: アプリケーションで生成されたエラー、警告、情報、およびデバッグ情報がログに記録されます。

Cisco Business Class Email アプリケーションのアップグレード

Cisco BCE アプリケーションのアップグレードは Google Play から入手できます。Google Play を使用して元のアプリケーションをインストールしている場合は、更新されたバージョンが入手可能になると、自動的にそれが通知されます。

アップグレード後も、これまでの設定が保持されます。

Cisco Business Class Email アプリケーションのアンインストール

Android 上の Cisco BCE をアンインストールするには、次の作業を実行します。

-
- ステップ 1 Android ホーム画面に移動します。
 - ステップ 2 [Settings] をタップします。
 - ステップ 3 [Apps]、[Cisco BCE] の順にタップします。
 - ステップ 4 [Uninstall] をタップし、[OK] をタップします。
アプリケーションが削除されます。
-

カスタマーサポート

Cisco Business Class Email に関する助言を得るには、担当のシステム管理者に問い合わせてください。