Cisco Secure Email Encryption Plug-in 1.2.1 管理者ガイド

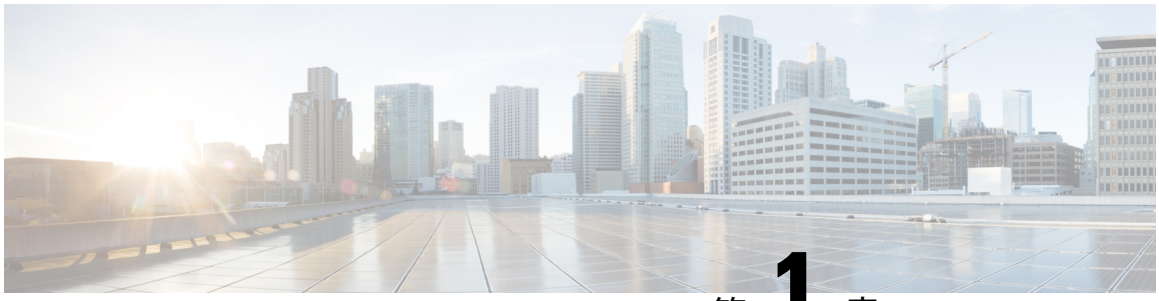
初版：2019 年 10 月 15 日

最終更新：2022 年 11 月 24 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

Cisco Secure Email Encryption Plug-in を使用する前に

この章は、次の項で構成されています。

サポートされている構成

リリース 1.2.1 でサポートされているオペレーティングシステムの詳細については、https://www.cisco.com/c/dam/en/us/td/docs/security/email_encryption/Compatibility_Matrix/Encryption_Compatibility_Matrix.pdfを参照してください。

セキュリティ設定の準拠のガイドライン

Cisco Secure Email Encryption Plug-in 1.2.1 がテストされ、以下の強化ガイドに記載されている設定および環境で作動することが確認されています。

- Microsoft Hardening Guides：https://www.microsoft.com/en-us/download/details.aspx?id=16776 で入手できる Microsoft Security Compliance Manager 3.0.60 を使用して設定されています。
- 次の場所にある 『NSA Security Configuration Guides』

  https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml#microsoft

関連資料

Encryption Plug-in を使用するには、Cisco Secure Email Gateway を実行し、Encryption Plug-in と連動するように正しく設定されているか、または Cisco Secure Email Encryption Service アカウントが必要です。Cisco Secure Email Gateway の設定方法については、次のガイドを参照してください。

- 『Cisco Secure Email Gateway Guide』。このマニュアルでは、電子メール暗号化のインストールおよび設定手順について説明しています。プラグインの設定と連動するように暗号化アプライアンスを設定する方法を理解する上で役立ちます。対象のリリースのガイドを検索するには、http://www.cisco.com/en/US/products/ps10154/prod_installation_guides_list.html を参照してください。

このマニュアルの使用方法

このガイドは、Cisco Secure Email Encryption Plug-in の機能について知るためのリソースとしてご利用ください。トピックは、論理的な順序で編成されていますが、必ずしもすべての章を読む必要はありません。目次を読んで、ご使用の設定に関連する章を確認してください。

このマニュアルは PDF 形式で電子的に配布されています。このマニュアルの電子版は、Cisco Customer Support Portal で入手できます。また、アプライアンスの GUI で HTML オンライン ヘルプ ツールにアクセスできます。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、または [File] > [Options] > [Add-in Options] > [Cisco Email Encryption] に移動します。
- Outlook 2007 では、ツールバーの [Plug-in Options] ボタンをクリックするか、または [Tools] > [Options] > [Cisco Email Security Encryption] > [Help] に移動します。

詳細情報の入手先

シスコは、Cisco Secure Email Encryption Plug-in についての理解を深めて頂くために次の資料を用意しています。

セキュリティ トレーニング サービスと認定

シスコ セキュリティ トレーニング サービスでは、シスコの製品とソリューションを使用するための比類のない指導とトレーニングを行っています。技術的なトレーニング コース用の的確なカリキュラムを通じて、このプログラムでは、さまざまな利用者向けの最新の知識とスキルが伝わります。

シスコ セキュリティ トレーニング サービスに連絡するには、次のいずれかの方法を使用してください。

トレーニング。登録、トレーニング全般、証明書、および認定試験に関するご質問の場合：

- https://www.cisco.com/c/en/us/products/security/email-security/index.html
- stbu-trg@cisco.com

シスコサポートコミュニティ

シスコサポートコミュニティは、シスコのお客様、パートナー、および従業員向けのオンラインフォーラムです。電子メールおよびWebセキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。このフォーラムにトピックを投稿して質問したり、他のシスコ ユーザと情報を共有したりできます。

シスコ サポート コミュニティには https://supportforums.cisco.com からアクセスできます。

シスコカスタマーサポート

（注） 利用可能なサポートのレベルは、お客様のサービスレベル契約によって異なります。シスコカスタマーサポートのサービスレベル契約の詳細については、サポートポータルをご覧ください。サポートレベルの詳細については、このページで確認してください。

サポートは、電話、電子メール、またはオンラインで依頼できます（24時間年中無休）。次のいずれかの方法でシスコカスタマーサポートにお問い合わせください。

- シスコサポートポータル：https://www.cisco.com/c/ja_jp/support/index.html
- 電話サポート：800-553-2447（米国/カナダ国内）または各国の電話番号から Cisco Technical Assistance Center（TAC）にお問い合わせください。
- 電子メール：tac@cisco.com

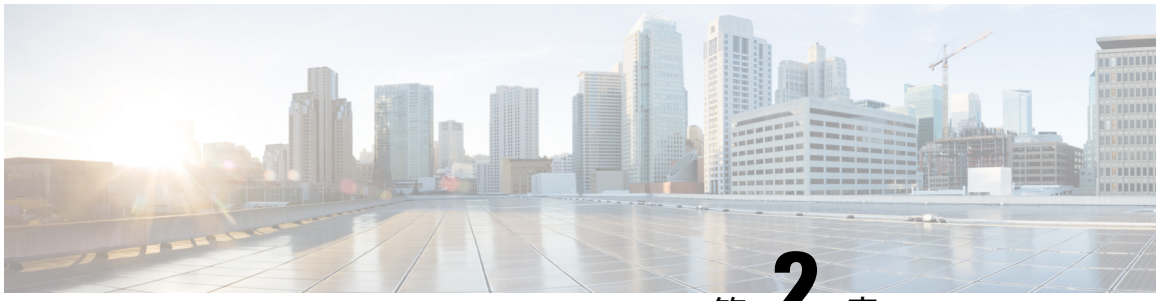
再販業者または別のサプライヤからサポートを購入した場合は、製品のサポートの問題について直接そのサプライヤに連絡してください。

Cisco Secure Email Encryption Plug-in の概要

Cisco Secure Email Encryption Plug-in をインストールすると（Microsoft Outlook からアクセス可能）、Microsoft Outlook メールクライアント上のコンポーネントが有効になります。この 1 つのインターフェイスで暗号化された電子メールを送信できます。暗号化プラグインはツールバーの [Encrypt Message] ボタンに配置され、ユーザーは暗号化された電子メールを電子メールプログラムから送信することも、組織外に送信する前に暗号化するように電子メールにフラグを設定することもできます。ユーザーは、暗号化した電子メールをロックまたはロック解除したり、ロックの理由を追加または変更することができます。また、暗号化された電子メールの失効日時を設定することもできます。

暗号化プラグインは便利なインターフェイスであり、ツールバーボタンを使用してコンテキストメニューを右クルックすることで暗号化されたメッセージを送信できます。

暗号化プラグインでは、Cisco Secure Email Gateway が存在し、正しく設定されているか、または Cisco Secure Email Encryption Service アカウントが必要です。



第 2 章

Cisco Secure Email Encryption Plug-in の展開

この章は、次の項で構成されています。

暗号化プラグイン

暗号化プラグインをインストールすると、電子メール メッセージのメニュー バーに [Encrypt Message] ボタンが表示されるので、送信者は、組織外部に送信する前に、暗号化して保護する必要があるメッセージを簡単にマークできます。

2 種類の暗号化（Flag 暗号化とデスクトップ暗号化）を使用できます。Flag 暗号化オプションを使用すると、暗号化に必要なフラグを設定できます。また、Cisco Secure Email Gateway によって電子メールが暗号化されてから電子メールがネットワークの外部に送信されます。デスクトップ暗号化では、シスコの暗号化テクノロジーを使用して電子メールプログラム内から電子メールを暗号化できます。その後、暗号化された電子メールが電子メールプログラムによりデスクトップから送信されます。デスクトップ暗号化は、組織内で送信するメールを暗号化する場合に使用できます。

暗号化プラグインは、機能している設定済みの Cisco Secure Email Gateway（ネットワーク内に存在している場合）と連動するように設計されています。暗号化プラグインに使用するコンフィギュレーションは、これらのアプライアンスの設定に合わせて設定する必要があります。これらのアプライアンスに同じ設定を使用しないと、暗号化メッセージを送信するときに問題が生じる可能性があります。

（注） 暗号化プラグインでは、Cisco Secure Email Gateway が存在し、正しく設定されているか、または Cisco Secure Email Encryption Service アカウントが必要です。

Cisco Secure Email Encryption Plug-in のインストール

ユーザーグループ向けに Cisco Secure Email Encryption Plug-in をインストールする場合、サイレントインストールを実行できます。サイレント インストールでは、エンド ユーザーに入力を求めることなくインストールを実行できます。サイレントインストールの詳細については、一括インストールの実行 （11 ページ）を参照してください。

（注） Cisco Secure Email Encryption Plug-in 7.x と Cisco Secure Email Encryption Plug-in 1.2 を一緒にインストールしないでください。レポート機能が必要な場合は、Cisco Secure Email Encryption Plug-in 1.x と Cisco Secure Email Reporting Plug-in 1.x の両方をインストールします。

コンフィギュレーション モード

Cisco Secure Email Encryption Plug-in は、3 種類のコンフィギュレーション モードで展開されます。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。

他のコンフィギュレーションモードを有効にするには、更新済みの添付ファイルを管理者から受け取り、それを使用して Outlook 電子メール アカウントを設定します。管理者は、エンド ユーザーの電子メール アカウントに BCE Config 添付ファイル（デフォルト名は *BCE_Config_signed.xml*）を送信します。エンド ユーザーはこのファイルを *securedoc.html* ファイルとして受信します。エンド ユーザーが *securedoc.html* 添付ファイルをクリックすると、メッセージに添付されている設定情報が Outlook アプリケーションによって検出され、更新済みの設定が適用されます。

（注） デフォルトのセキュアメッセージ名は *securedoc.html* です。添付ファイル名の値は管理者が変更でき、指定された新しい名前がメッセージに反映されます。

3 つの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できます。
- **Decrypt and Flag**：安全な電子メール メッセージの復号化とフラグ設定を行うことができます。flag オプションを使用すると、エンドユーザーは暗号化に必要なフラグを設定できます。また、Cisco Secure Email Gateway によって電子メールが暗号化されてから電子メー

ルがネットワークの外部に送信されます。フラグが設定されたメッセージを検出してサーバーで復号化できるようサーバーの設定を行う必要があります。

- **Decrypt and Encrypt**：安全な電子メール メッセージの暗号化と復号化を行うことができます。

次の表は、各コンフィギュレーション モードでサポートされる機能を示しています。

機能	Decrypt Only	Decrypt and Flag	Decrypt and Encrypt
暗号化したメッセージを送信			X
メッセージに暗号化フラグを設定		X	
暗号化された電子メールを開封	X	X	X
返信/すべてに返信/転送	X	X	X
電子メールのロックおよびロック解除	X	X	X
電子メールの有効期限	X	X	X
電子メールの診断	X	X	X
開封確認			X
セキュアメッセージの設定			X
設定	X	X	X

暗号化サービスキーサーバーを使用した Cisco Secure Email Encryption Plug-in の展開

Cisco Secure Email Encryption Service のキーサーバーで直接使用できるように、次の手順を実行して Cisco Secure Email Encryption Plug を展開します。

手順

ステップ 1 Encryption Service アカウント https://res.cisco.com/admin にログインし、[Accounts] タブに移動します。

ステップ 2 Encryption Plug-in を有効にするアカウントを選択します。次に、[BCE Config] タブに移動します。

ステップ 3 設定テンプレートで使用するトークンを選択します。

- [CRES]：キー サーバーが Encryption Service の場合に選択します。

ステップ 4 [Download Template] をクリックして、編集するテンプレート ファイルをダウンロードします。ファイル名は *BCE_Config.xml* です。

ステップ 5 コンフィギュレーション ファイルを編集します。

BCE_Config.xml ファイルには、特定の環境に合わせて編集する必要があるフィールドの詳細が含まれています。テキストエディタでファイルを開き、コメントに記載されている手順に従って必要な変更を行います。

（注） ローカリゼーションが目的の場合は、既存のメッセージセキュリティ ラベル（Low、Medium、High）を変更しないでください。

ステップ 6 [Browse] をクリックして、編集した *BCE_Config.xml* ファイルを探し、ファイルが見つかったら [Upload and Sign] をクリックします。

コンフィギュレーション ファイルに署名すると、その署名したバージョンが *BCE_Config_signed.xml* としてダウンロードされます。このファイルをローカル マシンに保存します。

ステップ 7 同時に多数のエンド ユーザーにコンフィギュレーション ファイルを展開するには、[Distribute Signed Configuration to Bulk List] オプションを使用します。次の手順を実行します。

1. ステップ 6 で作成した BCE 構成ファイルを参照します。
2. エンド ユーザーの電子メール アドレスが含まれているカンマ区切り形式のファイルの場所を参照します。
3. 必要に応じて電子メールの件名を変更します。
4. [Distribute Config] をクリックします。署名付き BCE Config を使用して一括インストールを実行するには、「BCE_Config.xml ファイルによる一括インストール （32 ページ） BCE_Config.xml ファイルを使用した一括インストール」の項を参照してください。

（注） XML 構成ファイルを別のエンド ユーザーに転送した場合は、管理者から受け取った場合とは異なり、自動設定が機能せず、エラーが表示されます。Cisco Secure Email Gateway または暗号化サービスによって暗号化された電子メールを介して、すべてのエンドユーザーに署名済み設定ファイルを送信することもできます。暗号化サービスアカウントで管理者としてリストされているメッセージ電子メールアドレスを送信する必要があります。

（注） メーリング リスト宛てに、署名された BCE Config ファイルを送らないでください。暗号化サービスはメーリングリストをサポートしていません。

Cisco Secure Email Encryption Plug-in の設定

Cisco Secure Email Encryption Plug-in をインストールすると、Outlook の [Cisco Secure Email Encryption] タブから設定を変更できるようになります。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options]ボタンをクリックするか、または [File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Encryption] に移動します。
- Outlook 2007 では、ツールバーの [Plug-in Options] > ボタンをクリックするか、または [Tools] > [Options] > [Cisco Email Encryption] に移動します。

Encryption Plug-in のインストールは変更が可能です。または、両方のプラグインのインストールに影響する汎用オプションを変更できます。たとえば、Cisco Secure Email Encryption Plug-in のロギングを有効または無効にしたり、特定の暗号化モードのオプションを変更できます。

暗号化する電子メールのマーキング方法を変更するには、*BCE_Config.xml* ファイルを変更して、自動設定を実行する必要があります。設定を指定する場合、それらの設定にはCisco Secure Email Gateway との互換性が必要です。

Outlook の設定を変更する場合は、Cisco Secure Email Encryption Plug-in for Outlook の設定と使用 （35 ページ）を参照してください。

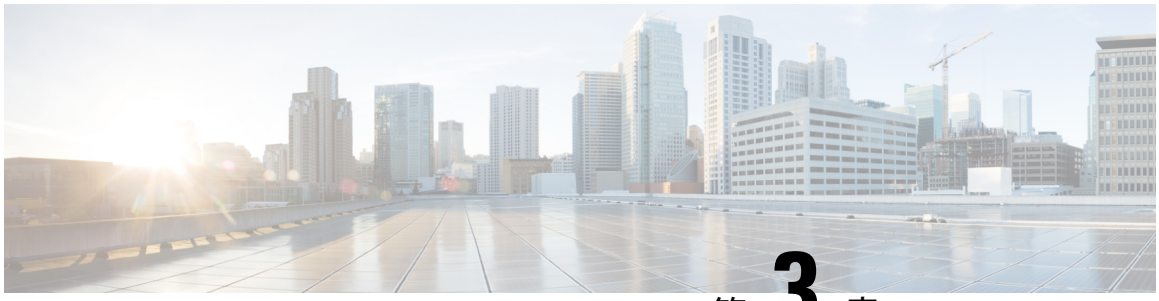
Cisco Secure Email Encryption Plug-in に必要なシステムプロセス

Cisco Secure Email Encryption Plug-in で必要なものは、TCP/IP DNS や DHCP などの必須のシステムプロセスのみで、これらのものは無効にすることはできません。ただし、データベースマネージャ、HTTP サーバー、ハードウェア設定デーモンなどの必須ではないシステムプロセスは、Cisco Email Encryption Plug-in の機能に影響を与えずに無効にすることができます。

Cisco Secure Email EncryptionPlug-in に必要な TCP サービス

ネットワークで次のTCPサービスとファイアウォールポートを開いていることを確認します。

デフォルト ポート	プロトコル	ホストネーム	目的
53	DNS	res.cisco.com	Encryption Service キーサーバーの URL を解決するには、DNSが必要です。 すべてのエンドユーザーがこのサービスにアクセスできる必要があります。
443	HTTPS	-	モードが暗号化、フラグ、および復号（デフォルト）の Encryption Service サーバーにアクセスするには、HTTPSが必要です。
		res.cisco.com	認証
		verify.res.cisco.com	BCE構成ファイルの署名（初回の場合）。
		updates.res.cisco.com	プラグインの更新の場合。



第 3 章

一括インストールの実行

この章では、複数のデスクトップに一括インストールする方法について説明します。ここで説明する内容は次のとおりです。

インストールの前提条件

Cisco Secure Email Encryption Plug-in アプリケーションをインストールする前に、次の要件が満たされていることを確認します。

- Java Runtime Environment 1.8 または Open Java Runtime Environment 11
- Microsoft .NET Framework 4.5.1
- Microsoft Office Primary Interop Assemblies

これらの項目がインストールされていない場合は、前提条件のリストに含まれるすべてのソフトウェアをインストールすることを求めるプロンプトがプラグインのインストーラに表示されます。

Java のインストールまたは更新に関する特記事項

Java（Oracle または Open JRE）は手動で更新しないことをお勧めします。Java を手動で更新する必要がある場合は、Open JRE を Eclipse Adoptium にアップグレードする際に、次の点に十分注意してください。

- インストール時に、**Set JAVA_HOME** 変数と **JavaSoft レジストリキー**に対して [機能全体がローカルハードディスクにインストールされます（Entire feature will be installed on local hard drive）] を選択します。

  コマンドラインを使用して Open JRE を更新する場合は、次のコマンドを使用します。

  ```
  msiexec /i OpenJDK11U-jre_x64_windows_hotspot_11.0.14_9.msi INSTALLLEVEL=3 /quiet
  ```

Eclipse Temurin JRE をすでにインストールしている場合は、いったんアンインストールしてから、Eclipse Temurin JRE がバンドルされている Cisco Secure Email Encryption Plugin 1.2.1-192 をインストールする必要があります。

Cisco Secure Email Encryption Plug-in の一括インストールツール

Cisco Secure Email Encryption Plug-in の一括インストールでは、組織内のユーザーが使用できるよう Cisco Secure Email Encryption Plug-in の配布パッケージを作成できます。

配布パッケージを保存するサーバーは、サーバー接続の手順でローカルマシンかリモートマシンかを選択できます。

また、一般オプションとアカウントオプションを編集してデフォルト設定を変更できます。インストールのさまざまな側面を変更するさまざまなコンフィギュレーションファイルを使用することもできます。たとえば、さまざまなパラメータ値をカスタマイズして、デフォルトのオプションを部分的に変更できます。また、特定のドメインのユーザのみを対象に構成を事前設定し、ユーザインターフェイスをローカライズしたり、ボタンの名前をカスタマイズしたりできます。

カスタマイズして準備の整った CommonComponentsConfig.xml や config_{n}.xml ファイルをアップロードできます。

最後のステップでは、一括インストールの実行に必要なすべてのファイルが格納されている共有フォルダのパスと、カスタマイズされたスクリプトを取得します。このスクリプトは、コピーして SCCM 管理ツールで再利用します。

一括インストールによって変更されるオプション

Cisco Secure Email Encryption Plug-in の一括インストールでは、インストールプロセスで使用される次のオプションが変更されます。

- 言語、ロギング、シスコへのデータ送信、更新チェックなどの一般的なオプション。
- アカウント オプション（指定ドメインのユーザー用に事前定義された構成）。

一括インストール ツールの実行

[Start] メニューまたは [Program Files] フォルダのいずれかから Cisco Secure Email Reporting Plug-In 一括インストールを実行します。

[Start] メニューから実行する場合：

- [Start] メニューボタンをクリックし、[Cisco Email Encryption Plug-in] > [Cisco Email Encryption Plug-in Mass Installation] に移動します。

または

[Program Files] フォルダから実行する場合：

- Cisco Secure Email Encryption Plug-in がインストールされているフォルダ（通常は **C:\Program Files (x86)\Cisco\Cisco Email Encryption Plug-in**）に移動し、*Cisco.EmailSecurity.MassInstall.exe* ファイルをダブルクリックします。

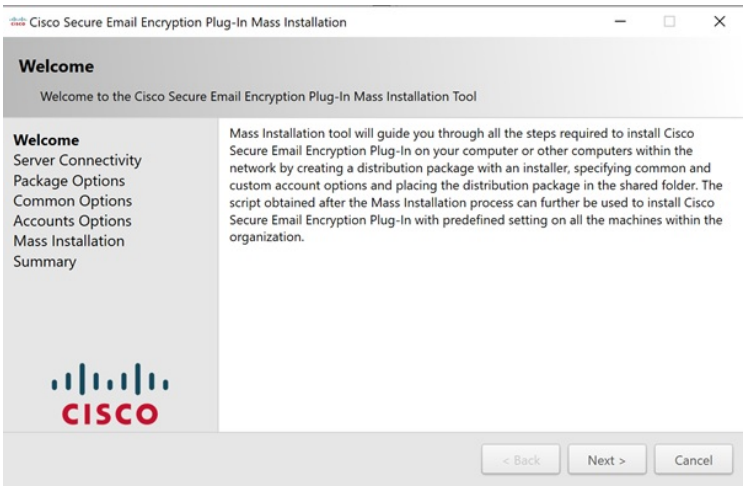
一括インストール パッケージとスクリプトの準備

手順は次のとおりです。

手順

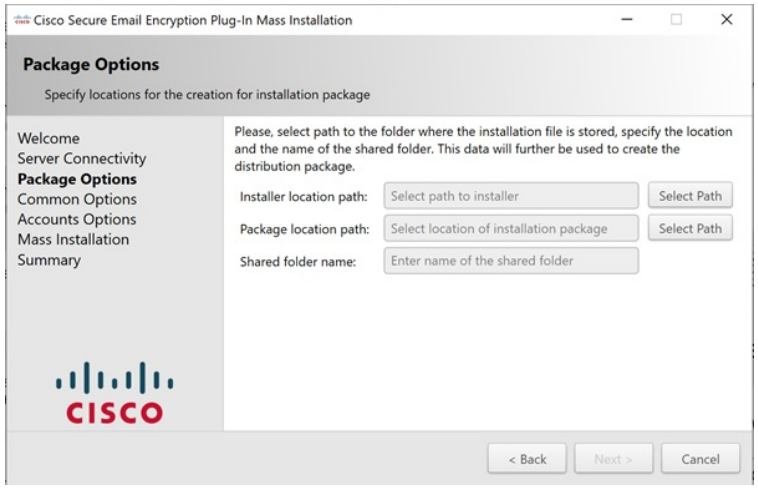
ステップ 1 一括インストールツールを実行します。

ステップ 2 [ようこそ（Welcome）] ウィンドウで、[次へ（Next）] をクリックします。

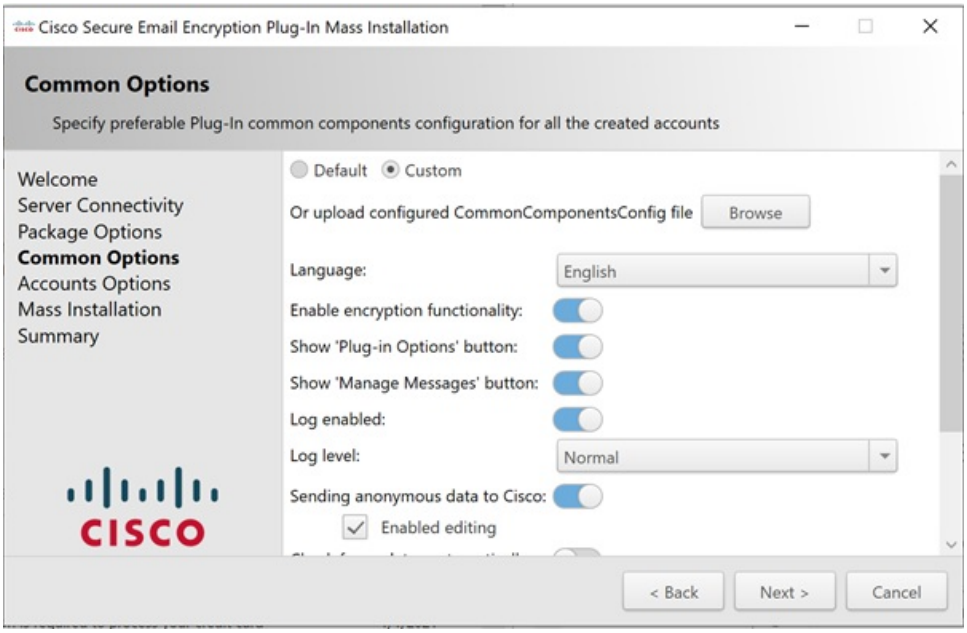


ステップ 3 [サーバー接続（Server Connectivity）] ウィンドウで、使用する接続を選択します。ローカルマシンまたはリモート マシンを使用できます。リモートマシンを選択した場合は、[マシン名またはIPアドレス、ユーザ名（Machine name or IP address, Username）] フィールドと[パスワード（Password）] フィールドに入力して [次へ（Next）] をクリックします。

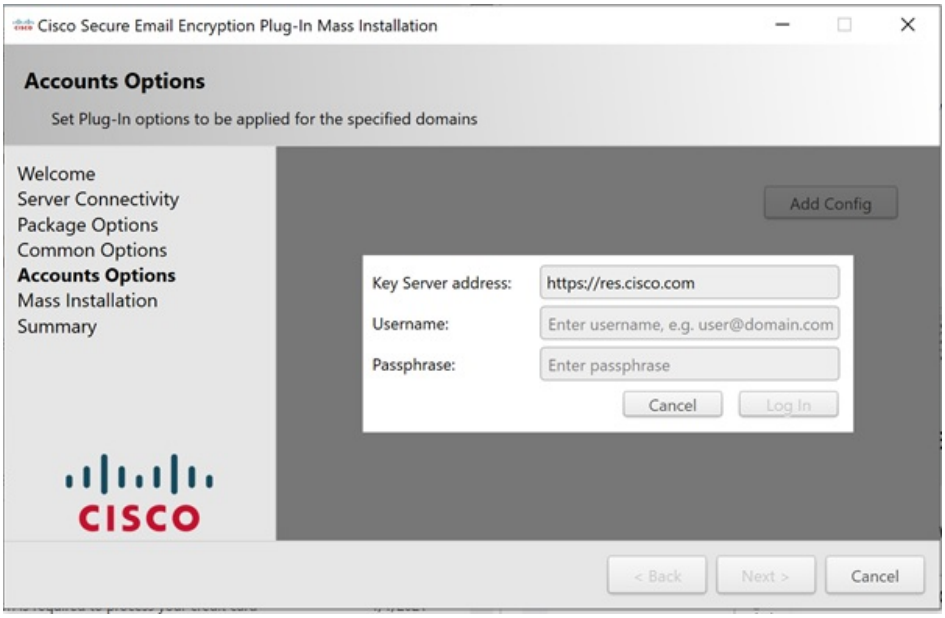
ステップ 4 [パッケージオプション（Package Options）] ウィンドウでインストールパッケージの作成先を指定して [次へ（Next）] をクリックします。

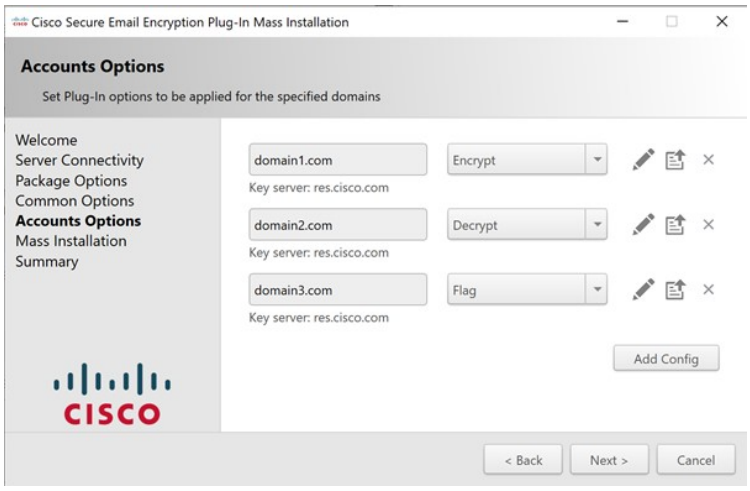


ステップ 5 [基本オプション（Common Options）] ウィンドウで、設定するプラグイン共通コンポーネントの構成を作成済みのすべてのアカウントに指定し、[次へ（Next）] をクリックします。

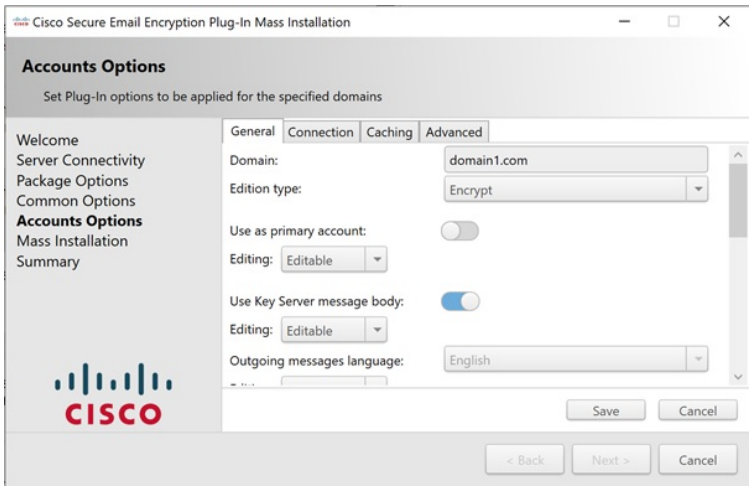


ステップ 6 [アカウントオプション（Account Options）] ウィンドウで、キーサーバーに管理者クレデンシャルを使用してログインし、有効な構成ファイルを受信して署名する必要があります。次に、指定したドメインに適用するプラグインオプションを設定して [次へ（Next）] をクリックします。

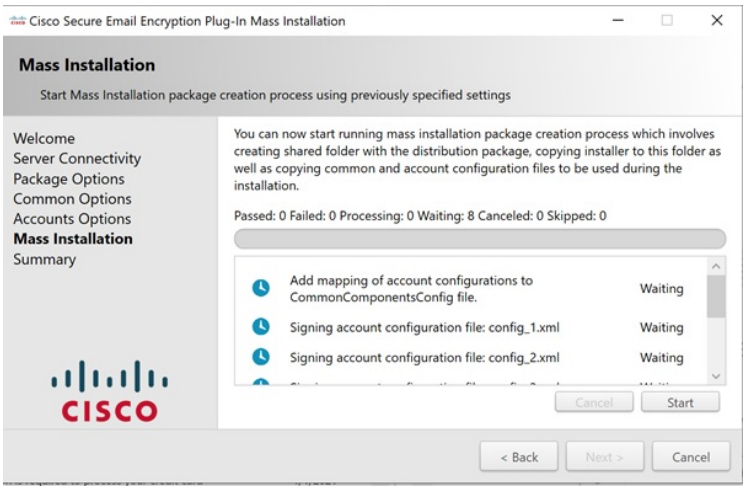




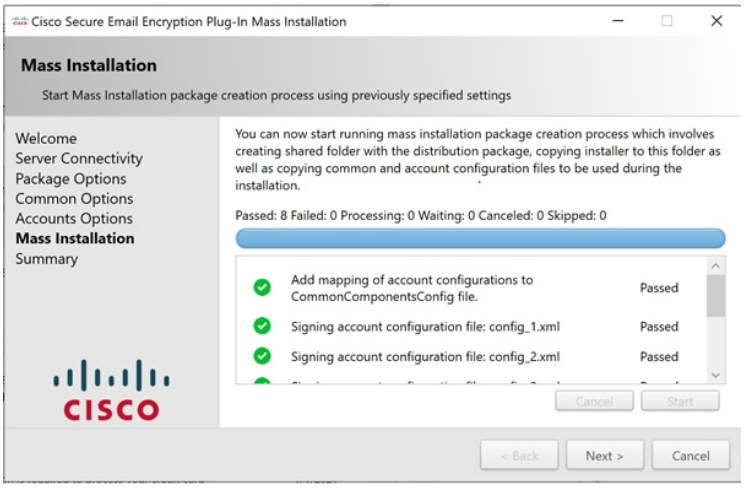
ステップ 7 [アカウントオプション（Account Options）] ウィンドウで [編集（Edit）] アイコンをクリックしてプラグインオプションを設定します。[保存（Save）] をクリックし、次に [次へ（Next）] をクリックします。



ステップ 8 [一括インストール（Mass Installation）] ウィンドウで [開始（Start）] をクリックし、一括インストールのプロセスを開始します。



ステップ 9 一括インストールの処理が完了するまで待ち、[次へ（Next）] をクリックします。

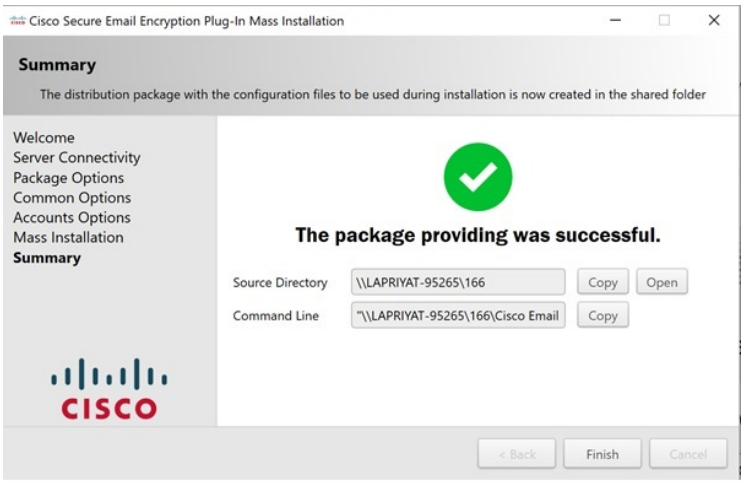


ステップ 10 [サマリー（Summary）] ウィンドウで、パッケージの格納場所へのパスと一括インストールスクリプトを取得できます。

配布パッケージとインストール時に使用するコンフィギュレーションファイルが共有のフォルダに作成されました。パスをこのフォルダにコピーするか、[オープン（OPEN）] をクリックしてフォルダの内容を表示できます。

指定したコマンドをコマンドラインで実行すると、SCCM 管理ツールで事前定義済みの設定を使用して Cisco Secure Email Encryption Plug-in を組織内のリモート マシンにインストールできます。SCCM 管理ツールの操作方法については、Cisco Secure Email Encryption Plug-in の一括インストールツール （12 ページ）をご覧ください。

SCCM ツールで再利用できるようこのスクリプトをコピーしたら、[終了（Finish）] をクリックします。



（注） パッケージと共有フォルダを作成したら、プロパティを確認してこのフォルダの [共有権限（Share Permissions）] を確認します。権限は [全員（Everyone）] に設定する必要があります。それ以外の場合は、手動で設定してください。フォルダを他のユーザーと共有する手順は、オペレーティングシステムによって異なる場合があります。

インストールの実行

インストールを実行するには、次の手順に従って、ネットワーク共有フォルダと配布パッケージを作成し、New Package Wizard と New Program Wizard を完了させます。

インストールを実行する手順：

手順

ステップ 1 インストール パッケージをダウンロードし、チェックサムを確認します。

a) 次の URL で Quick Hash GUI と SHA512 ハッシュアルゴリズムを使用して、インストールパッケージ用のチェックサムを生成します。https://sourceforge.net/projects/quickhash/

b) 生成されたチェックサムが次に一致することを確認します。

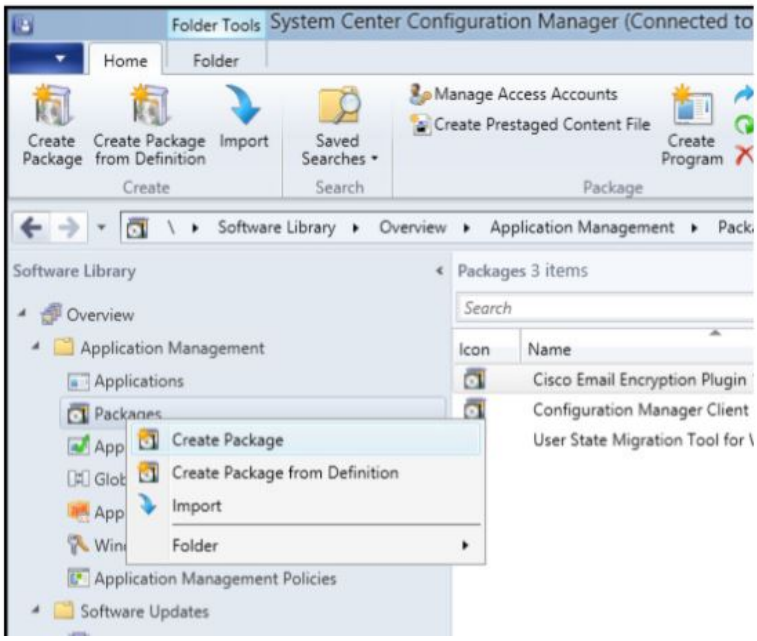
E858C451B9E638DD475BEEC79E53BEEA24DEA2827EEEE786921BD0
6A2D5404A3FA963EB72F9A8ECC4DBD7DBC4BF9C7B8E7448208E450 808E1693E1658C758C8E

ステップ 2 インストール パッケージを含むネットワーク共有フォルダを作成し、ユーザーに対して共有フォルダへのアクセス権限を付与します。

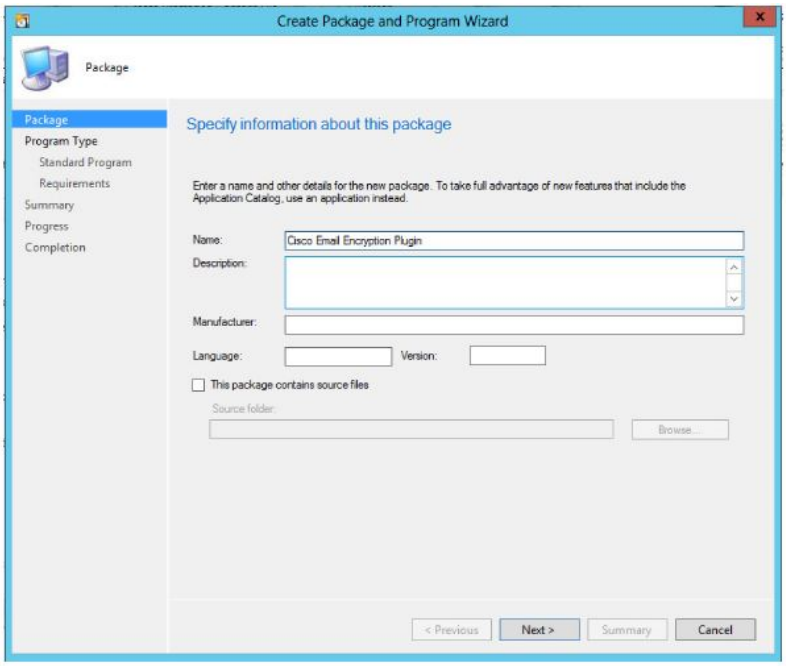
（注） dropbox、ネットワーク ドライブ、または共有システム フォルダからインストールを実行することはできません。

ステップ 3 **System Center Configuration Manager**（SCCM）管理ツールを開きます。

ステップ 4 左側のペインで [Application Management] を展開し、[Packages] を右クリックして [Create Package] をクリックします。



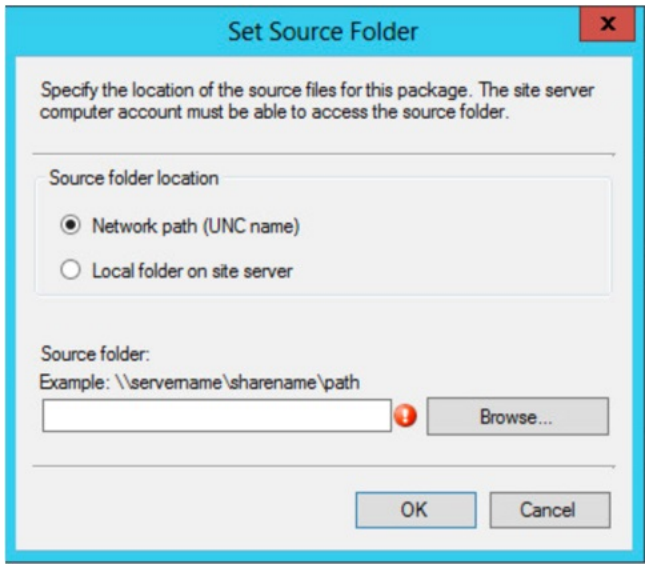
[Create Package and Program Wizard] ウィンドウが表示されます。



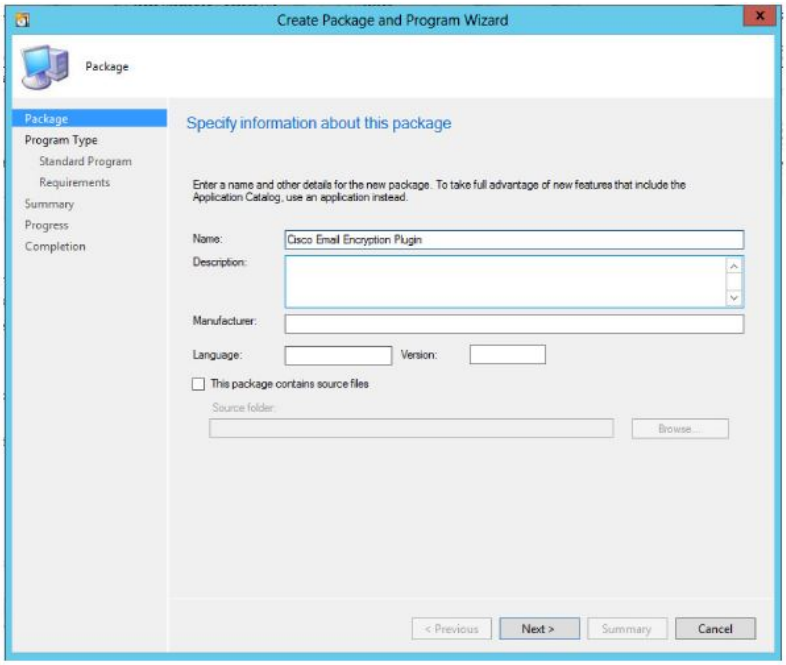
ステップ 5 [Name] ボックスに、パッケージの名前を入力します。たとえば、「*Cisco Email Encryption Plug-in*」と入力します。

ステップ 6 [This package contains source files] を選択し、[Browse] をクリックします。

ステップ 7 表示された [Set Source Folder] ポップアップで [Network path (UNC name)] を選択します。

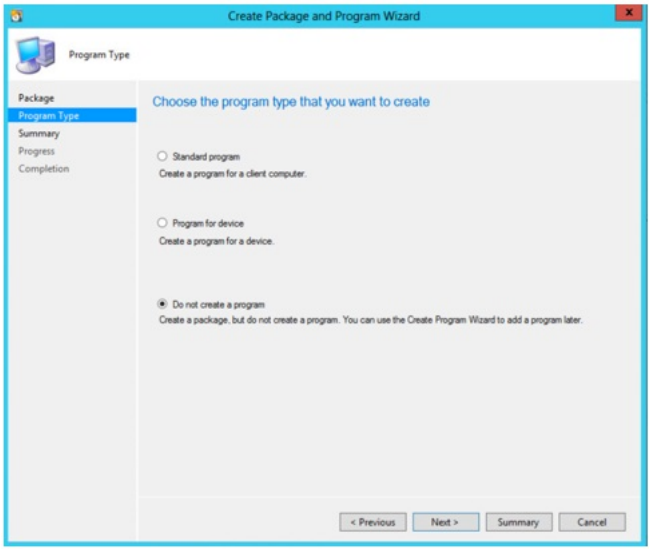


ステップ 8 [Source] フォルダにステップ 2 で作成したネットワーク ソース ディレクトリを入力し、[OK] をクリックします。

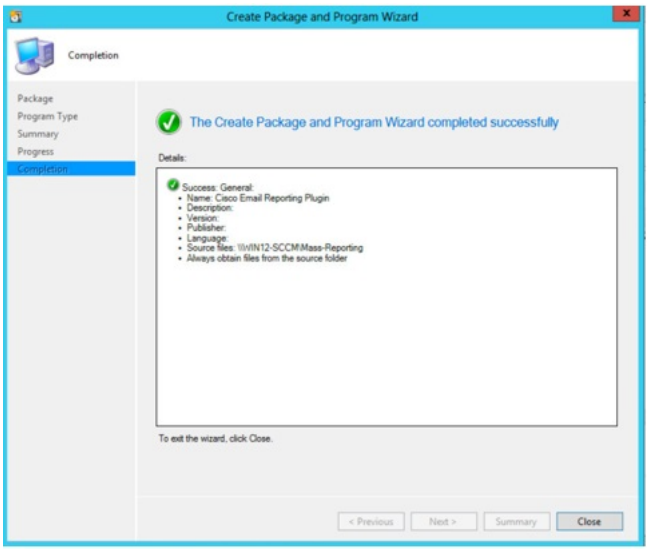


ステップ 9 [Next] をクリックします。

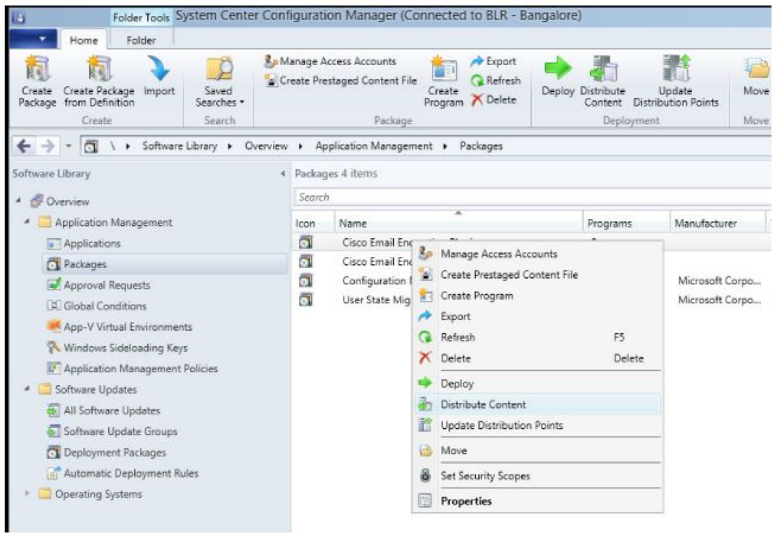
ステップ 10 [Do Not Create a Program] を選択し、[Next] をクリックします。



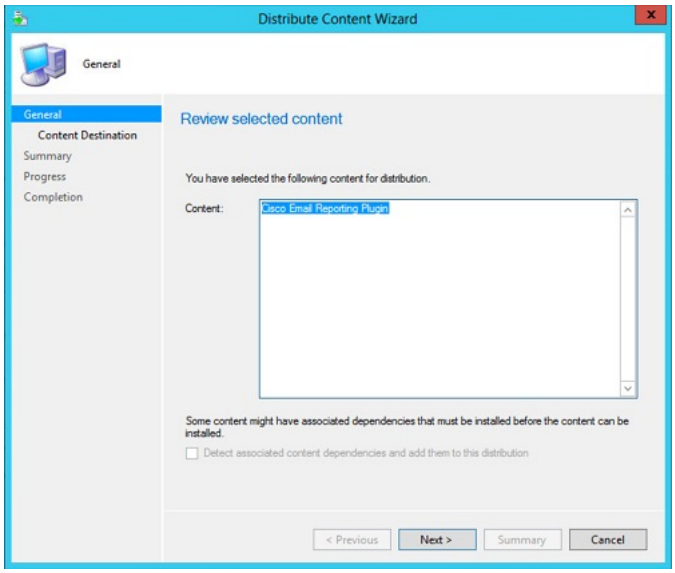
ステップ 11 [Next] をクリックし、[Create Package and Program Wizard] が正常に完了したら [Close] をクリックします。



ステップ 12 [System Center Configuration] で、作成したパッケージを右クリックし、[Distribute Content] をクリックします。

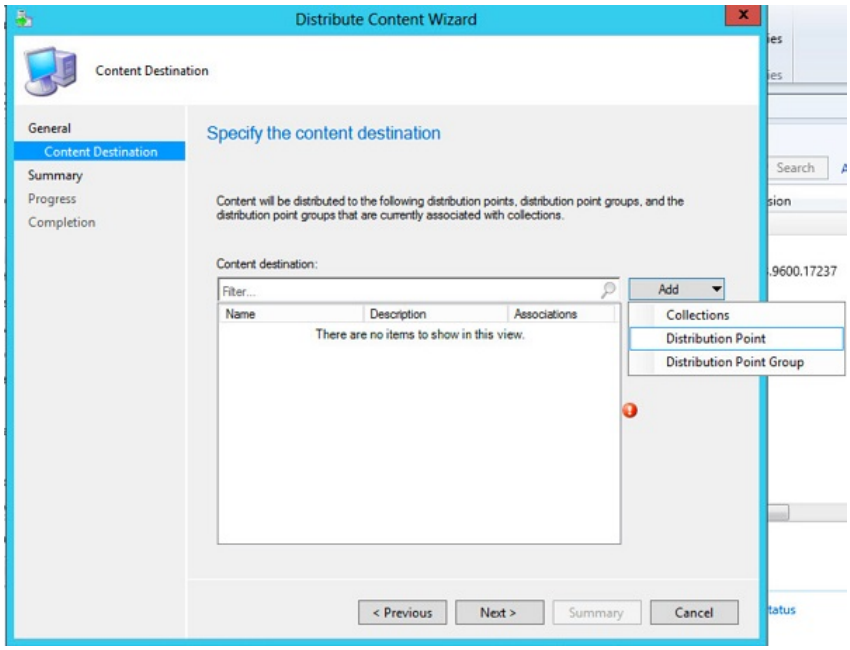


[Distribute Content Wizard] ウィンドウが表示されます。

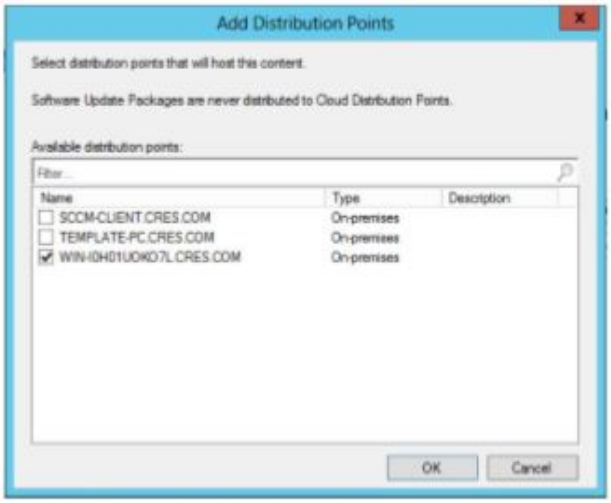


ステップ 13　[Next] をクリックします。

ステップ 14　[Content destination] 画面で [Add] > [Distribution Point] をクリックします。

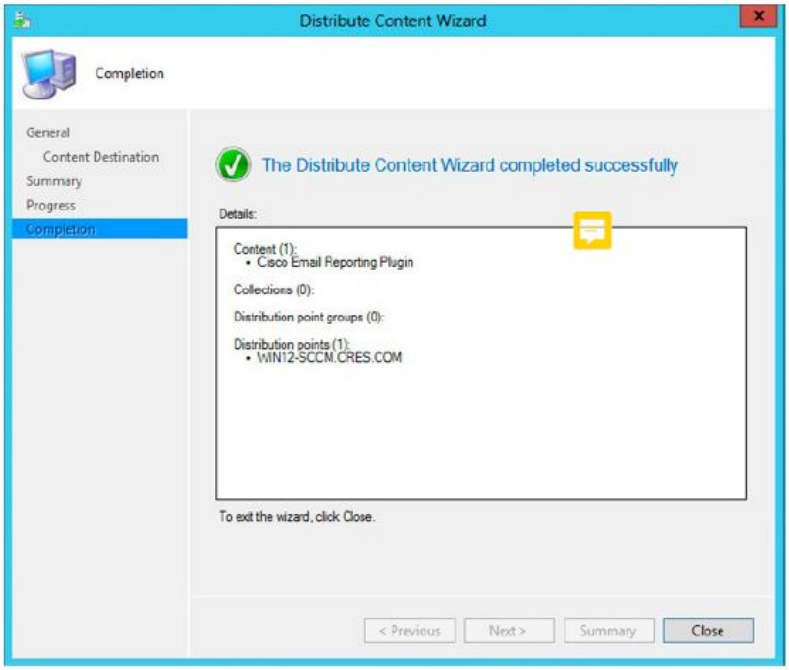


ステップ 15 表示された [Add Distribution Point] ポップアップで、必要な項目を選択し、[OK] をクリックします。

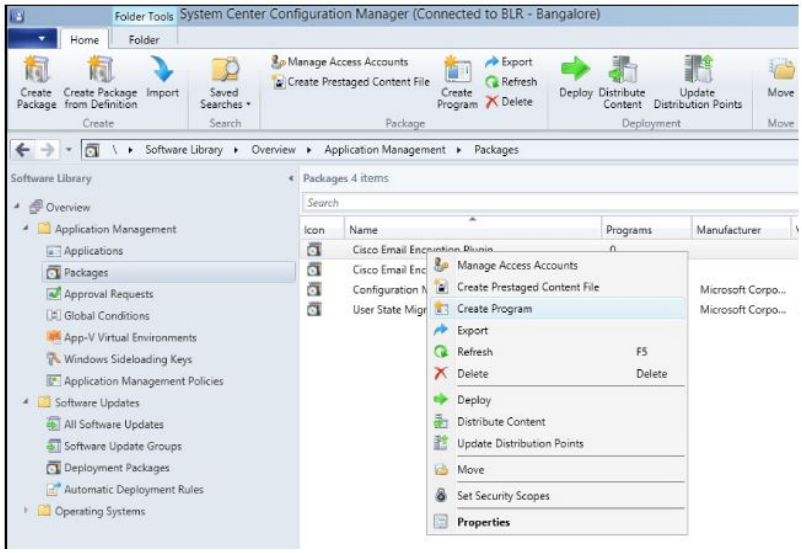


ステップ 16 [Next] をクリックします。

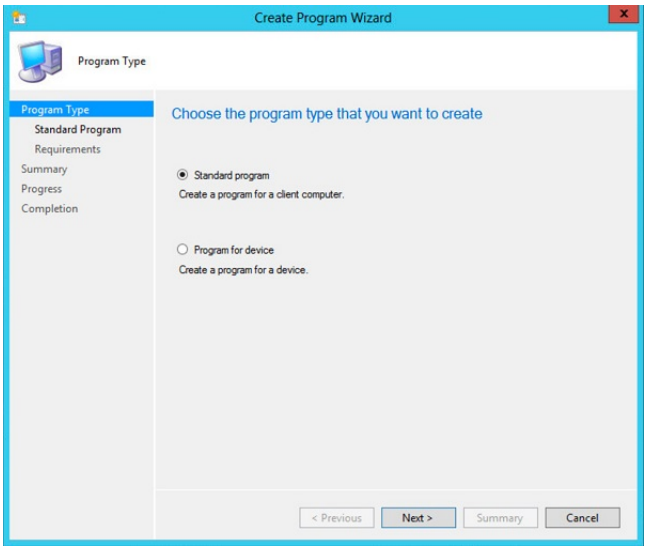
ステップ 17 [Next] をクリックし、[Distribute Content Wizard] が正常に完了したら [Close] をクリックします。



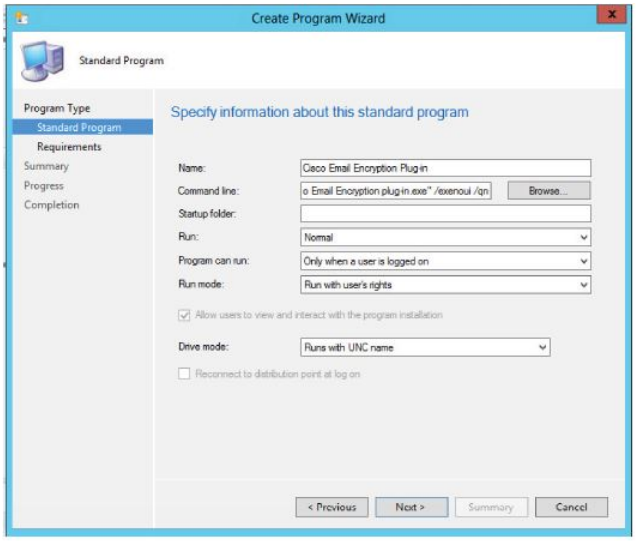
ステップ 18 [System Center Configuration] で、作成したパッケージを右クリックし、[Create Program] をクリックします。



[Create Package Wizard] ウィンドウが表示されます。



ステップ 19 [Standard Program] を選択して、[Next] をクリックします。

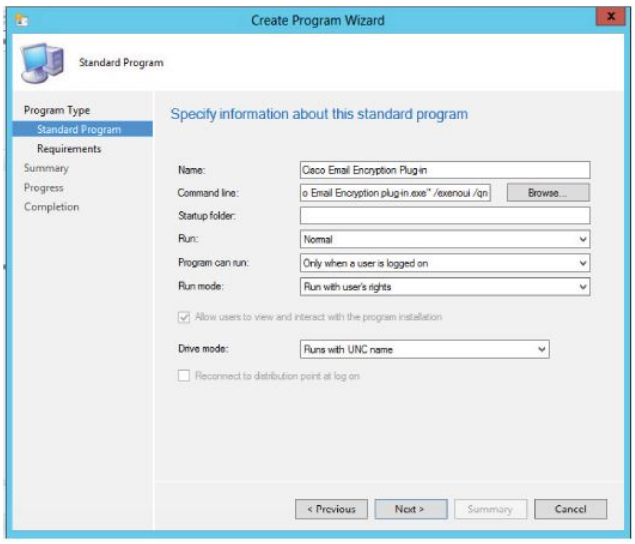


ステップ 20 [Command line] ボックスに *“Cisco Email Reporting Plug-in.exe” /exenoui /qn* と入力します。

（注） カスタマイズしたコンフィギュレーションファイルを使用する場合は、このステップで特殊キーを追加して、インストールでカスタムファイルを使用できるようにする必要があります。シンタックス *Cisco Email Encryption Plug-in.exe” /exenoui /qn UseCustomConfig="\\sc2007\Shared\config* を使用して特殊なキーをコマンドラインから追加できます（= 記号の後にカスタム コンフィギュレーション ファイルの場所を指定）。

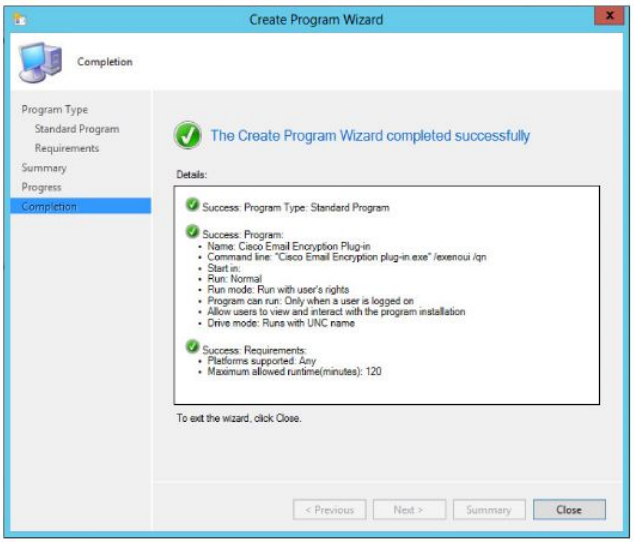
コンフィギュレーション ファイルの詳細については、カスタム コンフィギュレーション ファイルの使用 （30 ページ）を参照してください。

ステップ 21 [Next] をクリックします。

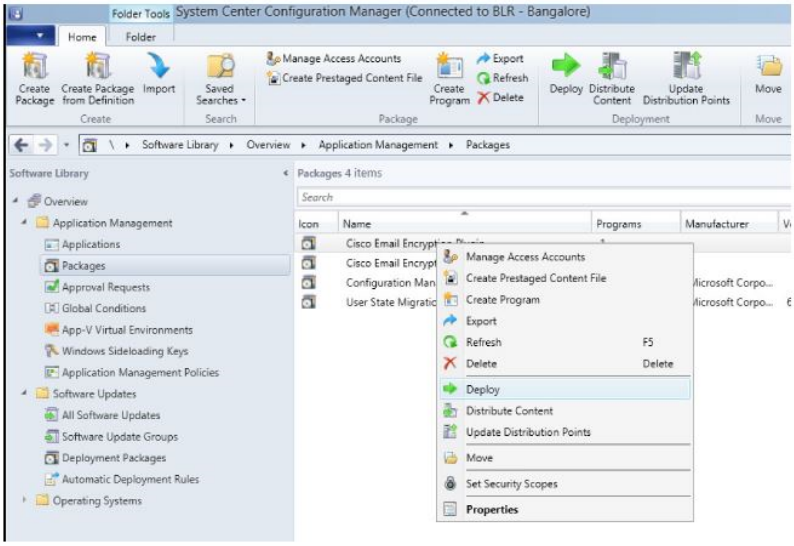


ステップ 22 [Next] をクリックします。

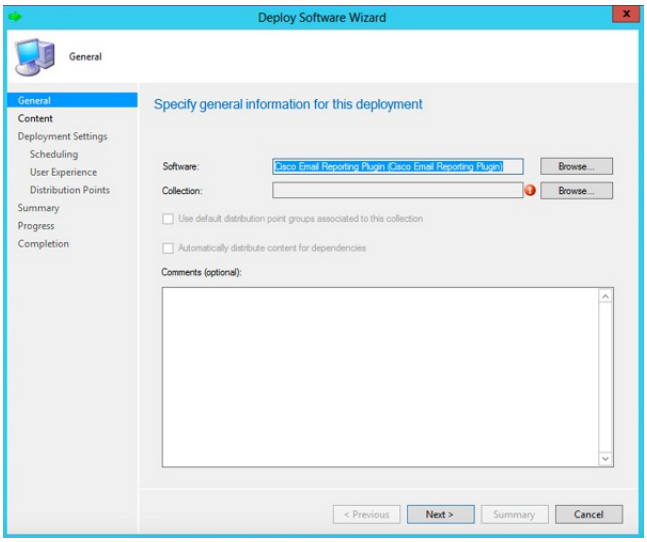
ステップ 23 [Next] をクリックし、[Create Program Wizard] が正常に完了したら [Close] をクリックします。



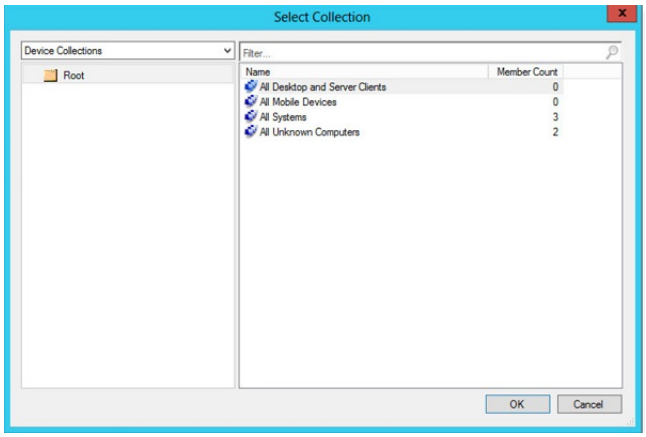
ステップ 24 System Center Configuration Manager で、作成したパッケージを右クリックし、[Deploy] をクリックします。



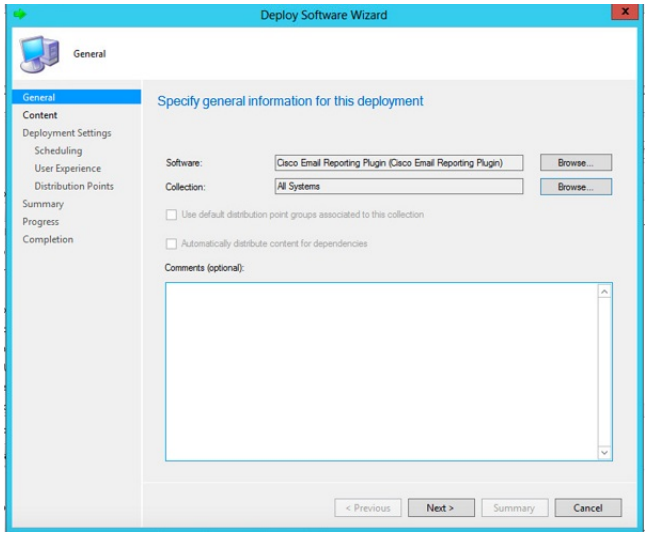
[Deploy Software Wizard] ウィンドウが表示されます。



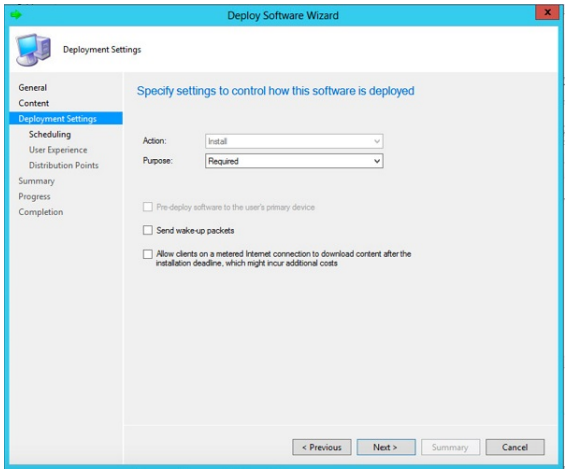
ステップ 25 [Collection] の横にある [Browse] をクリックします。



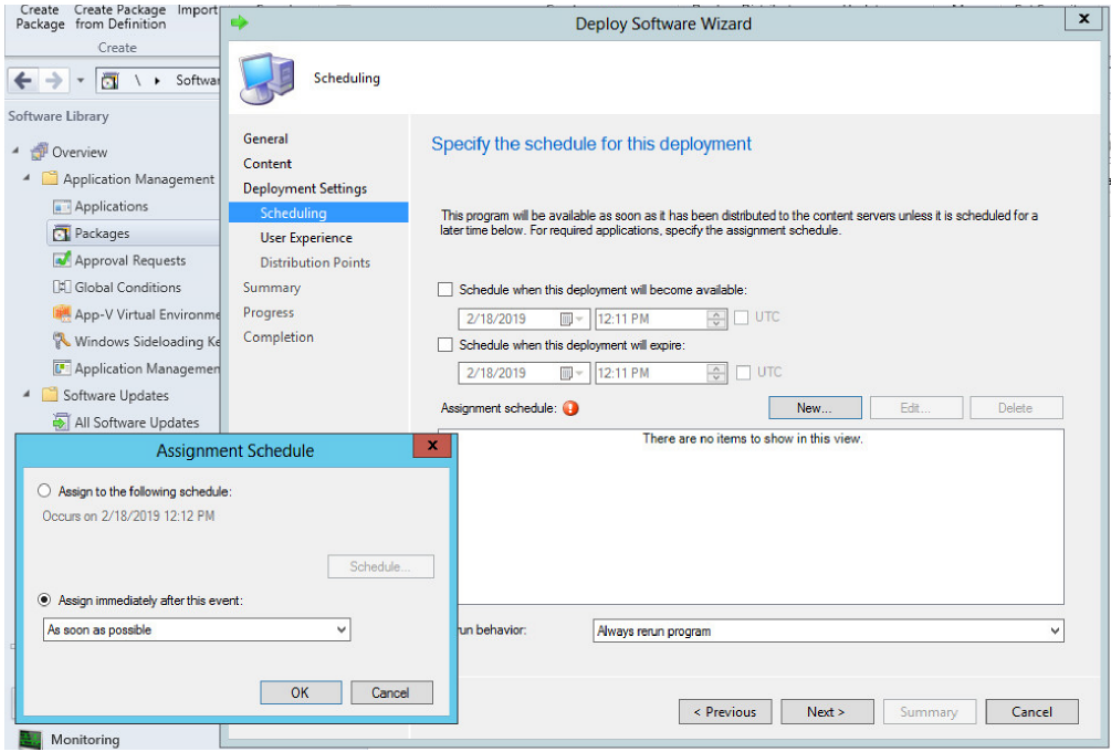
ステップ 26 表示された [Start Collection] ポップアップで、プラグインをインストールするクライアントのグループが含まれている必要なデバイスのコレクションを選択し、[OK] をクリックします。



ステップ 27 [Next] をクリックします。



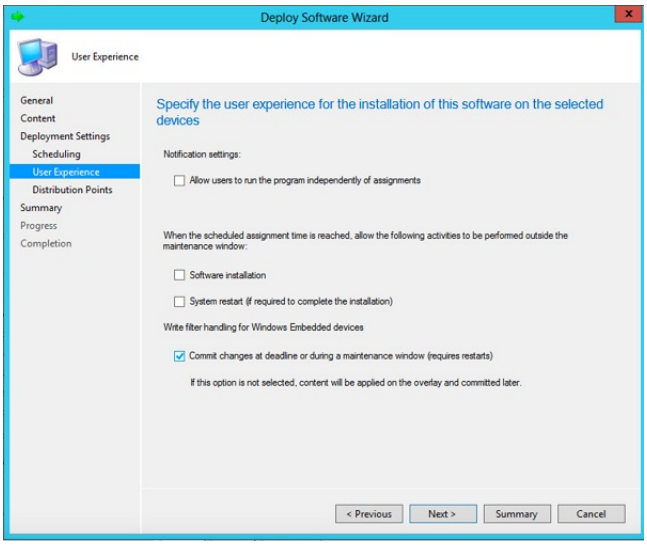
ステップ 28　[Next] をクリックします。



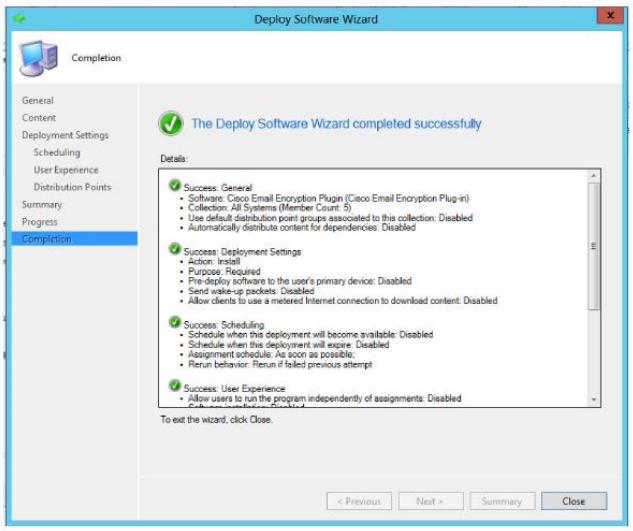
ステップ 29　[Scheduling] ページで [New] をクリックして、新しい割り当てスケジュールを作成します。

ステップ 30　[Assign immediately after this event] を選択し、ドロップダウンリストから [As soon as possible] を選択して [OK] をクリックします。

ステップ 31　[Next] をクリックします。



ステップ 32 [Deploy Software Wizard] が正常に完了したら [Next] をクリックし、[Deploy Software Wizard] をクリックします。



ステップ 33 [Deployment Status] を参照して、プロセスが正常に完了したことを確認します。

カスタム コンフィギュレーション ファイルの使用

Cisco Secure Email Encryption Plug-in では、インストールに含まれている一連の XML ファイルを編集することで、デフォルトの設定を変更できます。別のコンフィギュレーションファイルを使用して、インストールの設定を変更することもできます。たとえば、config_1.xml コンフィギュレーションファイルでファイルにフラグを付ける方法など、いくつかの暗号化オプションを変更できます（この変更は、暗号化アプライアンスでもこの方法を変更できる場合に限り行います）。ボタン名をカスタマイズしたり、さらに、ユーザーインターフェイスで使用されるテキストをローカライズすることもできます。

概要

カスタムコンフィギュレーションファイルを変更して展開するには、次の手順を実行します。

手順

ステップ 1 **\\%allusersprofile%\Cisco\Cisco Email Encryption Plug-In** ディレクトリのコピーを作成します。Common フォルダを含める必要があります。

（注） 妥当性を保つために、元のファイルのディレクトリ構造を維持する必要があります。**Cisco Email Encryption Plug-in** ディレクトリから始まる構造が維持され、構成ファイルとともにすべてのファイルが含まれていることを確認します。

ステップ 2 XML コンフィギュレーション ファイルを編集します。新しいファイルを作成する代わりに、インストール ファイルに含まれている XML ファイルを変更することをお勧めします。これらのファイルの変更方法については、XML コンフィギュレーション ファイルの編集 （31 ページ）を参照してください。

ステップ 3 インストールの前提条件 （11 ページ）の説明に従って一括インストールを実行し、カスタム コンフィギュレーション ファイルの展開 （33 ページ）の説明に従ってカスタマイズした XML ファイルを展開します。

XML コンフィギュレーション ファイルの編集

Cisco Secure Email Encryption Plug-in をインストールすると、構成データが作成されて XML ファイルに保存されます。文字列型の値を編集して、パラメータ値をカスタマイズすることができます。ただし、値を削除することや、ファイルの構造を変更することはお勧めしません。

デフォルトでは、プラグインによって、Outlook の次の場所にある %AllUsersProfile% ディレクトリにコンフィギュレーション ファイルがインストールされます。

```
%allusersprofile%\Cisco\Cisco Email Encryption Plug In
```

XML ファイルは次のデフォルトの場所にあります。

- **\\%allusersprofile%\Cisco\Cisco Email EncryptionPlug-In\Common\config_1.xml, config_{N}.xml**。この番号はユーザー アカウントの数によって異なります。デスクトップ暗号化プラグインに関連する構成データが含まれています。
- **\\%allusersprofile%\Cisco\Cisco Email EncryptionPlug-In\Common\CommonComponentsConfig.xml**。ログファイルの場所やローカライゼーションファイルの名前（デフォルトのローカライゼーションファイルは*en.xml*）などの暗号化プラグインに関する基本的な情報が含まれています。電子メールプログラムの設定を使用してログ ファイルの場所を変更し、一括インストール プログラムによってそれを展開できます。使用可能なローカリゼーションファイルとは異なる言語でローカリゼーション ファイルを作成する場合は、新しい XML ファイルの名前をここで指定する必要があります。
- **\\%allusersprofile%\Cisco\Cisco Email EncryptionPlug-In\Common\Localization\en.xml**。ローカル言語に関連するデータが含まれています。デフォルトの言語は英語です。ただし、*de.xml*、*es.xml*、*fr.xml*、*it.xml*、*zh.xml*、*pt.xml*、*ja.xml* など、いくつかのローカリゼーションファイルが使用可能です。これらの xml ファイルの対象外の言語を使用する場合は、カスタム xml ファイルを作成し、そのファイルを CommonConfig.xml ファイルで指定できます。

⚠

注意 < または > 記号の内側になるどの文字列 ID も変更しないでください。変更するとプラグインが正しく機能しなくなります。

BCE_Config.xml ファイルによる一括インストール

BCE_Config.xml ファイルを使用して一括インストールするには、次の手順を実行します。

手順

ステップ 1 **\\%allusersprofile%\Cisco\Cisco Email Encryption Plug-In\Common** ディレクトリに移動します。

ステップ 2 *config_1.xml* ファイルを削除します（ファイルがある場合）。

ステップ 3 BCE 構成ファイル（デフォルトでは *BCE_Config_signed.xml*）をこのディレクトリへコピーして、ファイル名を *config_1.xml* に変更します。

ステップ 4 **\\%allusersprofile%\Cisco\Cisco Email Encryption Plug-In\CommonComponentsConfig.xml** ファイルに移動します。

ステップ 5 *CommonComponentsConfig.xml* ファイルに次のタグが含まれていることを確認します。

例：

```
<accountFileNames>
   <accountFileName filePath="config_1.xml" emailAddressAndKeyServer="*" />
 </accountFileNames>
```

ヒント *accountFileName* タグには profileName 属性を含めないでください。属性が含まれている場合は、削除してください。

（注） 特定ドメイン内の選択したユーザーだけを設定するには、そのドメインを電子メール アドレスとして指定するように、*CommonComponentsConfig.xml* ファイルを変更する必要があります。

たとえば、シスコのユーザーだけに BCE コンフィギュレーション ファイルを適用するには、下記を変更します。

```
<accountFileName filePath="config_1.xml" emailAddressAndKeyServer ="*" />
```

が、次のように変わります。

```
<accountFileName filePath="config_1.xml" emailAddressAndKeyServer="@cisco.com"
 />
```

accountFileName タグが複数ある場合、filePath は、config_2.xml、config_3.xml のようになります。

次に例を示します。

```
<accountFileName filePath="config_2.xml" emailAddressAndKeyServer ="@cisco.com"
 />
```

ステップ 6 インストールの前提条件 （11 ページ）の説明に従って一括インストールを実行し、カスタム コンフィギュレーション ファイルの展開 （33 ページ）の説明に従って、カスタマイズした XML ファイルを展開します。

（注） **\\%allusersprofile%\Cisco\Cisco Email Encryption Plug-In\Common** ディレクトリの内容を **\\{SHARED_DIR}\{CONFIG_FOLDER}** にコピーする必要があります。また、{CONFIG_FOLDER} に Common フォルダが存在していなければなりません。UseCustomConfig コマンド パラメータを使用すると、変更したカスタム コンフィギュレーション ファイルをインストールで使用できます。

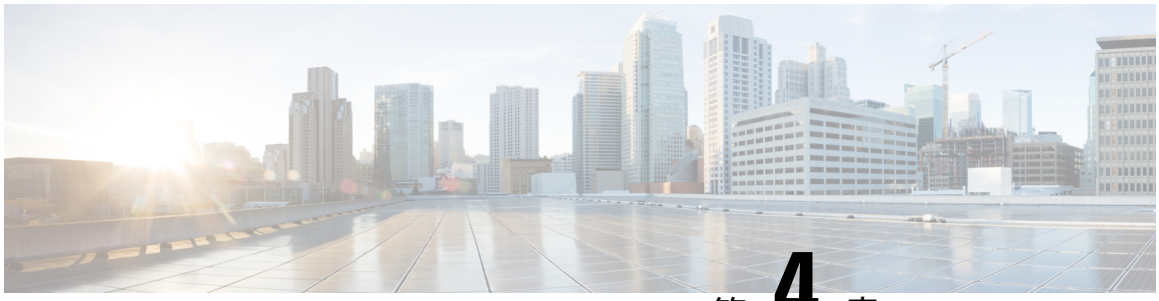
カスタム コンフィギュレーション ファイルの展開

コンフィギュレーションファイルの編集が完了したら、展開時に特殊キーを追加して、変更したカスタム コンフィギュレーション ファイルがインストーラで使用されるようにする必要があります。**UseCustomConfigs** コマンド ライン パラメータを使うと、インストールでカスタム コンフィギュレーション ファイルを使用できます。また、このパラメータによって、インストール時に使用するコンフィギュレーションファイルが格納されているフォルダのパスを指定します。

一括インストールで、次のシンタックスを使用してコマンドラインから **UseCustomConfig** キーを追加します（インストールの前提条件 （11 ページ）を参照）。

```
Cisco Email Encryption Plugin.exe /exenoui /qn
UseCustomConfig="\\{SHARED_DIR}\{CONFIG_FOLDER}
```

=の後ろのパスによって、カスタマイズしたコンフィギュレーションファイルのパスを指定します。



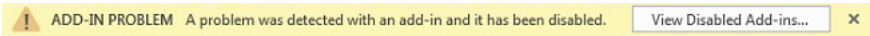
第 4 章

Cisco Secure Email Encryption Plug-in for Outlook の設定と使用

この章では、Cisco Secure Email Encryption Plug-in for Outlook で使用可能な機能について説明します。Cisco Secure Email Encryption Plug-in には Outlook 電子メールプログラムと連動するいくつかのタイプのプラグインが用意されています。

Cisco Secure Email Encryption Plug-in の有効化

インストール後に初めて Cisco Secure Email Encryption Plug-in を起動すると、Outlook によって無効にされることがあります。無効になっている場合には、次のメッセージが表示されます。



Cisco Secure Email Encryption Plug-in を有効にするには、通知バーの [View Disabled Add-ins] ボタンをクリックして [Disabled Add-ins] ダイアログを表示します。起動時にどれだけ時間がかかっても必ずアドインが実行されるように Outlook を設定するには、[Always enable this add-in] ボタンをクリックします。

使用状況データ収集の設定

Cisco Secure Email Encryption Plug-in を最初に起動すると、製品の改善に役立てるために匿名データをシスコに送信できるようにするかどうかを尋ねられます。[Send anonymous usage data to Cisco] チェックボックスをオンにすると、次の 2 つのタイプの情報が収集され、分析するために Cisco サーバーに保存されます。

- プラグインを実行しているマシンに関する一般情報
- アカウント固有の情報

以下では、この情報の詳細について説明します。

起動後に [プラグインオプション（Plug-in Options）] > [追加オプション（Additional Options）] > [使用状況を送信する（Sending usage data）] タブを選択し、使用率データの送信を有効または無効にすることができます。

使用状況データのシスコへの送信を有効または無効にするには、CommonComponentsConfig.xml ファイルで次のパラメータを設定します。

- callHomeAdminEnabled：Outlook を起動したときに使用状況データの送信を有効にするには true を、送信を無効にするには false を設定します。デフォルト値は true です。falseに設定すると、使用状況データ収集に関する通知を受信できず、シスコに匿名の使用状況データを送信することができなくなります。

一般情報

次の情報が収集されます。

- 識別子（UUID）：プラグインを最初にインストールするときに生成される非永続的な識別子。使用状況データが時系列で追跡する使用状況レポートを関連付ける目的でのみ使用します。[Plug-in Options] > [Additional Options] > [Privacy] タブを選択すると、識別子をリセットすることができます。
- オペレーティング システムのバージョン
- Microsoft Outlook のバージョン
- Cisco Outlook Plug-in のバージョン
- Cisco Encryption SDK のバージョン：この SDK は、セキュリティで保護されたメッセージの暗号化と復号化のためにプラグインが内部で使用するライブラリです。
- オペレーティング システムで使用される言語

- インストールされたすべての Outlook プラグインの名前

アカウント固有の情報

次の情報が収集されます。

- アカウント タイプ：タイプは暗号化、復号化、またはフラグのいずれかです。
- サーバ
- 受信者数：インストールされてから暗号化中に追加された受信者の数。フラグ設定中に追加された受信者も含まれます。
- 復号化カウント：プラグインを使用して復号化されたメッセージの数。
- 暗号化カウント：インストールされてからデバイスで暗号化されたメッセージの数。フラグが付けられたメッセージの数も含まれます。
- メッセージの管理カウント：[メッセージの管理] 画面へのアクセス回数。
- メッセージの管理の使用数：[Manage Messages] 画面を使用して更新されたメッセージの数。

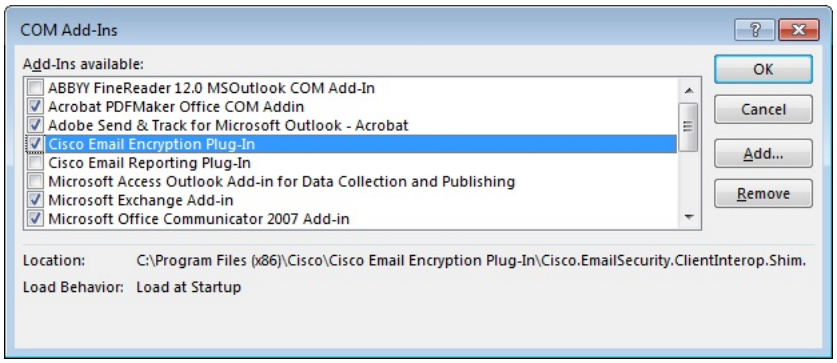
Cisco Secure Email Encryption Plug-in for Outlook の全般設定

Cisco Secure Email Encryption Plug-in の全般設定は、[Options] ページから行えます。

Enable または Disable

デフォルトでは、Cisco Secure Email Encryption Plug-in はインストール時に有効になります。Cisco Secure Email Encryption Plug-in は次の場所から無効にできます。

- Outlook 2010/2013/2016 では、[File] > [Options] に移動し、左側のナビゲーション バーから [Add-ins] を選択します。次に、ページの下部にある [Manage] ドロップダウン メニューから [COM Add-ins] を選択し、[Go...] をクリックします。
- Outlook 2007 では、[Tools] > [Trust Center] に移動し、左側のナビゲーション バーから [Add-ins] を選択します。次に、ページの下部にある [Manage] ドロップダウンから [COM Add-ins] を選択し、[Go] をクリックします。



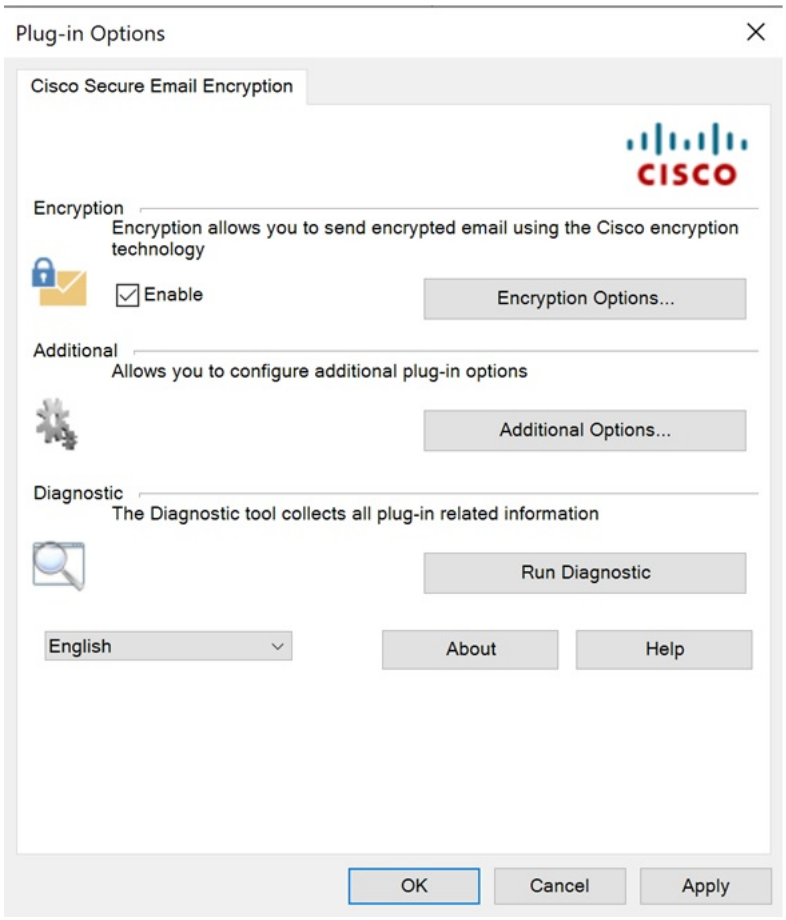
[COM Add-Ins] ウィンドウで、[Cisco Secure Email Encryption Plug-in] チェックボックスをオフにして [OK] をクリックします。

Outlook プラグインの基本設定

エンドユーザーは [Cisco Secure Email Encryption] タブで基本的な設定項目を設定できます。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、または [File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Encryption] に移動します。
- Outlook 2007 では、ツールバーの [Plug-in Options] ボタンをクリックするか、または [Tools] > [Options] > [Cisco Email Security Encryption] に移動します。

[Cisco Secure Email Encryption] タブ：



エンドユーザーは、このタブで[Enable]チェックボックスをオンにすることにより、暗号化のオプションを有効にできます。エンドユーザーは、[Additional Options] ボタンを選択して、その他のオプションを有効にすることができます。詳細な設定を行うには、[Encryption Options] または [Additional Options] ボタンをクリックします。エンドユーザーは、問題解決時に診断ツールを使用し、Cisco Secure Email Encryption Plug-in でレポートを実行してシスコのサポートに送信することもできます。Outlook を起動したときに、匿名の使用情報（Plug-in の使用に関する一般情報）をサーバーへ送信するように Plug-in を設定することもできます。

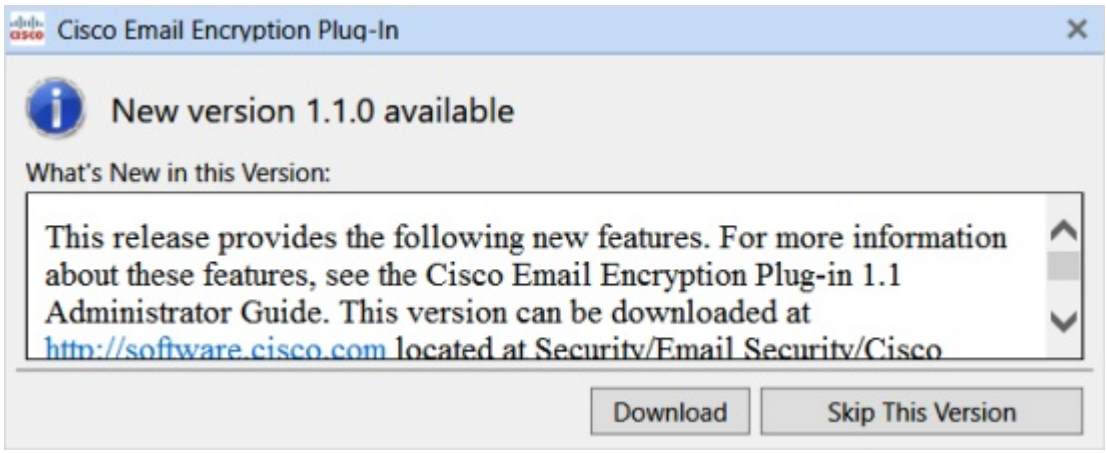
更新をチェックするための Outlook Plug-in の設定

更新を自動でチェックするようにプラグインを設定するには、CommonComponentsConfig.xml ファイルの checkForUpdates セクションで次のパラメータを設定します。

- checkAutomatically：Outlook を起動したときに更新の自動チェックを有効にするには true を、無効にするには false を設定します。デフォルト値は true です。
- serverURL：新しいバージョンを利用できるかどうかをチェックするためにプラグインで使用する URL を設定します。
- ignoredVersion：更新を探すときに、プラグインで無視するバージョン番号を設定します。

更新の通知

Desktop Encryption プラグインで更新を自動的にチェックするように設定されており、Desktop Encryption プラグインの現在のバージョンが最新ではない場合は、Outlook の起動時に次のダイアログボックスが表示されます。



（注） Cisco Secure Email Encryption Plug-in アプリケーションをダウンロードするための適切な権限が必要です。

Outlook を起動した後で更新をチェックするには、[Plug-in Options] ウィンドウの [About] ボタンをクリックし、次のダイアログボックスで [Check for updates] ボタンをクリックします。

BCE_Config ファイルを使用した共通オプションの設定

すべての Outlook アカウントおよびプラグイン全体で共通のオプションは、CommonComponentsConfig.xml ファイルに含まれています。これらのオプションを次に示します。

- diagnosticSupportAddress：診断ツールを実行したときに送信されるメッセージの受信者の電子メール アドレスを指定します。メッセージには、診断ツールの出力が含まれます。
- diagnosticReportSubject：診断ツールを実行したときに送信されるメッセージの件名を指定します。
- showPluginOptions：暗号化、診断、追加オプションを実行できる [Plug-in Options] ダイアログボックスを開く [Plug-in Options] ボタンを有効にするには true に、無効にするには false に設定します。false を設定すると、[Plug-in Options] ボタンは表示されません。
- showManageMessageButton：メッセージをロックしたり、メッセージの有効期限を設定できる [Manage Messages] ダイアログボックスを開く [Manage Messages] ボタンを有効にするには true に、無効にするには false に設定します。false を設定すると、[Manage Messages] ボタンは表示されません。
- checkAutomatically：Outlook を起動したときに更新の自動チェックを有効にするには true を、無効にするには false を設定します。デフォルト値は true です。詳細については、更新をチェックするための Outlook Plug-in の設定 （39 ページ）を参照してください。

- serverURL：新しいバージョンを利用できるかどうかをチェックするためにプラグインで使用する URL を設定します。
- callHomeAdminEnabled：Outlook を起動したときに使用状況データの送信を有効にするには true を、送信を無効にするには false を設定します。デフォルト値は true です。falseに設定すると、使用状況データ収集に関する通知を受信できず、シスコに匿名の使用状況データを送信することができなくなります。詳細については、使用状況データ収集の設定（36 ページ）を参照してください。
- callHomeEnabled：Outlook を起動したときに使用状況データの送信を有効にするには true を、送信を無効にするには false を設定します。デフォルト値は true です。false に設定すると、ユーザーは匿名の使用状況データをシスコに送信できません。詳細については、使用状況データ収集の設定 （36 ページ）を参照してください。

これらのオプションが BCE_Config.xml ファイルに設定されている場合は、プラグインが BCE_Config.xml を適用すると、オプションが CommonComponentsConfig.xml にコピーされます。それ以外の場合、これらのオプションをユーザー環境で変更するには、UseCustomConfig オプションで多数のインストールを実行する必要があります。詳細は、BCE_Config.xml ファイルによる一括インストール （32 ページ）のセクションを参照してください。

同様に、BCE_Config を適用して、アカウント固有のファイル（config_1.xml、config_2.xml など）でオプションを設定することもできます。ただし、BCE_Config.xml ファイルを使用してロギングの設定、またはプラグインのローカリゼーションを設定することはできません。

BCE_Config.xml のパラメータの詳細については、BCE_Config.xml のパラメータ （87 ページ）を参照してください。

暗号化メッセージのストレージオプションの設定

[メッセージからの読み取り（Read from Message）] 機能（旧 Easy Open）を使用すると、受信者は、クライアント側のアプリケーションをインストールすることなく、どのデバイスからでもエンベロープを開封することができます。これは、エンベロープを受信者への添付ファイルとして送信することに加えて、Cisco Secure Email Encryption Service または外部ストレージに暗号化されたメッセージのコピーを保存することによって実現できます。

有効になっている場合は、[メッセージを読む（Read Message）] ボタンを備えた新しいテンプレートにセキュアメッセージが表示されます。受信者がこのボタンをクリックすると、その受信者は、セキュアメッセージを認証して復号するように指示されます。

重要 [メッセージを読む（Read Message）] のサポートは、Cisco Secure Email Gateway（ESA）11.1.0-302、11.1.3-006、および 12.x（一般的な導入）以降のリリースで利用できます。

外部ストレージの設定

この機能が有効になっている場合、暗号化されたエンベロープのコピーを保存する優先ストレージを設定できます。次のストレージオプションを使用できます。

- Cisco ストレージ
- Microsoft OneDrive ストレージ

（注） 大きな添付ファイル用に OneDrive ストレージを使用しているときに、セキュアメッセージに [メッセージを読む（Read Message）] ボタンを表示するには、Microsoft Office365 アプリケーションに *files.write* および *file.readwrite* API 権限が存在している必要があります。

Cisco Secure Email Encryption Plug-in でメッセージからの読み取りと外部ストレージを設定するには、『Cisco Secure Email Encryption Service Account Administrator Guide』を参照してください。

Cisco Secure Email Encryption Plug-in で Easy Open 機能を設定した後に、セキュアメッセージのオープン （43 ページ） を参照してください。

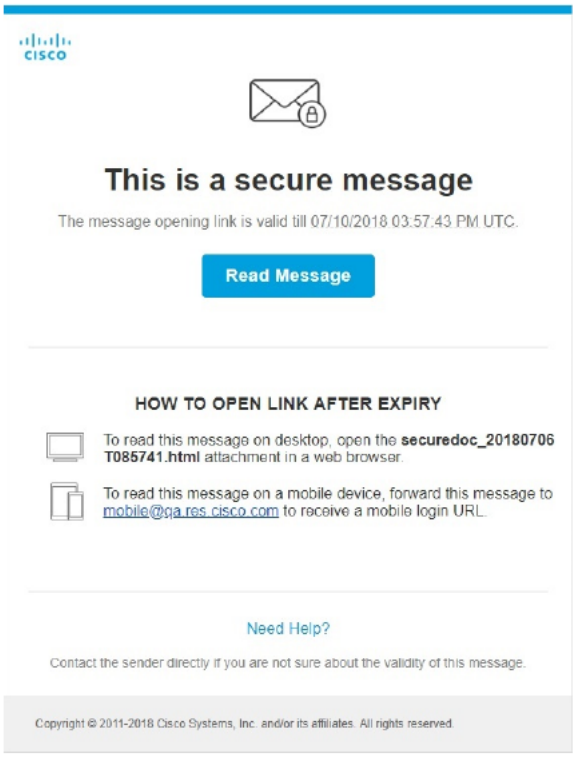
セキュアメッセージのオープン

Cisco Secure Email Encryption Service にユーザーアカウントを登録して、セキュアなメッセージを開くには、次の手順を実行します。

（注） アカウントで Easy Open を有効にしている場合は、[Read Message] ボタンと securedoc HTML 添付ファイルを通知メールメッセージに表示できます。

手順

ステップ 1 セキュアメッセージを読むには、通知メールメッセージの [Read Message] ボタンをクリックします。



ステップ 2 メールボックスのセキュアメッセージをダブルクリックします。[Register] ボタンが付いた [Decryption] ダイアログが表示されます。

ステップ 3 [Email Address] ドロップダウンメニューから電子メールアドレスを選択し、[Register] をクリックします。[New User Registration] ページが開きます。

（注） 複数のメールアドレスで登録済みエンベロープを受信する場合は、複数のユーザーアカウントを設定する必要があります。電子メールアドレスごとに個別のユーザーアカウントが必要です。

ステップ 4 フォームに入力して、[Register] をクリックします。

ステップ 5 受信箱フォルダにアカウントのアクティベーション メッセージが届いていないか確認します。電子メールのアクティベーション リンクをクリックします。

ステップ 6 元の電子メールに戻り、セキュアメッセージをダブルクリックします。

ステップ 7 [Password] フィールドに Encryption Service を入力し、[OK] をクリックしてセキュアメッセージを読み取ります。

次のタスク

暗号化されたセキュア メッセージを初めて開封する場合 （45 ページ）

暗号化されたセキュア メッセージを初めて開封する場合

暗号化されたセキュアメッセージを受信した場合、その暗号化されたメッセージを開くには、Cisco Secure Email Encryption Service に登録し、ユーザーアカウントを設定する必要があります。サービスに登録した後は、アカウントのパスワードを使用することで、受信したすべての暗号化メッセージを開くことができます。

新規ユーザー登録のオプション

フィールド	説明
Language	オプション。ドロップダウンメニューから、Encryption Service アカウントで使用する言語を選択します。登録ページはデフォルトでは英語で表示されますが、日本語、英語、フランス語、ドイツ語、スペイン語、ポルトガル語から選択できます。
First Name	必須です。Encryption Service ユーザーアカウントの名前（名）を入力します。
Last Name	必須です。Encryption Service ユーザーアカウントの名前（姓）を入力します。
Password	必須です。アカウントのパスワードを入力します。パスワードは 8 文字以上とし、数字とアルファベットの両方を含める必要があります。

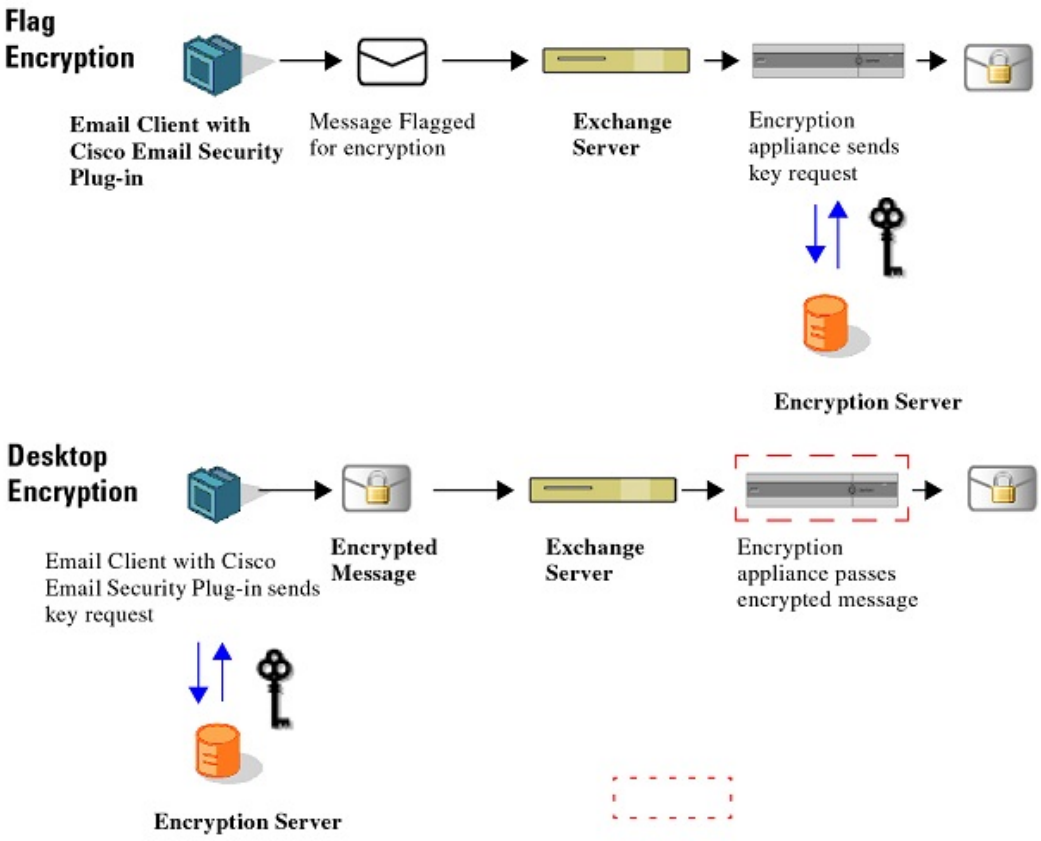
電子メールの暗号化

暗号化プラグインを使用すると、エンドユーザーは企業ネットワークの外部に電子メールを送信する前に、デスクトップからメールを暗号化したり、暗号化が必要な電子メールにフラグを設定することができます。次のいずれかの暗号化オプションを選択します。

- **Flag暗号化**。Flag暗号化オプションを使用すると、エンドユーザーは暗号化に必要なフラグを設定できます。また、Cisco Secure Email Gateway によって電子メールが暗号化されてから電子メールがネットワークの外部に送信されます。Flag 暗号化は、エンド ユーザーが組織外に送信するメールを暗号化する必要があり、組織内で送信するメールの暗号化を必要としない場合に使用できます。たとえば、機密の医療文書を扱っている組織では、患者に送信する前にそれらの文書を暗号化する必要があります。
- **デスクトップ暗号化**。デスクトップ暗号化では、Cisco 暗号化テクノロジーを使用して Outlook 内から電子メールを暗号化できます。その後、暗号化された電子メールがデスクトップから送信されます。デスクトップ暗号化は、エンド ユーザーが組織内で送信する

メールを暗号化する必要がある場合に使用できます。たとえば、組織内と組織外の両方の送信において、すべての機密財務データを暗号化する必要がある場合などです。

図 *1 : Flag* 暗号化とデスクトップ暗号化のワークフロー



（注） 暗号化の方式は、Outlook 電子メールアカウントから、署名された BCE Config 添付ファイルを復号化することによって決まります。デフォルトでは、Decrypt Only モードが有効になります。エンドユーザーは、管理者から更新済みの署名された BCE Config ファイルを受信して復号化することによって暗号化方式を変更できるように、インストールを変更できます。

Flag およびデスクトップ暗号化の設定

エンドユーザーの Outlook 電子メールアカウント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。フラグまたは暗号化機能を有効にするには、更新済みの添付ファイルを管理者から受け取り、それを使用してエンドユーザーの電子メール アカウントを設定し

ます。また、フラグおよび暗号化機能は一括インストールによって有効化できます。一括インストールでは、一連のコンフィギュレーション ファイルがユーザーの設定フォルダに直接配布されます。復号化したメッセージに、署名された BCE 構成添付ファイルが含まれている場合は、エンドユーザーがその構成ファイルを起動すると、Encryption Plug-in for Outlook が自動的に設定されます。 Cisco Secure Email Encryption Service はキーサーバーとして使用されます。エンド ユーザーがアカウントを持っていない場合は、登録を求めるプロンプトが表示されます。

次の 3 つのコンフィギュレーション モードを利用できます。

- **Decrypt Only**：受信した暗号化電子メールを復号化できます。
- **Decrypt and Flag**：安全な電子メール メッセージの復号化とフラグ設定を行うことができます。flag オプションを使用すると、エンドユーザーは暗号化に必要なフラグを設定できます。また、Cisco Secure Email Gateway によって電子メールが暗号化されてから電子メールがネットワークの外部に送信されます。フラグが設定されたメッセージを検出してサーバーで復号化できるようサーバーの設定を行う必要があります。
- **Decrypt and Encrypt**：安全な電子メール メッセージの暗号化と復号化を行うことができます。

Encryption Plug-in 構成ファイルの起動

エンド ユーザーは、Outlook 電子メール アカウントから、署名された BCE Config 添付ファイルを復号化することによって、Outlook 電子メール アカウントの暗号化を有効化したり設定することができます。エンドユーザーの受信トレイに添付ファイル付きの通知メールがない場合は、スパム メールまたは迷惑メールのフォルダを調べてください。

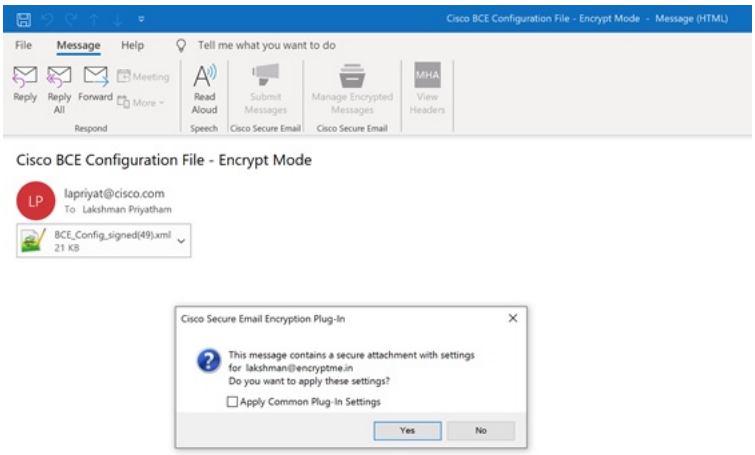
コンフィギュレーション ファイルを起動すると、署名された BCE Config 添付ファイル付きの通知メッセージを受信した電子メール アカウントにプラグインが設定されます。

（注） 通常は、プラグインのインストール時に Jave Runtime Environment（JRE）が自動的にインストールされます。ただし、これが実行されない場合は、JREを手動でインストールする必要があります。サポートされているバージョンは、JRE 1.8 または Open JRE 11 です。

Outlook 電子メールアカウントに対して Cisco Secure Email Encryption Plug-in を有効にして設定するには、次の手順を実行します。

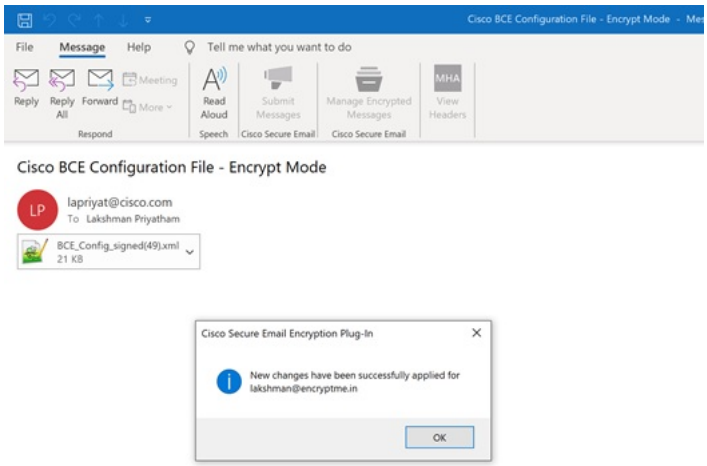
手順

ステップ 1 署名された BCE Config ファイルが添付された通知メール メッセージを開きます。設定の適用について確認を求めるメッセージが表示されます。



ステップ 2 [Yes] をクリックして、Cisco Secure Email Encryption Plug-in を設定します。設定が正常に適用されると、メッセージが表示されます。

[Apply Common Plug-in Setting] チェックボックスをオンにすると、プラグインの共通の設定も適用されます。共通のプラグインの設定については、BCE_Config ファイルを使用した共通オプションの設定 （41 ページ）を参照してください。



Flag 暗号化

Flag 暗号化オプションを使用すると、エンドユーザーは暗号化に必要なフラグを設定できます。また、Cisco Secure Email Gateway によって電子メールが暗号化されてから電子メールがネットワークの外部に送信されます。社内ネットワークから外部に発信されるメールに対してスパムやウイルスのスキャンが必要な場合は、Flag 暗号化方式を使用する必要があります。

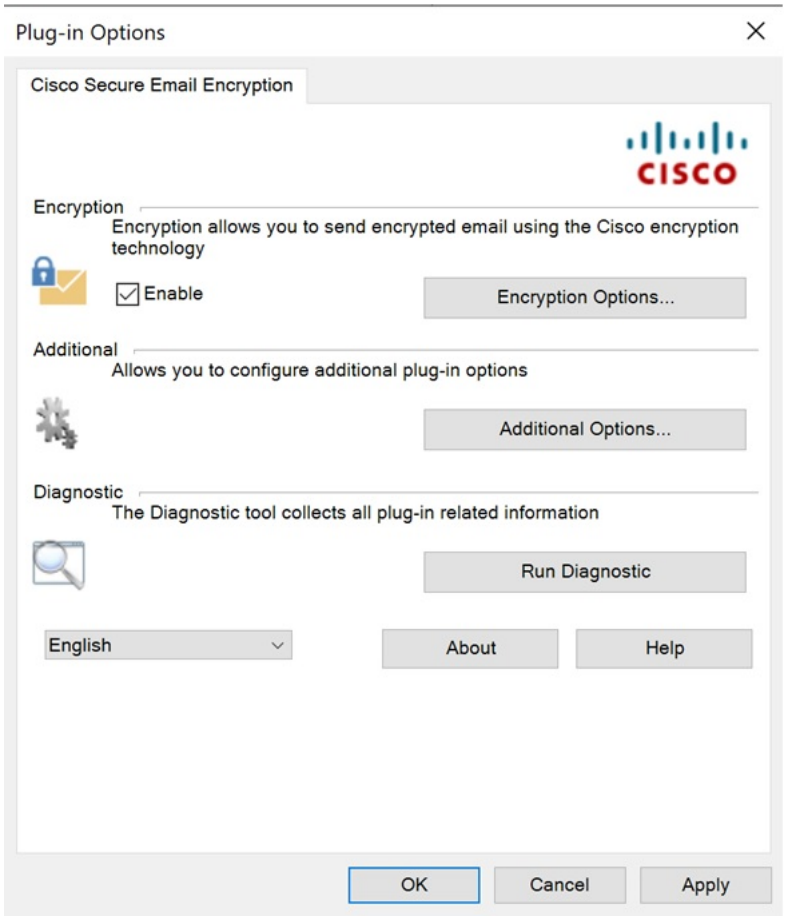
Flag 暗号化の設定は [Cisco Email Security Encryption] ページにあります。Flag 暗号化の設定を変更するには、次の手順を実行します。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、または [File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Encryption] > [Encryption Options] に移動します。
- Outlook 2007 では、ツールバーの [Plug-in Options] ボタンをクリックするか、または [Tools] > [Options] > [Cisco Email Encryption] > [Encryption Options] に移動します。

暗号化プラグインを有効または無効にするには、[Cisco Secure Email Encryption] タブで [Encryption] フィールドの [Enable] チェックボックスをオンまたはオフにします。

[Enable] をオンにすると、電子メールプログラムからセキュアエンベロープで機密メールを送信できます。

Cisco Secure Email Encryption の [Plug-in Options] ページ：

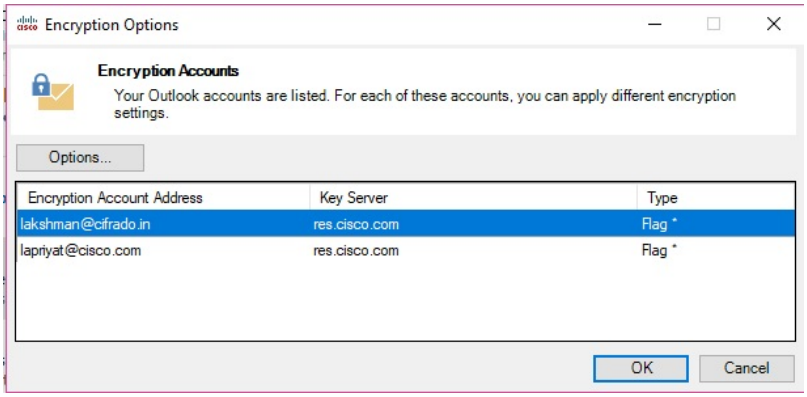


Flag 暗号化のオプション

[Encryption Options] をクリックすると、[Encryption Accounts] ページが表示されます。

[Encryption Accounts] ページには、Flag Encryption Plug-in のすべての電子メール ユーザー アカウントが表示されます。各行には、Outlook アカウントの電子メール アドレスと、それに関連付けられているキーサーバーおよび暗号化タイプ（Flag または Encrypt）が示されます。[Options] をクリックするか、アカウント アドレスをダブルクリックすると、[Encryption Options] ページが開きます。

[Encryption Accounts] ページ：



（注） Outlook の新規アカウントは [Encryption Accounts] リストに自動的に追加されます。Outlook アカウントが削除されると、そのアカウントは [Encryption Accounts] リストから自動的に削除されます。

Flag 暗号化された電子メールの送信オプション

エンドユーザーが送信電子メールを暗号化する場合に、暗号化対象として電子メールにマークを付ける、つまり「フラグを付ける」必要があります。これにより、管理者が作成したフィルタを使って暗号化が必要なメッセージを識別できます。

（注） 暗号化が必要な電子メールにフラグを設定するこの暗号化方式では、正しく機能するように電子メール フィルタを変更する必要がありますが、この変更は管理者だけが実行できます。

[Encrypt Message] ボタンは電子メールの作成時に使用できます。次のいずれかの方法で電子メールに暗号化のマークを設定できます。

[General] タブ

次の [General] のオプションから選択できます。

[General] のオプション	値
Flag Subject Text	暗号化の電子メールにフラグを設定するように発信電子メールの [Subject] フィールドに追加できるテキスト。[Subject] フィールドに追加するテキストを入力して、電子メールを暗号化する必要があることを示します（デフォルト値は [SEND SECURE]）。
Flag X-header name/value	暗号化対象として電子メールにフラグを付ける X ヘッダーを送信電子メールに追加できます。1 つめのフィールドに x ヘッダーを入力します（デフォルト値は *x-ironport-encrypt* です）。2 つめのフィールドに true または false を入力します。true を入力した場合、指定された x ヘッダーのメッセージが暗号化されます（デフォルト値は true です）。

[Connection] タブ

次の [Connection] のオプションから選択できます。

[Connection] のオプション	値
No proxy	プロキシを使用しない場合に選択します。
Use system proxy settings	デフォルトのシステム プロキシ設定を使用する場合に選択します。
Manual proxy configuration	特定のプロキシ設定を入力する場合に選択します。
Protocol	デフォルトの接続設定を使用しないことを選択した場合、[HTTP]、[SOCKS4]、[SOCKS4a]、[SOCKS5] のいずれかのプロトコルを選択します。
Host	システムまたはプロキシ サーバのホスト名または IP アドレスを指定します。
Port	システムまたはプロキシ サーバーのポートを指定します。
Username	サーバーでユーザー名が必要な場合に、ユーザー名を入力します。

[Connection] のオプション	値
Password	システムまたはプロキシ サーバーに対して入力したユーザー名に関連するパスワードを入力します。

[Remember Password] タブ

次の [Remember Password] のオプションから選択します。

パスワードのオプション	値
Never	このオプションを選択すると、電子メールを復号化または暗号化するときに、常に暗号化パスワードが必要になります。
Always	このオプションを選択すると、最初に電子メールを復号化または暗号化するときにのみ、暗号化パスワードが必要になります。パスワードはキャッシュされます。
Minutes	暗号化パスワードがキャッシュされるようにするには、このオプションをオンにします。パスワードを思い出すまでの分数を入力するか、矢印を使用して分数を変更します。指定した時間が経過すると、エンド ユーザーは、暗号化された電子メールを復号化する際に暗号化パスワードの再入力が必要になります。デフォルトは 1440 分です。

Desktop Encryption

デスクトップ暗号化オプションでは、Outlook 内から電子メールを暗号化し、それをデスクトップから送信できます。

Desktop Encryption 設定は [Cisco Email Security Encryption] ページにあります。Desktop Encryption の設定を変更するには、次の手順を実行します。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、または [File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Encryption] > [Encryption Options] に移動します。
- Outlook 2007 では、ツールバーの [Plug-in Options] ボタンをクリックするか、または [Tools] > [Options] > [Cisco Email Encryption] > [Encryption Options] に移動します。

エンドユーザーが暗号化プラグインを有効または無効にするには、[Cisco Secure Email Encryption] タブで [Encryption] フィールドの [Enable] チェックボックスをオンまたはオフにします。[Enable]

をオンにすると、電子メール プログラムからセキュア エンベロープで機密メールを送信できます。

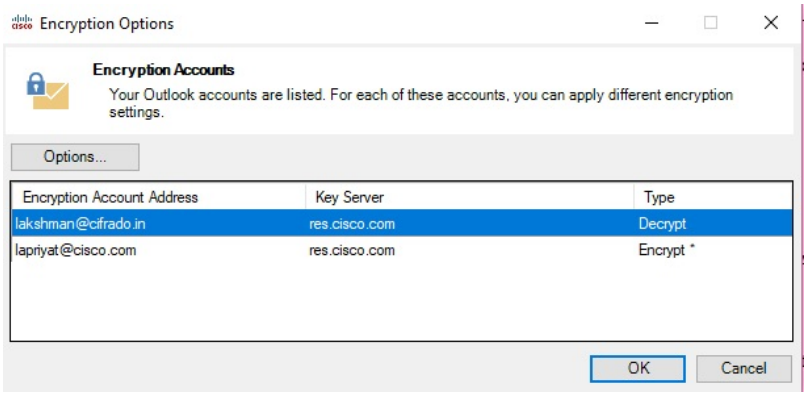
（注） エンドユーザーは [Cisco Secure Email Encryption] ページから暗号化プラグインを有効化/無効化できますが、暗号化モードに対する変更は、管理者が *BCE_config.xml* ファイルを使って行う必要があります。

デスクトップ暗号化のオプション

[Encryption Options] をクリックすると、[Encryption Accounts] ページが開きます。

[Encryption Accounts] ページには、Flag Encryption Plug-in のすべての電子メール ユーザー アカウントが表示されます。各行には、Outlook アカウントの電子メール アドレスと、それに関連付けられているキー サーバーおよび暗号化タイプ（Flag または Encrypt）が示されます。[Options] をクリックするか、アカウント アドレスをダブルクリックすると、[Encryption Options] ページが開きます。

[Encryption Accounts] ページ：



（注） Outlook の新規アカウントは [Encryption Accounts] リストに自動的に追加されます。Outlook アカウントが削除されると、そのアカウントは [Encryption Accounts] リストから自動的に削除されます。

[General] タブ

（注） 次の表に、[General] タブで使用できるすべてのオプションを示します。BCE_config.xml ファイルの設定によっては、表示されない、または使用できないオプションもあります。

次の [General] のオプションから選択します。

[General] のオプション	値
Use as default encryption account	アカウントを、デフォルトの暗号化アカウントとして設定する場合に選択します。
Encrypt by default	すべての送信電子メール メッセージをデフォルトで暗号化する場合に選択します。
Server URL	暗号化サーバの URL を入力します。
Always use message body from key server	プラグインが、各受信者のロケールセットに応じてメッセージ本文に使用する言語を判断できるようにします。このオプションは、同じロケールを使用する受信者に暗号化メッセージを送信する場合に使用します。このオプションをオフにすると、メッセージ本文は常に下のオプションで選択したデフォルトの言語を使用します。
Default language for outgoing messages	異なるロケールを使用する受信者へのメッセージを送信するときに、送信メッセージで使用する言語を指定します（すぐ上のチェックボックスがオンの場合）。 すべての送信メッセージで使用する言語を指定します（すぐ上のチェックボックスはオフになっています）。
Token File Name	トークンは、電子メール クライアントと暗号化サーバー間でデータを暗号化するために使用されるカスタマー固有のキーです。現在、この情報はカスタマー サポートでのみ使用され、変更できません。
Default Expiration (days)	暗号化された電子メールが有効な日数を指定します。有効期間の日数が経過すると、メッセージの有効期限が切れ、それ以降は受信者が開くことができなくなります。
Default read-by (days)	受信者が暗号化されたメッセージを読むことが予想される期間を日数で指定します。指定した期間内にメッセージが読まれなかった場合は、送信者に通知が送られます。
Attachment name	デフォルトのセキュアメッセージ名は *securedoc.html* です。添付ライフ名は変更でき、セキュアメッセージに指定した新しい名前が反映されます。

[General] のオプション	値
Message Security	暗号化した電子メールのセキュリティを設定します。デフォルト値は *BCE_Config.xml* ファイルに定義されています。 （注） ここで変更したメッセージセキュリティは、作成中のメッセージに対してのみ適用されます。 • [High（高）]：メッセージに高いセキュリティを指定した場合、暗号化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（中）]： メッセージに中程度のセキュリティを指定した場合、受信者のパスワードがキャッシュされていれば、メッセージを復号化する際でもパスワードは要求されません。 • [Low（低）]： メッセージに低いセキュリティを指定した場合、メッセージは安全に送信されますが、メッセージを復号化する際でもパスワードが要求されません。
Send return receipt	送信した電子メールを受信者が開封した際に返信確認メッセージを要求する場合に選択します。
Show dialog during message encryption	暗号化するメッセージごとに暗号化オプション ダイアログボックスを表示するには、このオプションをオンにします。

[Connection] タブ

次の [Connection] のオプションから選択できます。

[Connection] のオプション	値
No proxy	プロキシを使用しない場合に選択します。
Use system proxy settings	デフォルトのシステム プロキシ設定を使用する場合に選択します。
Manual proxy configuration	特定のプロキシ設定を入力する場合に選択します。

[Connection] のオプション	値
Protocol	デフォルトの接続設定を使用しないことを選択した場合、[HTTP]、[SOCKS4]、[SOCKS4a]、[SOCKS5] のいずれかのプロトコルを選択します。
Host	システムまたはプロキシ サーバのホスト名または IP アドレスを指定します。
Port	システムまたはプロキシ サーバーのポートを指定します。
Username	サーバーでユーザー名が必要な場合に、ユーザー名を入力します。
Password	システムまたはプロキシ サーバーに対して入力したユーザー名に関連するパスワードを入力します。

[Remember Password] タブ

次の [Remember Password] のオプションから選択します。

パスワードのオプション	値
Never	このオプションを選択すると、電子メールを復号化または暗号化するときに、常に暗号化パスワードが必要になります。
Always	このオプションを選択すると、最初に電子メールを復号化または暗号化するときにのみ、暗号化パスワードが必要になります。パスワードはキャッシュされます。
Minutes	暗号化パスワードがキャッシュされるようにするには、このオプションをオンにします。パスワードを思い出すまでの分数を入力するか、矢印を使用して分数を変更します。指定した時間が経過すると、エンド ユーザーは、暗号化された電子メールを復号化する際に暗号化パスワードの再入力が必要になります。デフォルトは 1440 分です。

[Advanced] タブ

（注） 次の表に、[General] タブで使用できるすべてのオプションを示します。BCE_config.xml ファイルの設定によっては、表示されない、または使用できないオプションもあります。

次の [Advanced] のオプションから選択します。

[Advanced] のオプション	値
Unsecure server URL	メッセージ バーのヘルプで使用する、セキュリティで保護されていないURL。このオプションを省略した場合は、外部のセキュア URL（http://res.cisco.com） が使用されます。
Connection timeout	キー サーバへの接続が確立されるまでの待機時間。
Socket timeout	キー サーバーからのデータを待機する時間の長さ。
Display "Open offline" check box	このオプションを選択すると、セキュアメッセージに [Open offline] チェックボックスが表示されます。
Display "Remember envelope key"	このオプションを選択すると、セキュアメッセージに [Remember envelope key] チェックボックスが表示されます。
Display "Enable personal security phrase"	このオプションを選択すると、セキュアメッセージに [Enable personal security phrase] チェックボックスが表示されます。
Add message bar	セキュア メッセージにメッセージ バーを追加する場合に選択します。
Show "Reply" button in the message bar	メッセージバーが有効になっている場合、メッセージ バーに [Reply] が表示されます。
Show "Forward" button in the message bar	メッセージバーが有効になっている場合、メッセージ バーに [Forward] が表示されます。
Show "Reply to All" button in the message bar	メッセージバーが有効になっている場合、メッセージ バーに [Reply to All] が表示されます。
Display "Remember me"	このオプションを選択すると、セキュアメッセージに [Remember me] チェックボックスが表示されます。

[Advanced] のオプション	値
Display "Auto open"	このオプションを選択すると、セキュアメッセージに [Auto open] チェックボックスが表示されます。
Open in the same window	セキュアメッセージと同じウィンドウでセキュア メッセージを開く場合に選択します。
Display “Encryption usage reminder”	このオプションを選択すると、ユーザーが暗号化を実行するたびに、ビジネス目的でのみ暗号化を使用するというリマインダが表示されます。

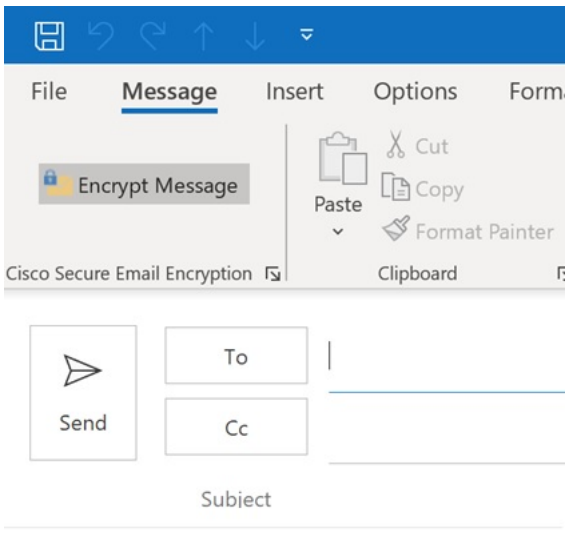
暗号化された電子メールの送信

（注） 暗号化電子メールのデフォルトの最大サイズは7MBですが、この値は管理者が *BCE_Config.xml* ファイルを使って変更できます（最大 25 MB）。

エンド ユーザーは電子メールの作成時に [Encrypt Message] ボタンをクリックすることで、電子メールを安全に送信することができます。セキュアメッセージを送信する前に、[Encrypt Message] ボタンがオンになっていることを確認してください。

[Encrypt Message] ボタンは電子メールの作成時に使用できます。

次の図に、[Mail Compose] ページの [Encrypt Message] ボタンと [Encryption Mail Options] トグルボタンを示します。



暗号化されたメッセージを送信するには、キーサーバーを選択してパスワードを入力します。

暗号化オプションを設定するには、右下隅の [Cisco Secure Email Encryption] ランチャをクリックして次の [Encryption Mail Options] ページを表示します。

（注） 次のスクリーンショットと表に [Encryption Mail Options] のオプションのすべてを示します。ただし、表示されるオプションは *BCE_config.xml* ファイルの設定に応じて異なります。

（注） [Encryption Mail Options] を変更した場合、その変更は作成中の電子メール メッセージにのみ適用されます。

次のメール オプションから選択します。

[Encryption Mail Options]	説明
Allow Reply	このオプションを選択すると、受信者は暗号化電子メールに返信できるようになり、返信の電子メール メッセージが自動的に暗号化されます。
Allow Reply All	このオプションを選択すると、受信者は暗号化電子メールを受信した全員に返信できるようになり、返信の電子メール メッセージが自動的に暗号化されます。
Allow Forward	このオプションを選択すると、受信者は暗号化電子メールを転送できるようになり、転送する電子メール メッセージが自動的に暗号化されます。

[Encryption Mail Options]	説明
Message Security	暗号化した電子メールのセキュリティを設定します。デフォルト値は *BCE_Config.xml* ファイルに定義されています。 （注） ここで変更したメッセージセキュリティは、作成中のメッセージに対してのみ適用されます。 • [High（高）]：メッセージに高いセキュリティを指定した場合、暗号化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（中）]： メッセージに中程度のセキュリティを指定した場合、受信者のパスワードがキャッシュされていれば、メッセージを復号化する際でもパスワードは要求されません。 • [Low（低）]：メッセージに低いセキュリティを指定した場合、メッセージは安全に送信されますが、メッセージを復号化する際でもパスワードが要求されません。
Expiration	ドロップダウンから、暗号化されたメールの有効期間（日時）を指定します。この有効期間が過ぎると、メッセージは期限切れとなり、それ以降は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。
Read By	ドロップダウンから、受信者が暗号化メッセージを読むと予想される期間（日時）を指定します。指定した期間内にメッセージが読まれなかった場合は、送信者に通知が送られます。

このオプションが無効になっていない場合は、エンドユーザーが [Send] をクリックすると、セキュアエンベロープのオプションの設定 （61 ページ）に示すような [Secure Envelope Options] ページが開きます。

設定を誤るとエラーが発生することがあります。詳細については、エラーとトラブルシューティング （74 ページ）を参照してください。

返信オプションの伝播

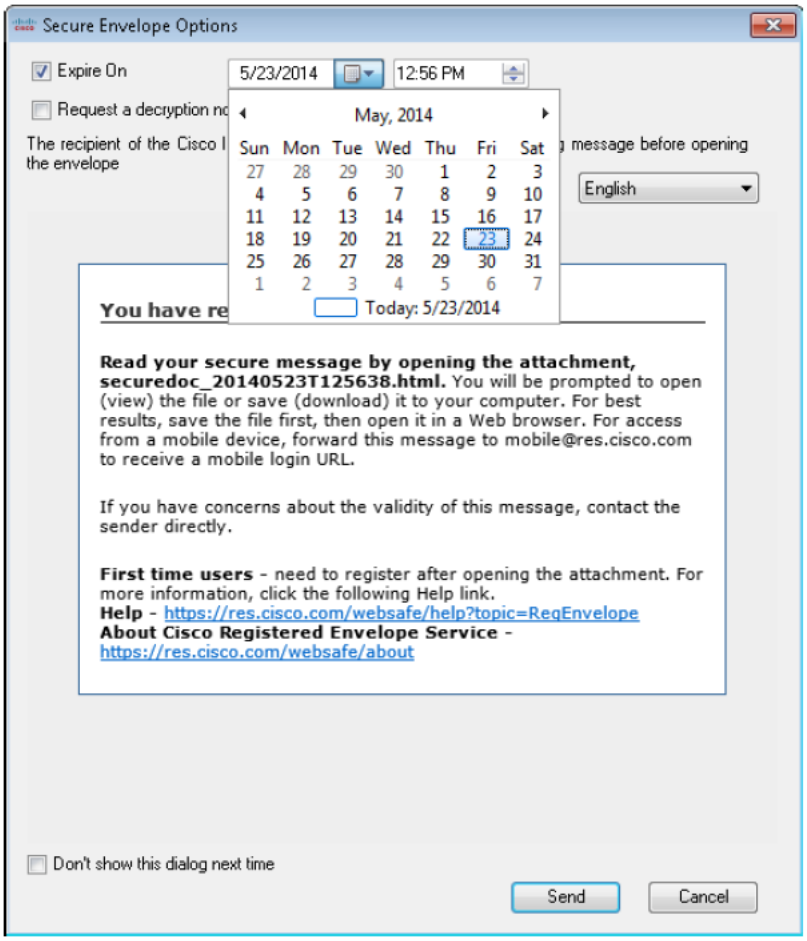
メッセージを復号化すると、[Reply]、[Reply All]、または [Forward] オプションのすべての設定と [Message Sensitivity] オプションのすべての設定が元のメッセージから継承されます。これらは変更できません。次に例を示します。

- デフォルトでは、メッセージは返信または転送される際に暗号化されます。
- [Reply]、[Reply All]、または [Forward] オプションを元のメッセージから継承できない場合は、返信メッセージや転送メッセージを送信できず、エンド ユーザーが [Send] をクリックするとそのことが通知されます。
- エンド ユーザーが [Reply]、[Reply All]、または [Forward] オプションを実行しているときは、元のメッセージに含まれている受信者を削除できません。
- エンド ユーザーが [Reply]、[Reply All]、または [Forward] オプションを実行しているときは、元のメッセージに含まれていない受信者を追加できません。
- エンド ユーザーが [Reply]、[Reply All]、または [Forward] オプションを実行しているときは、[To]、[Cc]、または [Bcc] フィールド間で受信者を混在させたり、移動することはできません。
- アカウントが [Decrypt Only] または [Flag Encrypt] に設定されている場合は、返信メッセージや転送メッセージを送信できず、エンド ユーザーが [Send] をクリックするとそのことが通知されます。
- アカウントの [Message Sensitivity] を [High] に設定すると、[Reply]、[Reply All]、または [Forward] のメッセージの機密性も [High] になります。
- アカウントの [Message Sensitivity] を [Medium] に設定すると、[Reply]、[Reply All]、または [Forward] のメッセージの機密性も [Medium] になります。
- アカウントの [Message Sensitivity] を [Low] に設定すると、[Reply]、[Reply All]、または [Forward] のメッセージの機密性も [Low] になります。
- [Reply]、[Reply All]、または [Forward] のメッセージは [Sent Items] フォルダに保存され、送信者によって復号化できます。
- 署名された BCE Config ファイルが含まれているメッセージを他のエンド ユーザーに転送すると、管理者から受け取る場合とは異なり、自動設定が機能せず、エラーが返されます。

セキュアエンベロープのオプションの設定

エンドユーザーは、次のスクリーンショットに示されているように、以下の表に記載されているセキュアエンベロープのオプションを設定できます。

（注） 設定によっては、画面に言語オプションが表示されないことがあります。また、通知の言語は受信者の設定に応じて選択されます。



セキュア エンベロープのオプション	説明
Expire on	このオプションを有効にする場合に選択します。暗号化電子メールが期限切れになる日時を指定します。その日時を過ぎるとメッセージは期限切れとなり、以降、受信者はそのメッセージを開くことができなくなります。日時は送信者のローカル タイム ゾーンに表示されます。
Request a Decryption Notification	送信者がメッセージの復号化通知を要求できるようになります。暗号化されたメッセージが開封されると、送信者に通知が送られます。
Language	通知テキストで使用する言語を選択します。ドロップダウンリストから言語を選択すると、その言語で受信者通知が表示されるようになります。

エンド ユーザーのアカウントに Flag 暗号化が設定されている場合は、組織から送信される前に、電子メールに暗号化のフラグが設定されます。エンドユーザーのアカウントにデスクトップ暗号化が設定されている場合、電子メールは、Exchange Server に送信される前に、デスクトップで暗号化されます。

セキュア メッセージの管理

エンド ユーザーは次の 2 つの方法でセキュア メッセージを管理できます。

- [Manage Secure Messages] ダイアログを使用して、選択したメッセージを管理します。このダイアログを使用して、送信した暗号化メールの有効期限をロック、ロック解除、または更新します。
- [メッセージの管理] ダイアログを使って、選択したアカウントから送信されたすべてのメッセージを管理します。このダイアログを使用して特定のメッセージを検索します。

セキュア メッセージを管理するこれらの2つの方法については、次のセクションで説明しています。エンドユーザーはいずれかの方法を使用して、送信した暗号化メールについて以下のことを実行できます。

- **電子メールのロック**。エンドユーザーは、以前に送信した暗号化電子メールをロックできます。また、ロックの理由を設定したり、メッセージがすでにロックされている場合はロックの理由を更新できます。受信者はロックされた電子メールを開くことができなくなります。
- **電子メールのロック解除**。エンドユーザーは、以前に送信した暗号化電子メールのロックを解除できます。これによって、受信者はその電子メールを復号化できるようになります。
- **有効期限の更新**。エンド ユーザーは、送信した暗号化電子メールに対して有効期限を設定、更新、クリアすることができます。暗号化された電子メールが期限切れになると、受信者はその電子メールを復号化できなくなります。

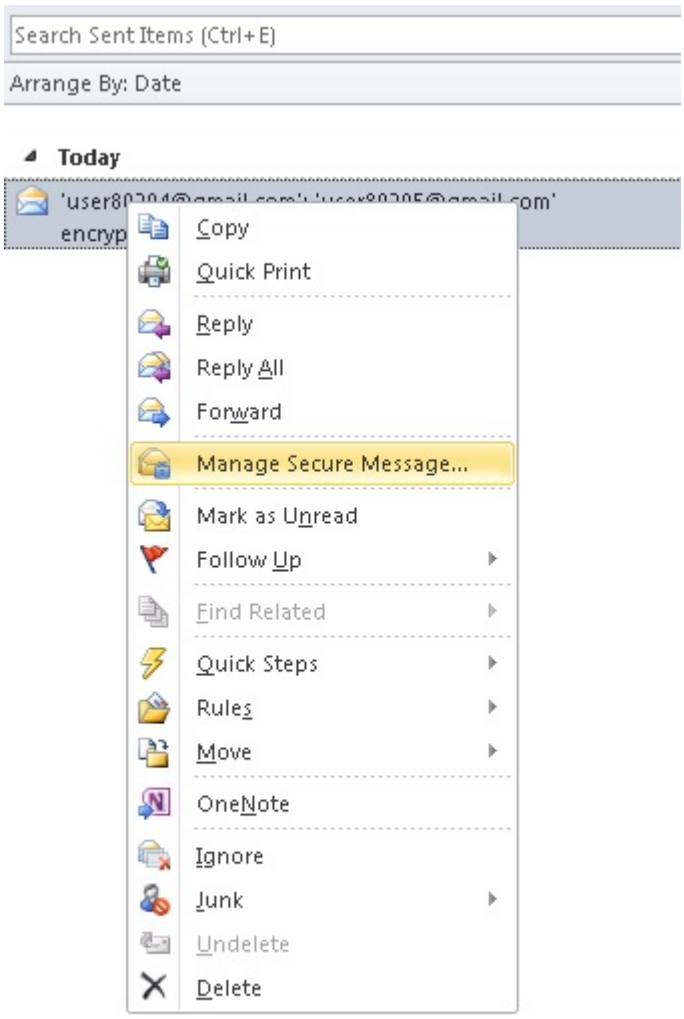
[Manage Secure Messages] ダイアログの使用

手順

ステップ 1 変更する送信済みの暗号化電子メールを選択し、その電子メールを右クリックして [Manage Secure Messages] メニュー オプションを表示します。

（注） また、エンド ユーザーは、暗号化された電子メールを復号化するときに [Manage Secure Messages] メニューにアクセスできます。エンド ユーザーが変更対象の電子メールの送信者である場合は、ツールバーに [Manage Secure Messages] ボタンが表示されます。ツールバーから [Manage Secure Messages] メニューにアクセスした場合は、同時に 1 つのメッセージにのみ有効期限の設定を適用できます。

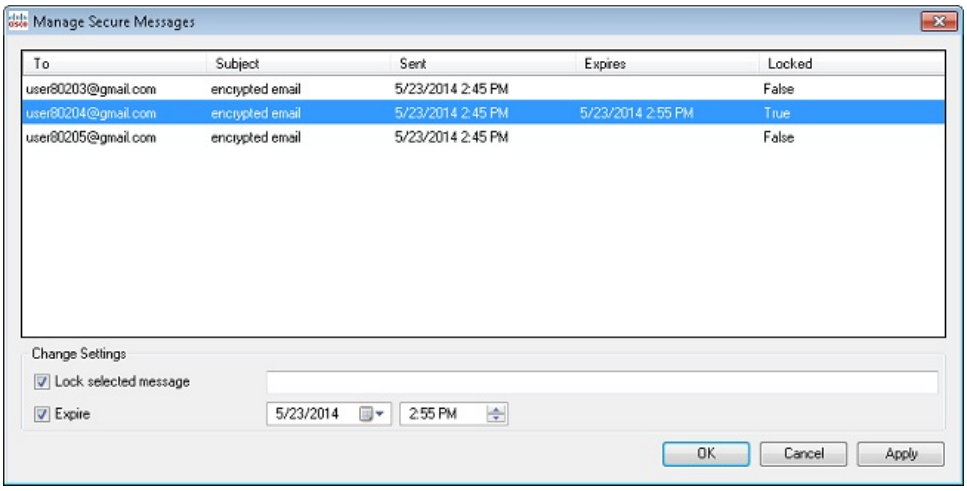
[Manage Secure Messages] メニューのオプション：



ステップ 2 [Manage Secure Messages] を選択します。

パスワードがキャッシュされていない場合は、パスワードの入力が求められます。

[Manage Secure Messages] ページが表示されます。



ステップ 3 受信者ごとにロックまたは有効期限のオプションを設定するには、送信した暗号化電子メールメッセージを 1 つ以上選択して [Lock] または [Expire] チェックボックスをオンにして、適切な情報を入力します。

（注） ツールバーまたはリボンから [Manage Secure Messages] メニューにアクセスした場合は、次のセクションに記載されているように、有効期限の設定は一度に 1 つのメッセージにしか適用できません。

[Manage Messages] ダイアログの使用

手順

ステップ 1 リボン（Outlook 2010/13 の場合）またはツールバー（Outlook 2007 の場合）の [Manage Messages] ボタンをクリックします。

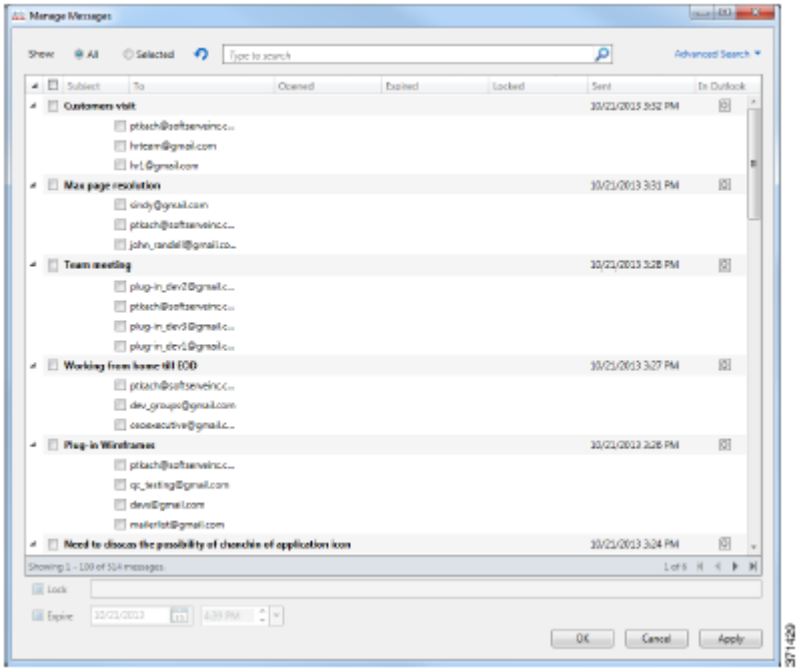
[Manage Messages] ダイアログが開きます。

（注） エンドユーザーはこのインターフェイスを使用して、送信したすべての暗号化メッセージを管理することができます。インターネット接続が遅く、多数の暗号化メッセージがある場合は、ロードのプロセスに数分かかることがあります。

ステップ 2 特定のメッセージを検索するには、[Basic Search] または [Advanced Search] をクリックします。

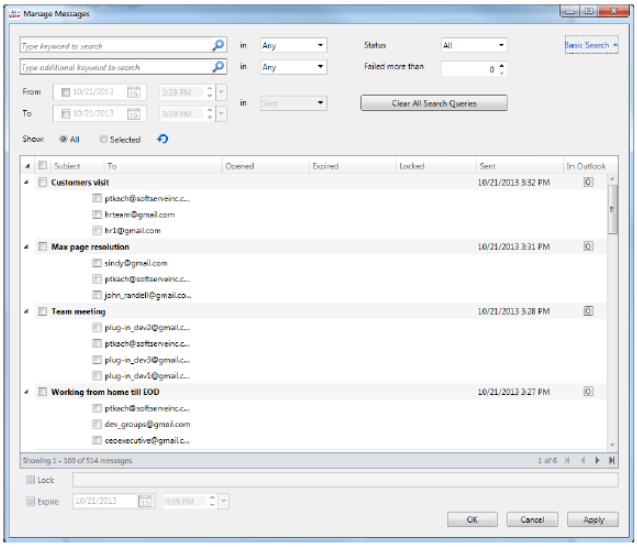
ステップ 3 基本の検索を実行するには、次の画面の [To] フィールドと [Subject] フィールドに検索するキーワードを入力します。

文字列の最大長は 500 です。



ステップ 4 高度な検索を実行するには、次の画面で以下の検索パラメータを 1 つ以上設定します。

- [Keyword 1]：この文字列を使用して、[To] フィールドまたは [Subject] フィールドにキーワードが含まれているメッセージを検索します。キーワードの最大長は 500 文字です。
- [Keyword 2]：[Keyword 1] と同じように使用します。両方のキーワードを指定すると、キーワードが 2 つとも含まれているメッセージを照合して検索が実行されます。
- [In]（キーワードの検索用）：[To]、[Subject]、または [Locked Reason] フィールドでキーワードの検索を行うかどうかを指定します。
- [Failed more than]：このオプションを使用すると、失敗した試行回数に基づいて検索が実行されます。結果として表示されるメッセージには、指定した値を超えた、メールが失敗した試行回数が含められます。最大値は 10 です。
- [Status]：このオプションを使用すると、[All]、[Unopened]、[Opened]、[Locked]、および [Expired] のいずれかのステータスの設定に基づいて検索を実行します。
- [From/To]：このオプションを使用すると、日付と時間の間隔に基づいて検索が実行されます。[From] の日付のみを設定した場合は、選択した日付より後に送信されたメッセージに対して検索が行われます。[To] の日付のみを設定した場合は、選択した日付より前に送信されたメッセージに対して検索が行われます。両方の日付を設定した場合は、選択した 2 つの日付の間に送信されたメッセージに対して検索が行われます。日付を設定するには、ドロップダウンのカレンダーを使用するか、または手動で日付を入力します。デフォルトの日付は現在の日時ですが、日付による検索はデフォルトで無効になっています。
- [In]（日付の検索用）：日付関係の検索の基準を指定します。使用できるオプションは [Sent]、[Opened]、および [Expired] です。



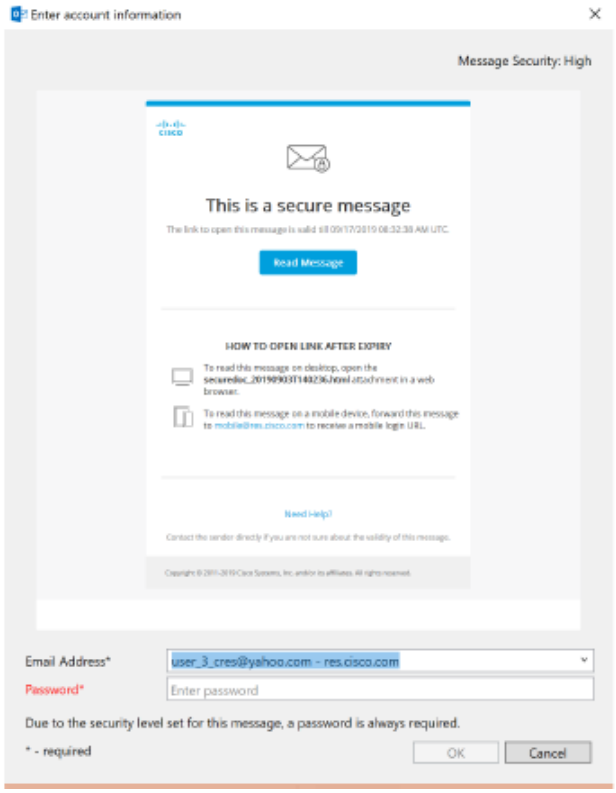
ステップ 5 [OK] をクリックします。

安全な電子メールの受信と返信

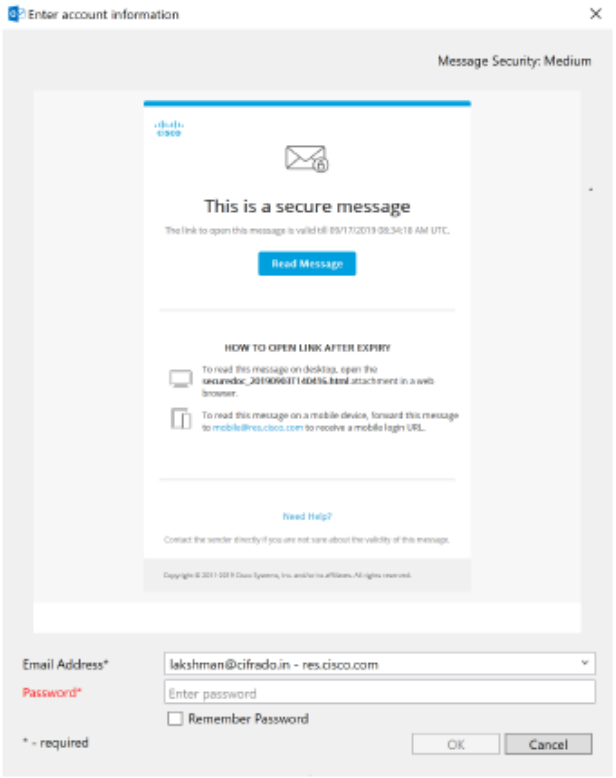
デスクトップ暗号化プラグインは安全な電子メールを自動的に検出し、Outlook 内でそれらの復号化を試みます。エンドユーザーが暗号化されたメッセージを受信した場合は、通常、エンベロープを開封するために暗号化パスワードを入力する必要があります。セキュアメッセージには、[High]、[Medium]、または [Low] のメッセージ セキュリティを設定できます。

（注） パスワードで保護されたセキュリティメッセージを受信した場合、エンドユーザーは、そのメッセージを開封するために、Cisco Secure Email Encryption Service にユーザーアカウントを登録して設定しなければならないことがあります。サービスに登録すると、アカウントパスワードを使用して、受信するすべての登録済みエンベロープを開封できます。詳細については、安全な返信/すべてに返信/転送 （71 ページ）を参照してください。

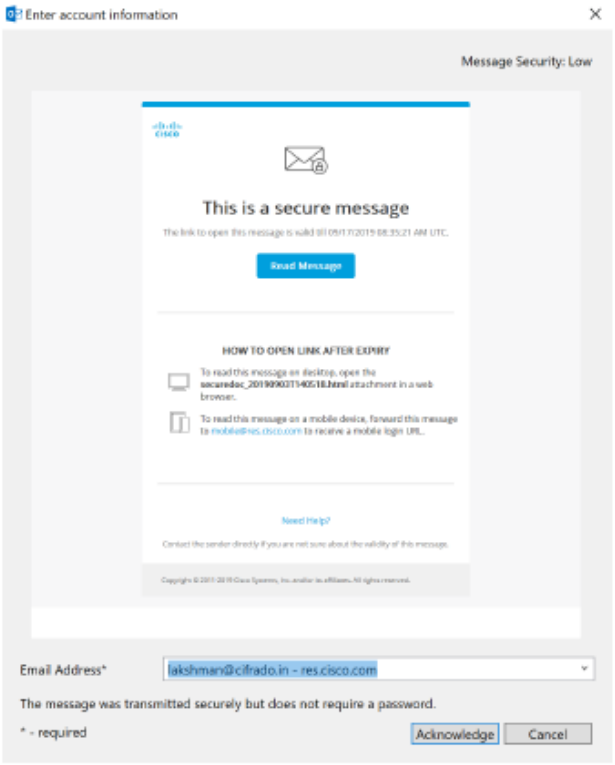
[Message Encryption High] ページ：



[Message Encryption Medium] ページ



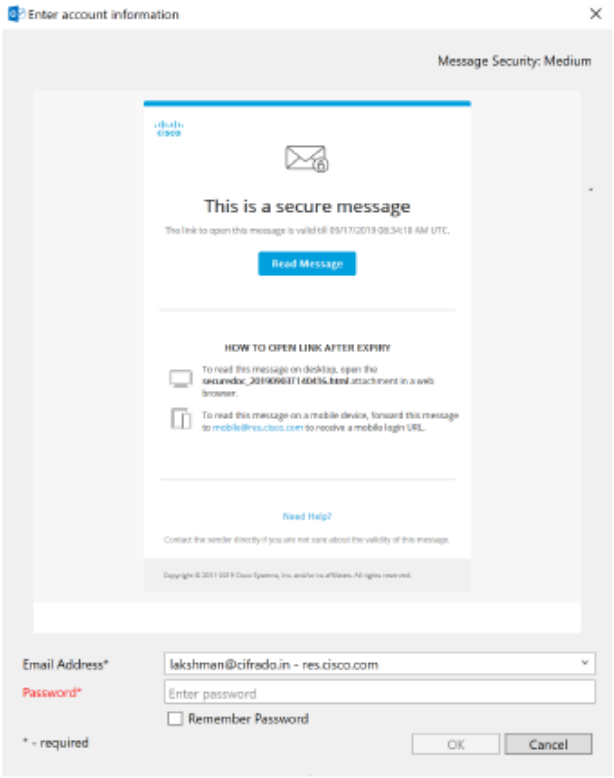
[Message Encryption Low] ページ：



次の表は、メッセージ セキュリティのオプションを示しています。

メッセージ セキュリティのオプション	説明
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る場合は、その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。

エンドユーザーがロックされた（または期限切れの）セキュアメッセージを受信すると、そのことを通知するメッセージが [Message Security] ページに赤い文字で表示されます。



安全な返信/すべてに返信/転送

Desktop Encryption または Decrypt Only モードを使用している場合に、暗号化されたメールに返信したり、転送したりすると、返信はデフォルトで自動的に暗号化されます。Flag 暗号化を使用している場合は、Cisco Secure Email Gateway によって応答メッセージが暗号化されます。セキュアメッセージの設定は、ユーザーが次のアクションを実行できるかどうかによって判断されます。

- 安全な返信
- 全員への安全な返信
- 安全な転送

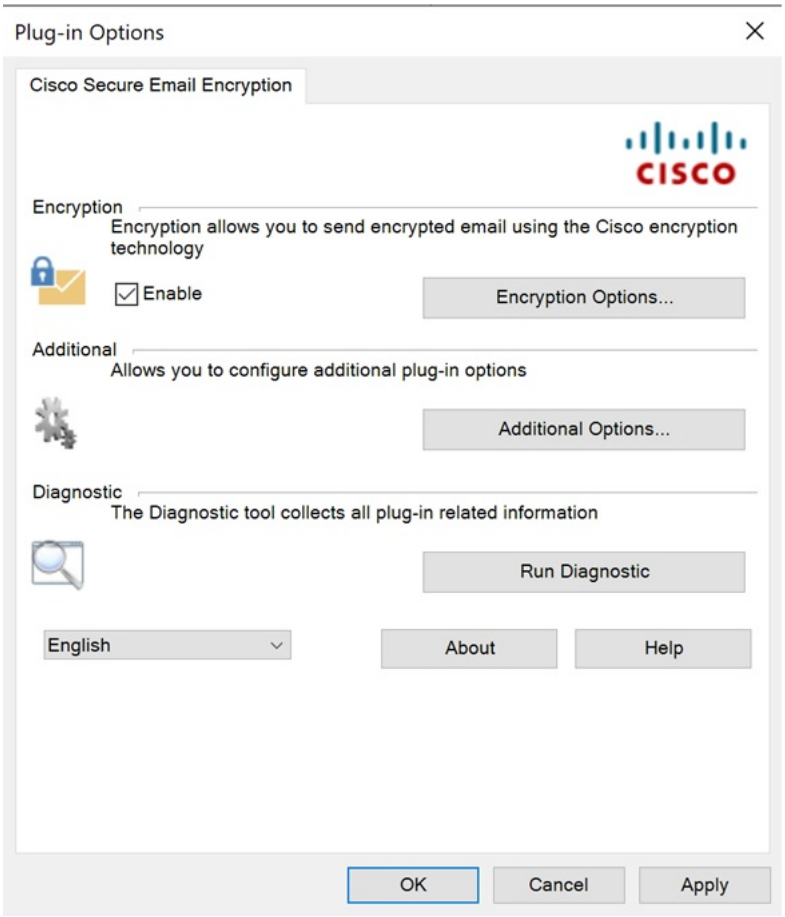
追加設定の変更

ログファイルには、すべての発生したアクションが記録されリスト化されています。

追加のオプションは [Cisco Secure Email Encryption] ページにあります。追加のオプションを変更するには、次の手順を実行します。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Encryption] > [Additional Options] を選択します。
- Outlook 2007 では、ツールバーの [Plug-in Options] ボタンをクリックするか、[Tools] > [Options] > [Cisco Email Encryption] > [Additional Options] を選択します。

Cisco Secure Email Encryption の [Plug-in Options] ページ：



[Encryption Additional Options] ページでは、次のタイプのオプションを設定することができます。これは以降のセクションで説明しています。

- Logging
- Sending Usage Data
- Privacy

[Logging] タブ

エンド ユーザーは [Logging] タブで次のオプションを設定できます。

オプション	説明
Enable Logging	Cisco Secure Email Encryption Plug-in のロギングを有効にする場合に選択します。
Log file name	ログ ファイルの名前を指定します。このファイルは %ALLUSERSPROFILE%\Cisco\Cisco Email Encryption Plug-in\<*username*> に保存されます。ログ ファイル名の最後には、.log 拡張子を付ける必要があります。
Log level	次のいずれかを選択します。 • [Normal] ：このオプションはデフォルトで有効になっています。標準ログには致命的なエラー、回復可能なエラー、警告が含まれます。 • [Extended]：ロギングを拡張すると、標準のロギングメッセージに加えて、役立つ情報とデバッグロギングメッセージも有効になります。 特定の状況に必要なトラブルシューティングのレベルに基づいてログ レベルを変更できます。たとえば、Cisco Secure Email Encryption Plug-in で問題が発生した場合、ロギングレベルが [Extended] に設定されていると、開発者に対して可能な限りの情報を提供し、問題の再現と診断に役立ちます。

[Sending Usage Data] タブ

エンド ユーザは [使用データの送信（Sending Usage Data）] タブで次のオプションを設定できます。

オプション	説明
Send anonymous usage data to Cisco	Cisco Secure Email Encryption Plug-in で、製品の改善に使用するためのデータを収集することができます。次の 2 つのタイプの情報が収集され、分析のためにCiscoサーバーに保存されます。 • プラグインを実行しているマシンに関する一般情報 • アカウント固有の情報

[Privacy] タブ

エンド ユーザは [プライバシー（Privacy）] タブで次のオプションを設定できます。

オプション	説明
Resets Identifier	使用状況レポートの関連付けに使用する ID をリセットします。
Clear All Passwords	すべてのアカウントのキャッシュされているすべてのパスワードをクリアします。

エラーとトラブルシューティング

この項では、Cisco Secure Email Encryption Plug-in for Outlook の使用中に発生する可能性がある一般的なエラーと、それらを解決するためのトラブルシューティングを説明します。

（注） 同じエラーメッセージを複数回受け取り、そのエラーによって Cisco Secure Email Encryption Plug-in が機能しなくなった場合、エンドユーザーは修復プロセスを実行できます。Cisco Secure Email Encryption Plug-in for Outlook ファイルの修復 （77 ページ）を参照してください。修復プロセスを実行しても同じエラーが発生する場合は、手順に従って診断ツールを使用し、シスコにフィードバックしてください。Cisco Secure Email Encryption 診断ツールの実行 （78 ページ）を参照してください。

Outlook 起動エラー

コンフィギュレーション ファイルの初期化中に発生するエラー

Outlook の起動時に次のメッセージが表示されることがあります。

- *An error occurred during <file_name> configuration file initialization. Some settings have been set to the default values.*
- *Config validation for account <account_address> has failed. Please set the correct configuration values or contact your administrator.*

これらのエラーメッセージは、一部の設定値が無効な場合や、%ALLUSERSPROFILE%\Cisco\Cisco Email Encryption Plug-In\<*username*>フォルダで一部の構成ファイルが破損している場合に表示されます。

解決策

Cisco Secure Email Encryption Plug-in は、破損した構成ファイルに含まれている一部の暗号化オプションのデフォルト値を復元しません。代わりに、一部の暗号化機能をオフにします。エ

ラー メッセージが繰り返し表示される場合は、修復プロセスを実行してコンフィギュレーション ファイルを修正してください。Cisco Secure Email Encryption Plug-in for Outlook ファイルの修復 （77 ページ） を参照してください。

コンフィギュレーション ファイルが見つからない

Outlook の起動時に次のエラー メッセージが表示されることがあります。

- *<file_name> configuration file was not found. Settings have been set to the default values.*

解決策

Cisco Secure Email Encryption Plug-in は、破損した構成 ファイルに含まれている一部の暗号化オプションのデフォルト値を復元しません。代わりに、暗号化モードを設定します。エラー メッセージが繰り返し表示される場合は、修復プロセスを実行してコンフィギュレーション ファイルを修正してください。Cisco Secure Email Encryption Plug-in for Outlook ファイルの修復（77 ページ） を参照してください。

復号化および暗号化に関するエラー

オプションを無効にしていない場合は、[Send] をクリックすると [Secure Message Options] ページが表示されます。電子メール アカウントで次のようなステータス メッセージを受信することがあります。

暗号化オプションが無効になっている場合

発生した接続の問題が修正されも [Encryption Options] が無効になっている場合は、Outlook を再起動してください。Outlookを再起動しても解決しない場合は、管理者に問い合わせてください。

アカウントがロックされている場合

- *Your account has been locked. Please contact your account administrator for more information.*

解決策

システム管理者に電子メール アカウントのロック解除を依頼してください。

アカウントがブロックされている場合

- *Your account has been blocked and you must reset your password. Please use the forgot password link to reactivate your account.*パスワードを忘れた場合

解決策

パスワードリンクをクリックして、パスワードセキュリティの確認用の質問に正しく回答し、パスワードをリセットしてください。

アカウントが一時停止された場合

- *You have no attempts remaining. Your account is locked for the next 15 minutes.*

解決策

後で https://res.cisco.com/websafe/ にログインを試みるか、サポート（https://res.cisco.com/websafe/help?topic=ContactSupport）に連絡してサポートを受けることができます。

受信者が未設定

送信する電子メールに受信者が記入されていない場合、次のメッセージを受け取ることがあります。

- *An error occurred during encryption: no recipients specified.*

復号化中にエラーが発生

メッセージの復号化中に予期しないエラーが発生しました。たとえば、SDKによって不明なエラー コードを返されたり、プラグインによって例外が報告されます。

- An error occurred during decryption.

解決策

診断ツールを実行して、サポート チームに診断レポートを送信してください。Cisco Secure Email Encryption 診断ツールの実行 （78 ページ） を参照してください。

暗号化中にエラーが発生

メッセージの暗号中に予期しないエラーが発生しました。たとえば、SDK によって不明なエラー コードを返されたり、プラグインによって例外が報告されます。

- An error occurred during encryption.

解決策

診断ツールを実行して、サポート チームに診断レポートを送信してください。Cisco Secure Email Encryption 診断ツールの実行 （78 ページ） を参照してください。

上限を超過

暗号化電子メールのデフォルトの最大サイズは7MBですが、この値は管理者がBCE_Config.xmlファイルを使って変更できます（最大25MB）。暗号化電子メールが最大値を超えている場合は、次のいずれかのメッセージを受け取ります。

- *This message exceeds the allowable limit and cannot be decrypted.*
- *This message exceeds the allowable limit and cannot be encrypted.*

- *An error occurred during encryption: an invalid attachment found.*
- *Failed to report this message. This message is too large.*
- *Failed to report {0} messages. {0} messages are too large.*

（注） 「Failed to report ...」で始まる最後の 2 つのメッセージは、現在は英語のみです。

Cisco Secure Email Encryption Plug-in for Outlook ファイルの修復

Cisco Secure Email Encryption Plug-in を修復するには、次の手順を実行します。

手順

ステップ 1 Outlook が終了していることを確認します。

ステップ 2 [Control Panel] > [Add or Remove Programs] を選択します。

ステップ 3 プログラムの一覧で [Cisco Secure Email Encryption Plug-in] を見つけて、[Uninstall/Change] をクリックします。

ステップ 4 [Repair] をクリックします。インストーラの修復プロセスが実行されます。

（注） 暗号化の設定は復元したり修正したりできません。暗号化の設定は、管理者のみが *BCE_Config.xml* ファイルを使って送信できます。

ステップ 5 エラーの原因になったアクションを実行します。修復プロセスの実行後も同じエラーが発生する場合、診断ツールを使用してシスコにフィードバックする手順を実行してください。Cisco Secure Email Encryption 診断ツールの実行 （78 ページ） を参照してください。

診断ツールを使用したトラブルシューティング

Cisco Secure Email Encryption Plug-in には、問題のトラブルシューティング時にシスコのサポートを支援する診断ツールが用意されています。診断ツールを使ってプラグイン ツールから重要なデータを収集し、それらをシスコ サポートに送ると問題の解決に役立ちます。

エラーが発生した場合や修復手順では解決できない Cisco Secure Email Encryption Plug-in に関する問題が発生した場合、エンドユーザーは診断ツールを使用できます。また、診断ツールを使用すると、不具合の報告時にシスコのエンジニアと重要情報を共有することもできます。

Cisco Secure Email Encryption Plug-in for Outlook ファイルの修復 （77 ページ）またはCisco Secure Email Encryption 診断ツールの実行 （78 ページ）を参照してください。

（注） エラーが発生した場合は、エラーとトラブルシューティング （74 ページ） のトラブルシューティングのヒントを参照してください。

Cisco Secure Email Encryption 診断ツールにより収集されるデータ

診断ツールは、ご使用のコンピュータから次の情報を収集します。

- 一部の COM コンポーネントに関する登録情報
- 環境変数
- Cisco Secure Email Encryption Plug-in 出力ファイル
- Windows および Outlook に関する情報
- システム ユーザ名および PC 名
- 他の Outlook プラグインに関する情報
- Outlook に関連する Windows イベント ログのエントリ

Cisco Secure Email Encryption 診断ツールの実行

Cisco Email Encryption 診断ツールは、次のいずれかの場所から実行できます。

- **Cisco Secure Email Encryption の [Options] タブから**。通常は、Cisco Secure Email Encryption の [Options] タブから診断ツールを実行します。
- 「Program Files\ Cisco Email Encryption Plug-in」フォルダ（通常は C:\Program Files\Cisco\Cisco Email Encryption Plug-in）から。これは、Cisco Email Encryption Plug-in がインストールされているフォルダです。
- [Start] メニュー > [All Programs] > [Cisco Email Encryption Plug-in] > [Cisco Email Encryption Plug-in Diagnostic] から。

Outlook の [Options] ページからの診断ツールの実行

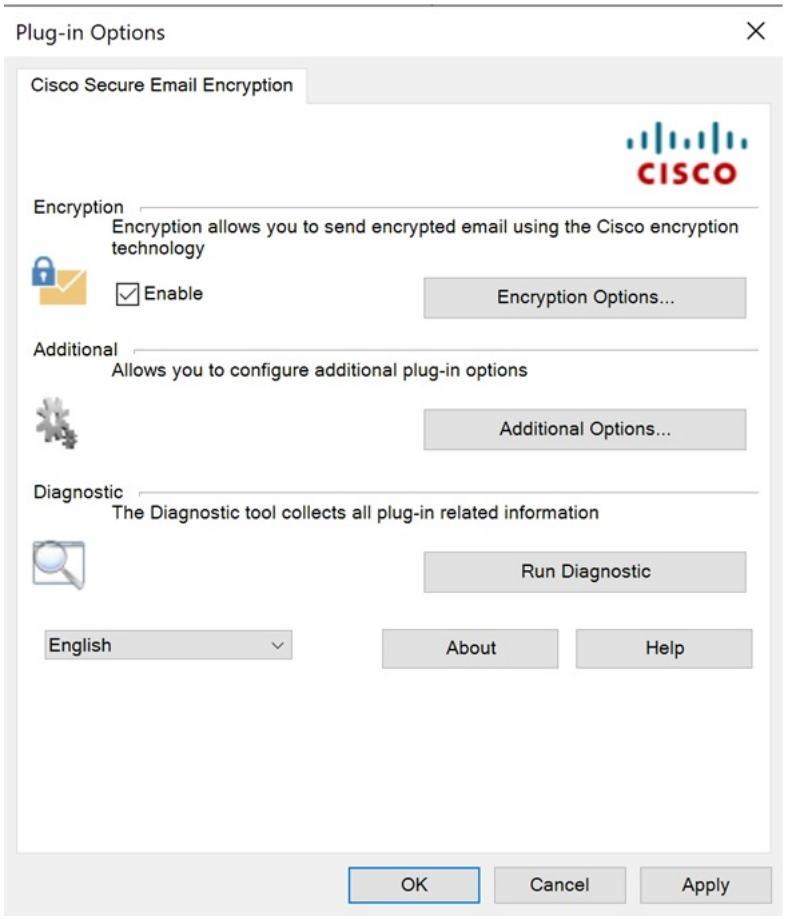
手順

ステップ 1 診断ツールを実行するには、次のように移動します。

- Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、または **[File]** > **[Options]** > **[Add-ins]** > **[Add-in Options]** > **[Cisco Email Encryption]** > **[Run Diagnostic]** に移動します。

- Outlook 2007 ではツールバーの [Plug-in Options] ボタンをクリックするか、**[Tools]** > **[Options]** > **[Cisco Email Security Encryption]** > **[Run Diagnostic]** に移動します。

Cisco Secure Email Encryption の [Plug-in Options] ページ：



ステップ 2 診断ツールがデータを収集するまで数秒間待ちます。診断ツールがデータを収集し終わったら、データが正常に収集されたことを示すメッセージが表示されます。

診断ツールにより、*CiscoDiagnosticReport.zip* ファイルが生成され、現在のユーザーの **My Documents** フォルダに保存されます。そのファイルはエンドユーザーがシステム管理者に送信するか、管理者がシスコサポートの担当者に送信できます。レポートを表示するには、*CiscoDiagnosticsReport.zip* ファイルをダブルクリックします。

Program Files からの診断ツールの実行

次の 2 種類の方法で Program files から診断ツールを実行できます。

- [Start] > [Programs] > [Cisco Email Encryption Plug-in] > [Cisco Email Encryption Plug-in Diagnostic] から診断ツールを実行します。

または

- Cisco Secure Email Encryption Plug-in がインストールされているフォルダ（通常は C:\Program Files\Cisco\Cisco Email Encryption Plug-in）に移動し、*Cisco.EmailEncryption.Framework.Diagnostic.exe* ファイルをダブルクリックします。

シスコの診断ツールの一般的なエラーのトラブルシューティング

適切なデバッグを行うには、すべての診断ログを拡張モードにする必要があります。

実行中の診断ツールでログ収集が完了したら、次の手順を実行します。

1. *CiscoEncryptionDiagnosticReport\Outlook\UsersAppDataFiles\CiscoEmailEncryption.log* に移動します。
2. ログファイルを開き、次のいずれかの問題が存在するかどうかを確認します。
   - 問題：TLS 接続をネゴシエートできません。 （80 ページ）
   - 問題：DNS 名を解決できません。 （80 ページ）
   - 問題：HTTP要求を送信できません。 （81 ページ）
   - 問題：Web プロキシサーバーからの応答が無効です。「HTTP/1.0 407 プロキシ認証が必要です」 （81 ページ）
   - 問題：クライアントマシンで Java ランタイム環境が見つかりません。 （81 ページ）

問題：TLS 接続をネゴシエートできません。

障害：プラグインが Encryption Service サーバー（res.cisco.com）に接続できず、TLS 接続をネゴシエートします。

解決策：プラグインがインストールされているクライアントマシンに Encryption Service サーバー（res.cisco.com）を接続していることを確認します。Encryption Service サーバーとクライアントマシンの間のネットワークでファイアウォールを実行している場合は、次のポートを開く必要があります。

- `res.cisco.com` （デフォルト（復号）、暗号化、およびフラグモードに使用されます）。
- `verify.res.cisco.com`（BCE Config 署名中に使用されます）。
- `updates.res.cisco.com`（Microsoft Outlook の [Plug-in] オプションで [Check for Updates] オプションをクリックすると使用されます）。

問題：DNS 名を解決できません。

障害：プラグインが Encryption Service サーバー（res.cisco.com）に接続できず、DNS 名を解決できません。

解決策：プラグインがインストールされているクライアントマシンに適切なインターネット接続があることを確認します。

問題：HTTP要求を送信できません。

障害：プラグインが Encryption Service サーバー（res.cisco.com）に HTTP 要求を送信できません。

解決策：プラグインがインストールされているクライアントマシンに Encryption Service サーバー（res.cisco.com）を接続していることを確認します。Encryption Service サーバーとクライアントマシンの間のネットワークでファイアウォールを実行している場合は、次のポートを開く必要があります。

- `res.cisco.com` （デフォルト（復号）、暗号化、およびフラグモードに使用されます）。
- `verify.res.cisco.com`（BCE Config 署名中に使用されます）。
- `updates.res.cisco.com`（Microsoft Outlook の [Plug-in] オプションで [Check for Updates] オプションをクリックすると使用されます）。

問題：Web プロキシサーバーからの応答が無効です。「HTTP/1.0 407 プロキシ認証が必要です」

障害：次のいずれかの理由により、プラグインがプロキシサーバーを使用して Encryption Service アプリケーションに接続できません。

- プロキシサーバー認証の詳細（ユーザー名とパスワード）がインストール時に提供されません。
- プロキシサーバーの詳細が無効です。

解決策：プラグインのインストール時に、BCE 構成ファイルで提供されるプロキシサーバーの詳細を確認する必要があります。

問題：クライアントマシンで Java ランタイム環境が見つかりません。

障害：プラグインを含むクライアントマシンに Java ランタイム環境がインストールされていません。

解決策：Java ランタイム環境がクライアントマシンにインストールされていることを確認します。この環境にプラグインが含まれています。

エンベロープでの JavaScript の無効化

受信電子メールがエンベロープで JavaScript を使用している場合、エラーが生じる原因となったり、エンベロープを開けなくなったりする可能性があります。これらの問題を回避するには、次の手順を実行し、生成されたエンベロープで JavaScript を無効にします。

手順

ステップ 1 キー サーバーから BCE Configuration ファイルのテンプレートをダウンロードします。

キーサーバーに管理者としてログインし、[Accounts] > [Manage Accounts] > [BCE Config] > [Download Template] を選択します。

ステップ 2 BCE Configuration ファイルを編集し、<encryption> セクションのいずれかの場所に <usescript>false<usescript> を追加するか、<usescript> タグがすでに存在している場合は値を false に設定します。

ステップ 3 BCE Configuration ファイルを保存して、キー サーバー上でファイルに署名します。

ステップ 4 署名した BCE Configuration ファイルをユーザーに送信します。

Cisco Secure Email Encryption Plug-in のアンインストール

Cisco Secure Email Encryption Plug-in をアンインストールするには、[Control Panel] > [Add/Remove Program] オプションを使用するか、または setup.exe プログラムを実行します。

アンインストールすると、次の項目が削除されます。

- プラグインによって作成されたすべてのレジストリ エントリ
- [プログラムの追加と削除（Add/Remove Program）] に一覧表示されているプラグインのエントリ
- プラグインに関連するファイルの一部。すべてのファイルが削除されるわけではないので注意してください。
- プラグイン ツールバー（Outlook から削除）

（注） プラグインをアンインストールしても Outlook のパフォーマンスには影響しません。アンインストールするときは Outlook を終了しておいてください。

Cisco Secure Email Encryption Plug-in for Outlook をアンインストールするには、次の手順を実行します。

Encryption Plug-in for Outlook のアンインストールに使用できる方法には次の 2 つがあります。

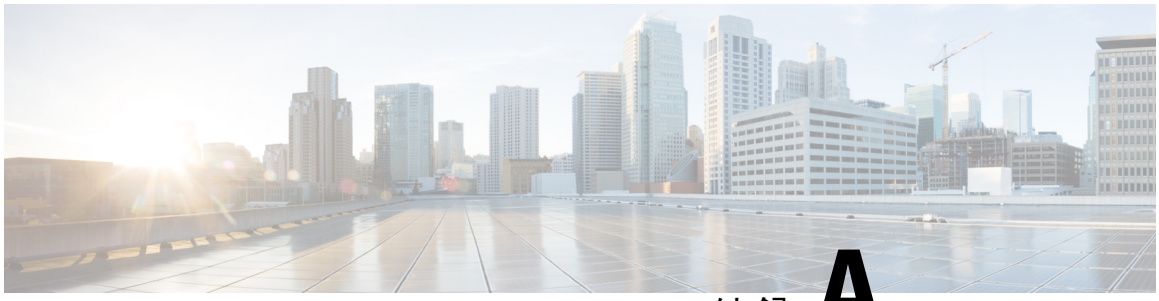
手順

ステップ 1 **[Start]** > **[Control Panel]** > **[Add/Remove Programs]** をクリックします。

ステップ 2 [Cisco Secure Email Encryption Plug In] > を選択し、**[Uninstall/Change]** > **[Next]** > **[Remove]** をクリックします。

もう 1 つのアンインストール方法：

- プラグインのセットアップファイル（プラグインのインストールに使用したファイル）をダブルクリックし、[Remove] オプションを選択して Cisco Secure Email Encryption Plug-in をアンインストールします。

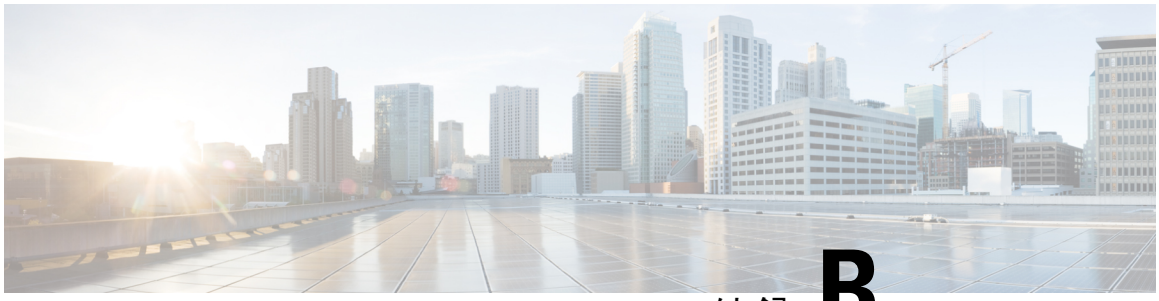


付録 A

シスコ エンド ユーザー ライセンス契約

Cisco エンドユーザーライセンス契約の詳細については、https://www.cisco.com/c/ja_jp/products/security/web-security-appliance/index.html を参照してください。

シスコ エンド ユーザー ライセンス契約



付録 B

BCE_Config.xml のパラメータ

次の表に、アカウント管理者が変更できる BCE_Config.xml ファイルのパラメータを示します。

パラメータ	オプション	説明	許容値
plugin	Edition	プラグイン タイプ	encrypt、decrypt、 flag
	maxMailSize	暗号化メールの最大サイズ	デフォルト：7MB、最大値 = 25 MB
checkForUpdates	checkAutomatically	Outlook を起動したときに更新の自動チェックを有効にするには true を、無効にするには false を設定します。デフォルト値は true です。	true、false

パラメータ	オプション	説明	許容値
callHome	callHomeEnable	Outlook を起動したときに使用状況データの送信を有効にするには true に、送信を無効にするには false に設定します。デフォルト値は true です。false に設定すると、ユーザーは匿名の使用状況データをシスコに送信できません。	true、false
	callHomeAdminEnable	Outlook を起動したときに使用状況データの送信を有効にするには true に、送信を無効にするには false に設定します。デフォルト値は true です。falseに設定すると、使用状況データ収集に関する通知を受信できず、シスコに匿名の使用状況データを送信することができなくなります。	true、false
	displayUsageReminder	暗号化中に使用状況リマインダを表示するかどうかを指定します。	true、false
	encryptByDefault	暗号化を有効にするかどうかを指定します。iOS または Andriod には適用されません。	true、false

パラメータ	オプション	説明	許容値
	subjectFlag	plugin edition が「flag」の場合にのみ使用して、メッセージの暗号化にフラグを付ける方法を定義します。subjectFlag：指定したテキストを件名フィールドに追加します。元の件名に ${subject} を使用します。	例：[SECURE]${subject}
Password	duration	ユーザーパスワードをキャッシュする期間（分単位の整数）。 max == 0 の場合、パスワードキャッシュはなく、毎回パスワードが必要です。 max == -1 の場合、パスワードは無期限にキャッシュされます。	min = 0、max = 1440（分）

パラメータ	オプション	説明	許容値
outlook	showEncryptDialog	暗号化されたメッセージの送信中に [Secure Envelope Options] ダイアログを表示します。	true、false
	showPluginOptions	暗号化、診断、追加オプションを実行できる [Plug-in Options] ダイアログボックスを開く [Plug-in Options] ボタンを有効にするには true に、無効にするには false に設定します。false を設定すると、[Plug-in Options] ボタンは表示されません。	true、false
	showManageMessageButton	true または false に設定して、[Manage Messages] ダイアログボックスを開く [Manage Messages] ボタンを有効または無効にします。このダイアログボックスでメッセージをロックしたり、メッセージの有効期限を設定したりできます。false を設定すると、[Manage Messages] ボタンは表示されません。	true、false
	useKeyServerMessageBody	true の場合、プラグインはプラグインの代わりにキーサーバーからの発信メッセージの本文を使用します。このフィールドは、Microsoft Outlook にのみ適用されます。	true、false
	locale		en、es、it、ja、de、zh、fr、pt

パラメータ	オプション	説明	許容値
		未登録ユーザーの場合など、受信者のロケール設定を決定できない場合のデフォルトロケールを定義します。この値を省略すると、キーサーバーがデフォルトロケールを決定します。 キーサーバーでサポートされているロケールのリスト：	
keyserver	connection_timeout	キーサーバーへの接続が確立されるまでに待機する時間の長さ。	整数（ミリ秒単位）
	socket_timeout	キー サーバーからのデータを待機する時間の長さ。	整数（ミリ秒単位）
	accept_untrusted_certificates	無効な証明書に対してSSL接続を続行するかどうかを決定します。	true、false

パラメータ	オプション	説明	許容値
proxies	proxy	プロキシ設定の名前。<proxies> セクションに指定し、キーサーバーと通信する場合に使用します。	空白、カスタム名
	proxy name	特定のプロキシの設定を入力する場合に選択します。	デフォルト
	host	システムまたはプロキシサーバーのホスト名または IP アドレスを指定します。	有効な IP アドレスまたはホスト名。
	port	システムまたはプロキシサーバーのポートを指定します。	整数
	user	サーバーでユーザー名が必要な場合に、ユーザー名を入力します。	character
	password	システムまたはプロキシサーバーに対して入力したユーザー名に関連するパスワードを入力します。	パスワード
	addmessagebar	セキュアメッセージにメッセージバーを追加する場合に選択します。	true、false
message	sensitivity	暗号化した電子メールのセキュリティを設定します。デフォルト値は BCE_Config.xml ファイルに定義されています。	0 = 低、10 = 中、50 = 高

パラメータ	オプション	説明	許容値
messagebar	replyenabled	メッセージバーが有効になっている場合、メッセージ バーに [Reply] が表示されます。	true、false
	replyallenabled	メッセージバーが有効になっている場合、メッセージ バーに [Reply to All] が表示されます。	true、false
	forwardenabled	メッセージバーが有効になっている場合、メッセージバーに [Forward] が表示されます。	true、false
	openinsamewindow	エンベロープと同じウィンドウでセキュアメッセージを開く場合に選択します。	true、false
	sendreturnreceipt	受信者が送信された電子メールが開いたときに受信確認を要求するには、このオプションを選択します。	true、false

パラメータ	オプション	説明	許容値
recipient	menu	エンベロープが登録済みエンベロープの受信者のドロップダウンメニューを表示するかどうかを決定するブール値。true の場合、ドロップダウンメニューが表示されます。それ以外の場合は、メッセージの一意の受信者がエンベロープに埋め込まれ、メニューが不要になります。 このメッセージの受信者が複数いる場合、この値は無視されます。	true、false

（注） このリストに示されていないパラメータは変更しないことを推奨します。

一例として、サンプルの BCE_Config.xml ファイルを以下に示します。

注意 次のコードスニペットの内容をコピーして使用しないでください。これは参考のみとしてください。

```
<?xml version="1.0" encoding="UTF-8"?>
<!--&#xa;If the plugin supports the possibility for the user to edit a parameter in the
 UI,&#xa;the display XML attribute gives the account administrator the ability to
change&#xa;this behavior by setting it to one of the following values:&#xa;    editable
 - The configuration is visible and editable in the UI&#xa;    readonly - The configuration
 is viewable but not editable in the UI&#xa;    hidden - The configuration is not viewable
 in the UI&#xa;-->
<encryption acctId="XXXX" version="1.0" id="$Revision: 1.27 $">
    <!--&#xa;    Plugin related configuration. Valid type edition values are:&#xa;
  decrypt - Plugin can only decrypt PXE envelopes.&#xa;       flag - Plugin can decrypt
 and flag a message for encryption.&#xa;       encrypt - Plugin can decrypt and encrypt
 a message on the device.&#xa;    -->
    <plugin edition="encrypt">
        <!-- reportingComponent - section responsible for configuring reporting plug-in.
 -->
        <reportingComponent>
            <lockUiOptions>false</lockUiOptions>
            <enabled>true</enabled>
            <keepSentReports>false</keepSentReports>
          <!--&#xa;              reportFormat - Defines format of the report. Supported
 values:&#xa;                  encrypted - report will be encrypted before sending;&#xa;
                  plain - report will be sent without encryption;&#xa;
```

BCE_Config.xml のパラメータ

```
Default value: encrypted.&#xa;            -->
        <report>
            <format>encrypted</format>
            <subject>Cisco Email Security Plug-in Report (${reportType})</subject>
        </report>
        <maxMailSize>1005000</maxMailSize>
        <attachmentName>orig_msg.enc</attachmentName>
        <showReportSuccessOne>true</showReportSuccessOne>
        <showReportSuccessMultiple>true</showReportSuccessMultiple>
        <addExplorerCommandBar>true</addExplorerCommandBar>
        <addInspectorCommandBar>true</addInspectorCommandBar>
        <addContextMenu>true</addContextMenu>
        <addBlockSenderButton>true</addBlockSenderButton>
        <reportTypes>
            <reportType name="spam">
                <!-- Only one email address is allowed for each report type -->
                <address>outlook_spam@access.ironport.com</address>
                <copyAddressInPlainFormat></copyAddressInPlainFormat>
                <headerValue>spam</headerValue>
                <showInJunkFolder>true</showInJunkFolder>
                <largeRibbonButton>true</largeRibbonButton>
            </reportType>
            <reportType name="ham">
                <!-- Only one email address is allowed for each report type -->
                <address>outlook_ham@access.ironport.com</address>
                <copyAddressInPlainFormat></copyAddressInPlainFormat>
                <headerValue>ham</headerValue>
                <showInJunkFolder>true</showInJunkFolder>
                <largeRibbonButton>true</largeRibbonButton>
            </reportType>
            <reportType name="virus">
                <!-- Only one email address is allowed for each report type -->
                <address>outlook_virus@access.ironport.com</address>
                <copyAddressInPlainFormat></copyAddressInPlainFormat>
                <headerValue>virus</headerValue>
                <showInJunkFolder>true</showInJunkFolder>
                <largeRibbonButton>false</largeRibbonButton>
            </reportType>
            <reportType name="phish">
                <!-- Only one email address is allowed for each report type -->
                <address>outlook_phish@access.ironport.com</address>
                <copyAddressInPlainFormat></copyAddressInPlainFormat>
                <headerValue>phish</headerValue>
                <showInJunkFolder>true</showInJunkFolder>
                <largeRibbonButton>false</largeRibbonButton>
            </reportType>
            <reportType name="marketing">
                <!-- Only one email address is allowed for each report type -->
                <address>outlook_mktg@access.ironport.com</address>
                <copyAddressInPlainFormat></copyAddressInPlainFormat>
                <headerValue>marketing</headerValue>
                <showInJunkFolder>true</showInJunkFolder>
                <largeRibbonButton>false</largeRibbonButton>
            </reportType>
        </reportTypes>
    </reportingComponent>
    <!-- Check for update for the plugin -->
    <checkForUpdates>
        <checkAutomatically display="hidden">false</checkAutomatically>
        <serverURL>http://updates.res.cisco.com</serverURL>
    </checkForUpdates>
    <!-- Call home section -->
    <callHome>
         <callHomeEnabled>true</callHomeEnabled>
```

BCE_Config.xml のパラメータ

```
            <callHomeAdminEnabled>true</callHomeAdminEnabled>
        </callHome>

       <!-- Specify whether show Usage Reminder during encryption (true) or not (false).
 -->
        <displayUsageReminder>true</displayUsageReminder>
        <!--&#xa;        In case of an error, this will be the email address and subject
 that will&#xa;        appear in the user generated diagnostic email.&#xa;        The
diagnostic  email field should only be used when a company is hosting their own&#xa;
     encryption helpdesk.&#xa;        The following entries are not allowed:
support@cisco.com,support@res.cisco.com &#xa;        This feature is not supported in
Outlook.&#xa;        -->
        <diagnostic>
          <email display="readonly"><!-- Add your support email address here --></email>

            <subject display="readonly">Cisco BCE Diagnostic Information</subject>
        </diagnostic>
        <!--&#xa;        Specify whether encryption should be enabled (true) or not
(false).&#xa;        Not applicable on iOS or Android.&#xa;        -->
        <encryptByDefault display="editable">false</encryptByDefault>
        <!--&#xa;        Used only if plugin edition="flag", defines how the message
should&#xa;       be flagged for encryption. Only one of the following XML elements&#xa;
        can be specified.&#xa;            subjectFlag - Add specified text to subject
field.&#xa;                          Use ${subject} for the original subject.&#xa;
       headerFlag  - Add specified MIME header.&#xa;        For example:&#xa;
  <subjectFlag>[SECURE]${subject}[ME]</subjectFlag>&#xa;        or:&#xa;
<headerFlag>X-IronPort-Encrypt: True</headerFlag>&#xa;        Note: Not all plugins
support the XML element, headerFlag, especially, mobile devices.&#xa;        -->
        <subjectFlag>[SECURE]${subject}</subjectFlag>
        <!-- Note: Not all plugins will provide access to these links -->
        <links>
        <!-- URL containing help about the PXE envelope -->
        <!-- If help xml element is not defined the plugin should use its system default
 <help display="hidden"/> -->
        </links>
        <cache>
            <password>
                <!--&#xa;               How long user passwords should be cached (an
integer, in minutes).&#xa;               if max == 0, there is no password cache and
passwords are required everytime.&#xa;               if max == -1, passwords are cached
 indefinitely.&#xa;               -->
                <duration min="0" max="1440" display="editable">1440</duration>
            </password>
            <!-- The section below sets the caching of the session in clients -->
            <samlSession>
                    <cacheSession>True</cacheSession>
            </samlSession>
            <envelope>
                <!-- Cache size of PXE envelope storage (an integer, in MB) -->
                <storage display="editable">6</storage>
               <!-- Maximum duration to retain envelopes files (an integer, in minutes).
 -->
                <duration display="editable">43200</duration>
            </envelope>
        </cache>
        <outgoingSMTP>
            <!-- If true then outgoing SMTP is enabled, otherwise native mail client
will be used.&#xa;             display=editable will allow user to change the approach,
 in case if he is outside of corporate VPN network. -->
            <isEnabled display="hidden">false</isEnabled>
            <!-- Corporate server address -->
            <server></server>
            <!-- SMTP port -->
            <port></port>
```

BCE_Config.xml のパラメータ

```
            <!-- Enable or disable SSL for connection -->
            <sslEnabled></sslEnabled>
        </outgoingSMTP>
        <!-- Outlook specific configuration -->
        <outlook>
            <!-- Show "Secure Envelope Options" dialog while sending encrypted message
(true) or not (false). -->
            <showEncryptDialog display="editable">true</showEncryptDialog>
            <!--&#xa;            Used only if plugin edition="flag", defines how the
message should&#xa;           be flagged for encryption using the Outlook message
sensitivity flag.&#xa;          Valid values are private, confidential, and public&#xa;
            <sensitivityFlag display="editable"></sensitivityFlag>&#xa;           -->
            <!-- Determines whether plug-in options dialog will be shown in Outlook -->
            <showPluginOptions>true</showPluginOptions>
            <!-- Determines whether the manage message button will be shown in Outlook
-->
            <showManageMessageButton>true</showManageMessageButton>
        </outlook>
        <!--&#xa;           If true, the plugin will use the outgoing message body from
 the key server&#xa;           instead of the plugin.  This field is only applicable
to Microsoft Outlook.&#xa;        -->
        <useKeyServerMessageBody display="editable">true</useKeyServerMessageBody>
    </plugin>
    <application>
        <!-- ##################################### -->
        <!-- Do not modify these "application" URLs -->
        <!-- ##################################### -->
        <companyURL>https://res.cisco.com</companyURL>
        <helpURL>https://res.cisco.com/websafe/help?topic=RegEnvelope</helpURL>
       <notListedURL>https://res.cisco.com/websafe/help?topic=AddrNotShown</notListedURL>


<forgotPasswordURL>https://res.cisco.com/websafe/pswdForgot.action</forgotPasswordURL>

<passwordNotShownURL>https://res.cisco.com/websafe/help?topic=PPNotShown</passwordNotShownURL>

    </application>
    <external>
       <!--&#xa;       Secure base URL to use for the key server, message bar logo,&#xa;
        message bar secure reply, and enrollment URL.&#xa;        -->
        <secure><url>https://res.cisco.com</url></secure>
       <!--&#xa;       Unsecure base URL to use for the message bar help and GET Payload
 Transport.&#xa;        If omitted, then external secure url will be used.&#xa;
-->
        <unsecure><url>http://res.cisco.com</url></unsecure>
    </external>
    <!--&#xa;    Defines the default locale if the recipient's locale preference&#xa;
  can not be determined, such as for an unregistered user. If this value&#xa;    is
omitted, the key server will determine the default locale.&#xa;    List of locales
supported by the key server:&#xa;       en - English (US)&#xa;       nl_NL - Dutch&#xa;
       de - German&#xa;        es - Spanish&#xa;        fr - French&#xa;        it -
Italian&#xa;        pl - Polish&#xa;        pt - Portugese&#xa;        ru - Russian&#xa;
       zh_CN - Chinese (Simplified)&#xa;       ja - Japanese&#xa;       ko - Korean&#xa;
    List of locales supported by Outlook plug-in:&#xa;        en - English&#xa;
es - Spanish&#xa;        it - Italian&#xa;        ja - Japanese&#xa;        de -
German&#xa;        zh - Chinese&#xa;        fr - French&#xa;        pt - Portuguese
 &#xa;    Please note, if you want to use locales from plug-in, useKeyserverMessageBody
 option should be set to 'False'&#xa;    -->
    <locale display="editable"></locale>
    <keyserver>
        <!-- Key server token file used for encryption. -->

<token><![CDATA[data@id=19916&aId=7058&name=Token7058&desc=Default+Token&value=gsCkHZRpF0QxhAXJ4jr2ugDCSbG7nKw3]]></token>
```

BCE_Config.xml のパラメータ

```
        <!-- How long to wait for a connection to the key server to be established (an
integer, in milliseconds). -->
        <connection_timeout display="editable">20000</connection_timeout>
       <!-- How long to wait for data from the key server (an integer, in milliseconds).
 -->
        <socket_timeout>30000</socket_timeout>
        <!-- Determines if the SSL connection should continue for invalid certificates
-->
        <accept_untrusted_certificates>false</accept_untrusted_certificates>
        <!-- Name of proxy configuration, specified in the <proxies> section, to use
when&#xa;             communicating with key server. Supported values are:&#xa;
    blank - No Proxy (Recommended).  For Outlook, this will update the plugin's&#xa;
                connection settings to either "No Proxy" or "Use System Proxy
Settings",&#xa;                  depending if the <proxy> name is specified as "Default"
 in the <proxies>&#xa;                    section.&#xa;            custom_name - Name
of a custom proxy configuration to use, defined in the&#xa;                    <proxies>
 section.  For Outlook, do not use "Default" as a custom name.&#xa;
To update Outlook to use the system proxy, this field should&#xa;
remain blank.&#xa;        -->
        <proxy></proxy>
    </keyserver>
    <!--&#xa;    Proxy configurations. This feature is not supported on Android, or
iOS.&#xa;    -->
    <proxies>
        <!-- Name of the proxy configuration that will be used when communicating with
the key server.&#xa;            For Outlook, specifying a name of "Default" will update
 the plugin's connection setting&#xa;            to "Use System Proxy Settings".  In
this case, the proxy settings are irrelevant and ignored.&#xa;        -->
        <proxy name="Default">
            <!--&#xa;            Proxy implementation class to use. Supported values
are&#xa;               Web&#xa;               SOCKS4&#xa;               SOCKS4a&#xa;
               SOCKS5&#xa;            -->
            <type></type>
            <!-- Host name of proxy server. -->
            <host></host>
            <!-- Port number of proxy server. -->
            <port></port>
            <!-- User name, if applicable, to authenticate with proxy server. -->
            <user></user>
            <!-- Password, if applicable, to authenticate with proxy server. -->
            <password></password>
If you have enabled Easy Open on your account and you are using a proxy server, make
sure that you configure the user credentials for the proxy server.
        </proxy>
    </proxies>
    <!-- Whether to add the message bar to the secure message (true) or not (false). -->

    <addmessagebar>true</addmessagebar>
    <address>
        <!-- Forwarding email address used for Mobile Device Support. -->
        <mobile>mobile@res.cisco.com</mobile>
    </address>
    <algorithms>
        <!--&#xa;        Payload encryption algorithm to use when creating the
envelope.&#xa;       Valid values are:&#xa;           ARC4&#xa;           ARC4-160&#xa;
            ARC4-256&#xa;            AES&#xa;            AES-128&#xa;
AES-192&#xa;            AES-256&#xa;        -->
        <PayloadEnc>AES</PayloadEnc>
        <!--&#xa;        Payload verification algorithm to use when creating the
envelope.&#xa;       Valid values are:&#xa;           CRC-32&#xa;           SHA-1&#xa;
            SHA-256&#xa;        -->
        <PayloadVer>SHA-256</PayloadVer>
        <!--&#xa;        Key server key hash algorithm to use when creating the
envelope.&#xa;       Valid values are:&#xa;           plain&#xa;           SHA-1&#xa;
```

BCE_Config.xml のパラメータ

```
        plain should only be used when the user is authenticated against&#xa;        an
 external repository, like an LDAP server, and the repository&#xa;        requires
cleartext passwords&#xa;        -->
        <KeyServerKeyHash>SHA-1</KeyServerKeyHash>
    </algorithms>
    <!--&#xa;    Name of the envelope attachment file where&#xa;    ${date} and ${time}
 are replaced by the date and time&#xa;    when the envelope was generated.&#xa;    -->
    <attachmentname display="hidden">securedoc_${date}T${time}.html</attachmentname>
    <checkbox>
        <!--&#xa;        Boolean indicating whether the checkbox for open offline
should&#xa;        be visible on the envelope (true) or not (false).&#xa;        This
feature is not visible in Outlook.&#xa;        -->
        <openoffline>false</openoffline>
        <!--&#xa;        Boolean indicating whether the checkbox for remember user
key&#xa;        should be visible on the envelope (true) or not (false).&#xa;
This feature is not visible in Outlook.&#xa;        -->
        <rememberkey>false</rememberkey>
       <!--&#xa;       Boolean indicating whether the checkbox for remember envelope&#xa;
        key should be visible on the envelope (true) or not (false).&#xa;        This
feature is not visible in Outlook.&#xa;        -->
        <rememberenvelopekey>false</rememberenvelopekey>
        <!--&#xa;        Boolean indicating whether the checkbox for remember me
should&#xa;        be visible on the envelope (true) or not (false).&#xa;        -->
        <rememberme>true</rememberme>
        <!--&#xa;        Boolean indicating whether the checkbox for enable personal
security&#xa;       phrase should be visible on the envelope (true) or not (false).&#xa;
        -->
        <enablepsp>false</enablepsp>
The Enable Personal Security Phrase functionality is no longer supported for Encryption
 Service. Make sure that you always set the tag as false in the BCE_Config.xml file.
       <!--&#xa;       Boolean indicating whether the checkbox for auto open should&#xa;
        be visible on the envelope (true) or not (false).&#xa;        This feature is
not visible in Outlook.&#xa;        -->
        <autoopen>false</autoopen>
    </checkbox>
    <date>
        <!--&#xa;        Time format string when a reminder notification will be sent
to&#xa;        the recipient if the envelope has not been read.&#xa;        Note: Cisco
 Secure Email Encryption Service does not support this feature.&#xa;            Format
        Description&#xa;           ======         ===========&#xa;           +hh:mm:ss
       Relative time *&#xa;            +d              Relative time in days&#xa;
      s               Absolute time in UTC milliseconds from the epoch *&#xa;
  0               No reminder notification&#xa;            * Not supported on mobile
devices&#xa;        -->
        <readby display="hidden">0</readby>
        <!--&#xa;            Time format string when the envelope will expire.&#xa;
        Format          Description&#xa;            ======          ===========&#xa;
         +hh:mm:ss       Relative time *&#xa;            +d              Relative time
in days&#xa;           s               Absolute time in UTC milliseconds from the epoch
 *&#xa;           0               Never expires&#xa;            * Not supported on
mobile devices&#xa;        -->
        <expiration display="editable">0</expiration>
    </date>
    <!-- Envelope profile to use. -->
    <envelopeprofilename>CRES</envelopeprofilename>
    <!-- Image profile to use. -->
    <imageProfileName>CRES</imageProfileName>
    <message>
        <!--&#xa;            Sensitivity of the envelope. Acceptable levels are 0 to
50.&#xa;           For label, the values should be listed in the order they will be
displayed.&#xa;          For localization purposes, do not change or reword the existing
 sensitivity&#xa;            labels Low | Medium | High.&#xa;        -->
       <sensitivity label="Low=0&amp;Medium=10&amp;High=50"
display="editable">50</sensitivity>
```

BCE_Config.xml のパラメータ

```
    </message>
    <messagebar>
       <!--&#xa;       If the message bar is enabled, show "Reply" button in the message
 bar (true) or not (false).&#xa;        -->
        <replyenabled display="editable">true</replyenabled>
        <!--&#xa;        If the message bar is enabled, show "Reply to All" button in
the message bar (true) or not (false).&#xa;        -->
        <replyallenabled display="editable">true</replyallenabled>
        <!--&#xa;        If the message bar is enabled, show "Forward" button in the
message bar (true) or not (false).&#xa;        -->
        <forwardenabled display="editable">true</forwardenabled>
    </messagebar>
    <!--&#xa;    Boolean indicating whether the envelope's payload should force the
applet to&#xa;    open the main document in the same window as the envelope. If set to
true,&#xa;    the applet opens the main document in the window it's running in, but as
a&#xa;    consequence can't delete the files in the payload when shutting down,
leaving&#xa;    decrypted files on disk. It does, however, avoid pop-up blockers, as no
 new&#xa;    window is being opened.&#xa;    -->
    <openinsamewindow>true</openinsamewindow>
    <!--&#xa;    Whether a return receipt email should be sent when the recipient opens
 the email (true) or not (false).&#xa;    -->
    <sendreturnreceipt display="editable">false</sendreturnreceipt>
    <show>
        <recipient>
            <!--&#xa;            Boolean that determines if the envelope will show a
dropdown&#xa;            menu of recipients for Registered Envelopes. If true, the
dropdown&#xa;            menu will be shown, otherwise the unique recipient of the
message&#xa;          will be embedded in the envelope to make the menu unnecessary.&#xa;
            If there is more than one recipient for this message then this&#xa;
    value will be ignored.&#xa;            -->
            <menu>true</menu>
        </recipient>
    </show>
   <!--&#xa;    Boolean indicating whether the envelope's payload should suppress opening
 with the&#xa;    applet. If set to true, opening an envelope with a multi-file payload
 uses the online&#xa;    opener instead of the applet.&#xa;    -->
    <suppressappletforopen>true</suppressappletforopen>
</encryption>
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。