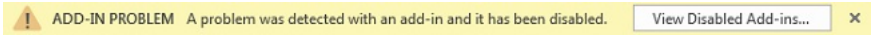
Cisco Secure Email Reporting Plug-in for Outlook の設定と使用

この章では、Cisco Secure Email Reporting Plug-in for Outlook で使用可能な機能について説明します。この章は、次の項で構成されています。

Cisco Secure Email Reporting Plug-in の有効化

インストール後に初めて Cisco Secure Email Reporting Plug-in を開始すると、Outlook によって無効になっていることがあります。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 Reporting 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 Reporting 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、分析するためにシスコのサーバに保存されます。

- 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

この情報の詳細について以下に説明します。

起動後に [Plug-in Options] > [Additional Options] > [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 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。

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主に使用します。[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
- オペレーティング システムで使用する言語
- 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

非標準レポート アドレスが使用されているかどうかに関する情報を収集します。

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

Cisco Secure Email Reporting Plug-in の全般設定は、[Options] ページから設定できます。

Enable または Disable

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

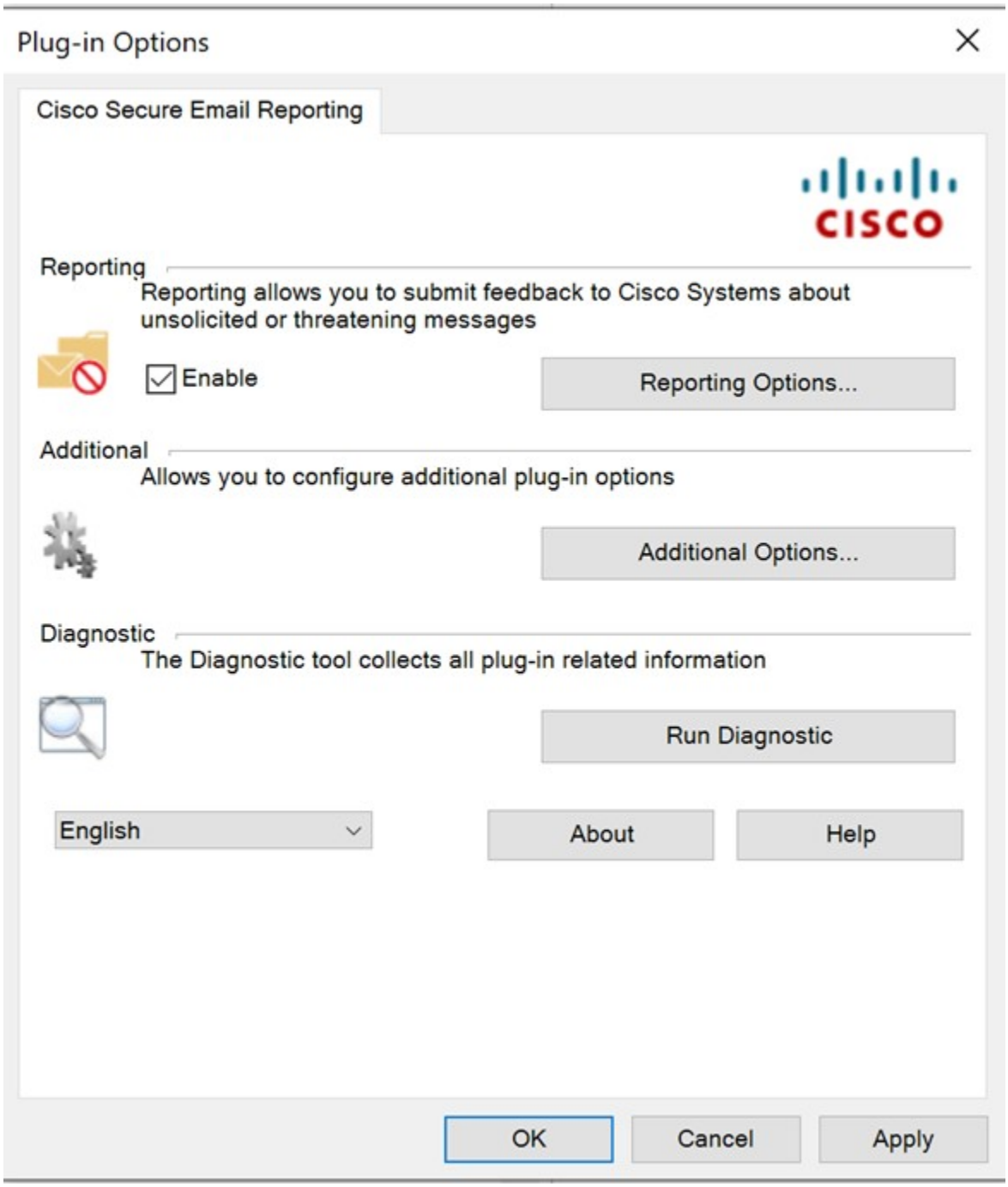
Outlook 2010/2013/2016 では、[ファイル（File）] > [オプション（Options）] に移動し、左側のナビゲーション バーから [アドイン（Add-ins）] を選択します。次に、ページの下部にある [Manage] ドロップダウンメニューから [COM Add-ins] を選択し、[Go] をクリックします。

Outlook プラグインの基本設定

エンドユーザは [Cisco Secure Email Reporting] 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 [プラグインオプション（Plug-in Options）] ボタンをクリックするか、または [ファイル（File）] > [オプション（Options）] > [アドイン（Add-ins）] > [アドインオプション（Add-in Options）] > [Cisco Email Reporting] を選択します。

[Cisco Secure Email Reporting] タブ：



エンドユーザは、このタブで該当する [有効にする（Enable）] チェックボックスをオンにすることにより、レポートのオプションを有効にすることができます。[Additional Options] ボタンを選択すると、その他のオプションも有効化できます。設定をさらに細かく行うには[レポートオプション（Reporting Options）] ボタンをクリックします。エンドユーザは、問題解決時に診断ツールを使用し、Cisco Secure Email Reporting 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。

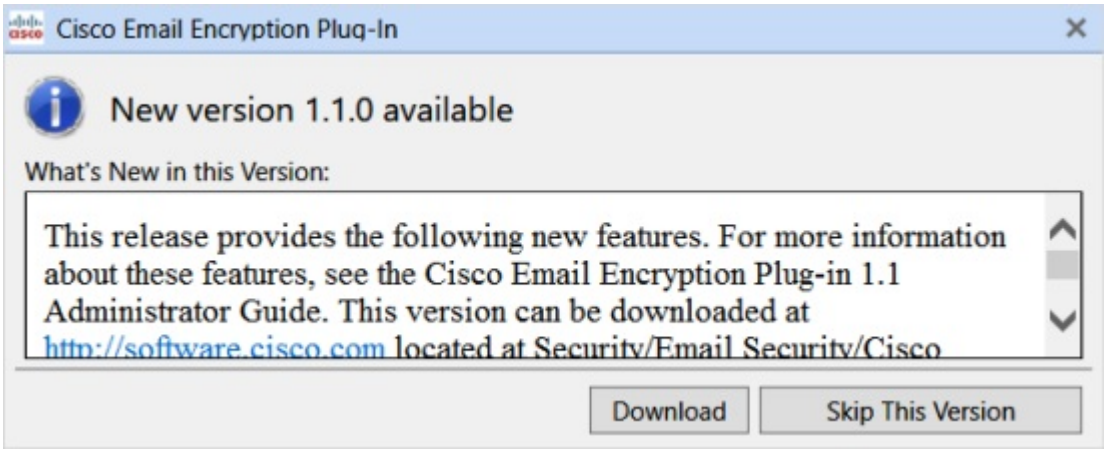
更新をチェックするための Outlook Plug-in の設定

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 に、無効にするには false に設定します。デフォルト値は false 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。

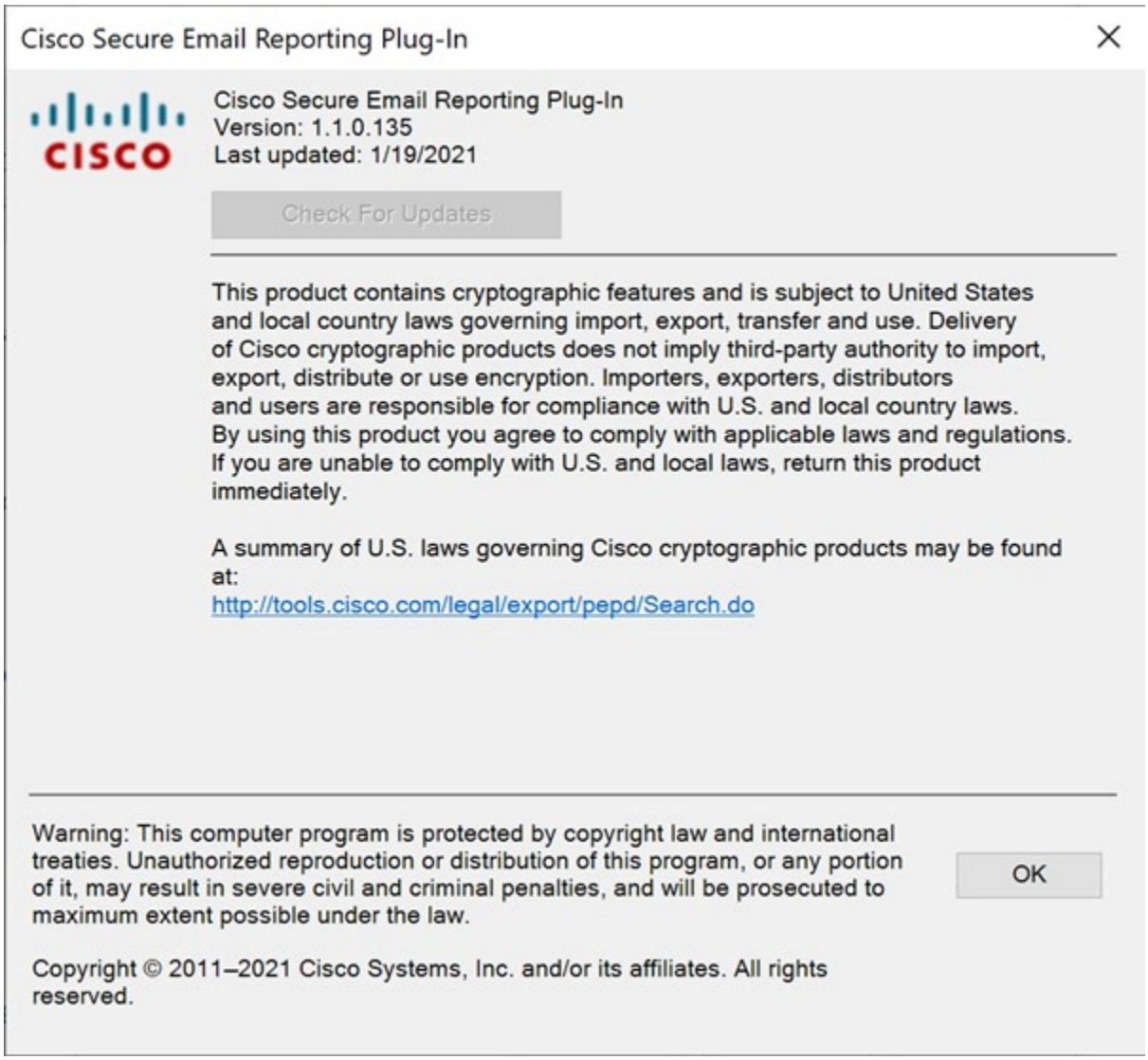
更新の通知

Cisco Secure Email Reporting Plug-in で更新を自動的にチェックするように設定されており、Cisco Secure Email Reporting Plug-in 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 Reporting 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。



コンフィギュレーション 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**：レポート、診断、追加オプションを実行できる [Plug-inオプション（Plug-in Options）] ダイアログ ボックスを開く [Plug-inオプション（Plug-in Options）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 に設定すると、[Plug-in Options] 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 に、無効にするには false に設定します。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 （5 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**：7chapter.fm 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。詳細については、使用状況データ収集の設定 （2 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 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 （2 ページ）を参照してください。

これらのオプションが CommonComponentsConfig.xml ファイルで設定されている場合、これらのオプションをユーザ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。詳細については、Reporting Plug-in for Outlook の使用方法 （10 ページ）を参照してください。

不要な電子メールによるスパム、マーケティング、ウイルス、およびフィッシング攻撃の報告

レポート プラグインを使用すると、エンド ユーザは、受信した電子メールがスパム、マーケティングのメール、フィッシング攻撃、またはウイルスであった場合にシスコに報告できます。また、誤ってスパムと分類されたメールについても報告できます（「ハム」とも呼ばれます）。

Cisco Secure Email Reporting Plug-in for Outlook は、Outlook の [オプション（Options）] ページを使用して設定できます。レポートを有効にするには、次の手順を実行します。

Outlook 2010/2013/2016 では、リボンの [プラグインオプション（Plug-in Options）] ボタンをクリックするか、または [ファイル（File）] > [オプション（Options）] > [アドイン（Add-ins）] > [アドインオプション（Add-in Options）] > [Cisco Email Reporting] を選択します。[Cisco Secure Email Reporting] タブで [レポート（Reporting）] フィールドの [有効化（Enable）] チェックボックスをオンにします。

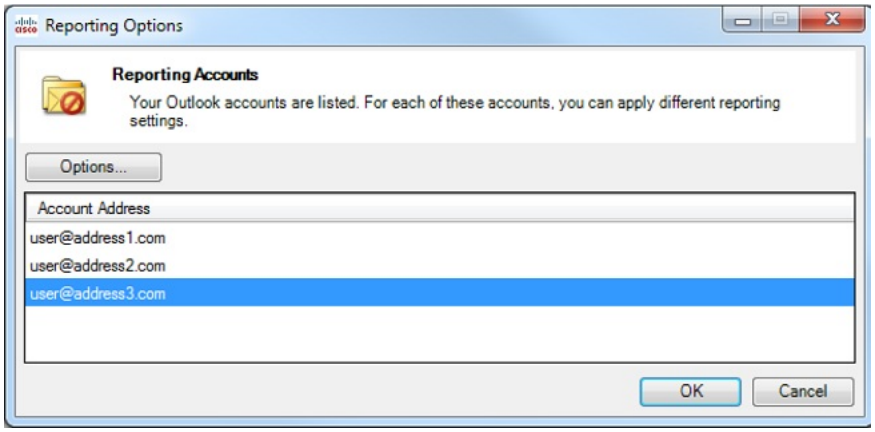
レポート オプション

レポートの設定は [Cisco Secure Email Reporting] ページにあります。レポートの設定を変更するには、次の手順を実行します。

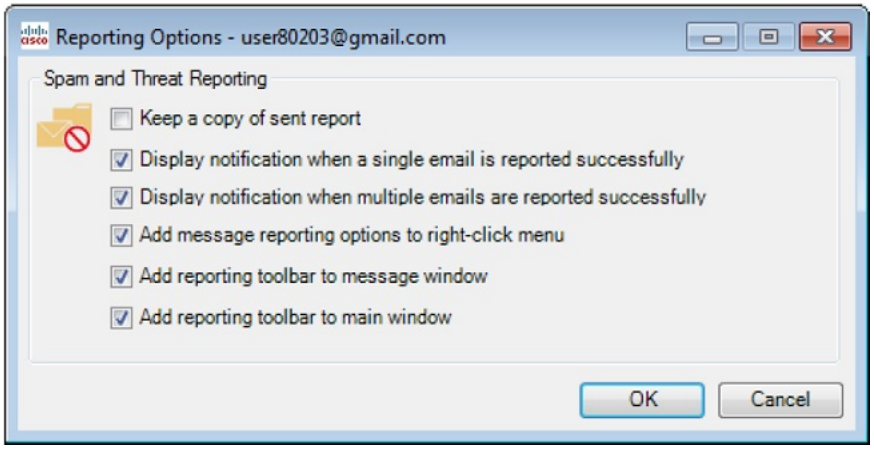
Outlook 2010/2013/2016 では、リボンの [Plug-in Options] ボタンをクリックするか、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Reporting] の順に選択して、[Reporting Options] ボタンをクリックします。

また、アカウントの config_{N} ファイルに設定しなければならないレポート オプションもあります。詳細については、スパム レポートの暗号化の設定 （12 ページ）を参照してください。

次の [レポートアカウント（Reporting Accounts）] ページは、Outlook に設定されているすべてのアカウントを示しています。あるアカウントについてレポート オプションを設定するには、対象のアカウントを選択して [オプション（Options）] ボタンをクリックします。そのアカウントのレポートオプションが表示されます。



次のようなアカウント固有の [Reporting Options] ページには、選択したアカウントのレポートオプションが表示されます。ここで、それぞれの機能を有効または無効にすることができます。詳細については、次の表を参照してください。



この表は、エンド ユーザが設定可能なレポート オプションを示しています。

オプション	説明
Keep a copy of sent report	デフォルトでは、スパムまたはウイルスの電子メール メッセージ、あるいは誤ってスパムまたはウイルスであると分類された電子メール メッセージについて、エンドユーザがシスコに報告した場合、その送信された報告電子メールは削除されます。このオプションを選択すると、電子メールは削除されません。
Display notification when a single email is successfully reported	1 件の電子メールがスパムやウイルスとして正常に報告された場合に、成功を示すメッセージを Outlook のダイアログボックスに表示できます。このオプションをオフにすると、このダイアログボックスは表示されません。
Display notification when multiple emails are successfully reported	一連の電子メールがスパムやウイルスとして正常に報告された場合に、成功を示すメッセージを Outlook のダイアログボックスに表示できます。このオプションをオフにすると、このダイアログボックスは表示されません。
Add message reporting options to right-click menu	デフォルトでは、Cisco Secure Email Reporting Plug-in をインストールすると、Outlook の右クリック コンテキスト メニューにレポートプラグインのメニュー項目が追加されます。このオプションをオフにすると、このメニュー項目は右クリック コンテキスト メニューに追加されません。
Add reporting toolbar to the message window	デフォルトでは、エンドユーザが Cisco Secure Email Reporting Plug-in をインストールすると、電子メール メッセージ ウィンドウにプラグインツールバーが追加されます。このオプションをオフにすると、ツールバーは電子メール メッセージ ウィンドウに追加されません。
Add reporting toolbar to the main window	デフォルトでは、エンドユーザが Cisco Secure Email Reporting Plug-in をインストールすると、Outlook のメインウィンドウにプラグインツールバーが追加されます。このオプションをオフにすると、このツールバーは Outlook のメイン ウィンドウに追加されません。

Reporting Plug-in for Outlook の使用方法

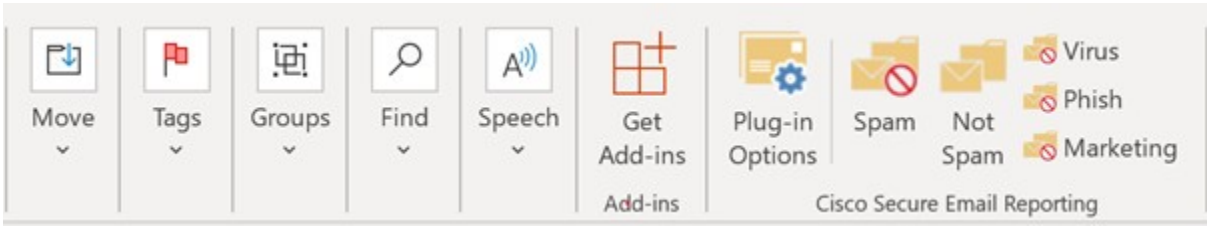
概要

Cisco Secure Email Reporting Plug-in for Outlook では、エンドユーザは、受信トレイに受信したスパム、ウイルス、フィッシング、またはマーケティングのメールについてシスコにフィードバックを送信できます。たとえば、誤分類された場合やスパムとして扱うべき場合に、それらの電子メールメッセージについてシスコに報告できます。シスコでは、このフィードバックを活用して、不要なメッセージが受信ボックスに配信されないようにフィルタを更新します。

このプラグインをインストールすると、Outlook のメニュー バーと右クリック メッセージメニューに便利なインターフェイスが追加されます。このインターフェイスを使用して、スパム、ウイルス、フィッシング、マーケティングの電子メールや、誤分類された電子メールを報告することができます。電子メールを報告すると、レポートが送信されたことを示すメッセージが表示されます。エンドユーザが報告したメッセージは、シスコの電子メールフィルタの強化に使用されます。これによって、受信トレイに一方的に送りつけられるメールの全体量が減少します。

シスコへのフィードバック

プラグインを使用すると、Outlook に次のボタンを持つツールバーが追加されます：[スパム（Spam）]、[スパムではありません（Not Spam）]、[ウイルス（Virus）]、[フィッシング（Phish）]、[マーケティング（Marketing）]。



これらのボタンを使用して、スパム、ウイルス、フィッシング、およびマーケティングのメールを報告します（フィッシング攻撃とは、「不正な」偽装 Web サイトにリンクしている電子メールを送りつける攻撃です。これらの Web サイトは、クレジットカード番号、口座の名義人名とパスワード、社会保障番号など、個人の金融情報を受信者に漏洩させることを目的としています。たとえば、個人の銀行口座情報を不正に要求する電子メールが *infos@paypals.com* から送信されてくることがあります）。また、右クリック コンテキストメニューを使用して、スパム、誤分類されたメール、ウイルス、フィッシング、およびマーケティングを報告することもできます。

さらに、メッセージ ウィンドウのボタンを使用して、スパム、ウイルス、フィッシング、マーケティング、誤分類されたメールを報告できます（誤分類されたメールとは、誤ってスパム、ウイルス、フィッシング、またはマーケティングとしてマークされたメールです）。

スパム、ウイルス、フィッシング、またはマーケティングとして報告された電子メールのメッセージ処理の流れ

スパム、誤分類、ウイルス、フィッシング、またはマーケティングとしてメッセージが報告された場合、そのメッセージは次のように処理されます。

受信トレイのメッセージ：

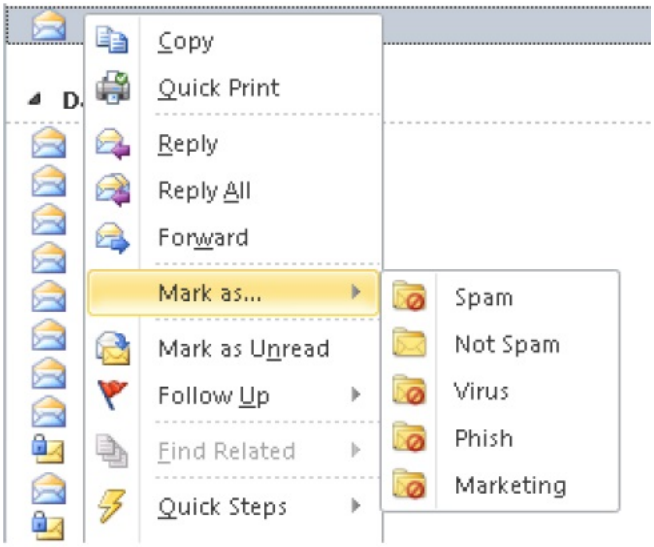
- スパム、ウイルス、フィッシング、またはマーケティングとして報告された受信トレイのメッセージは、[Junk Email] フォルダに移動されます。
- スパムではないと報告された受信トレイのメッセージは受信トレイ フォルダに残ります。

迷惑メッセージ：

- スパム、ウイルス、フィッシング、またはマーケティングとして報告された迷惑メッセージは、[Junk Email] フォルダに残されます。
- スパムではないと報告された迷惑メールは受信トレイ フォルダに移動します。

受信した電子メールがスパムと誤分類された場合（つまり、フィルタリングされ、[Junk Email] フォルダに送られた場合）は、[Not Spam] ボタンをクリックして、電子メールが誤分類されたことを報告できます。これにより、この送信者からのメールは今後スパムとして分類されることはありません。

エンド ユーザは、右クリック コンテキスト メニューを使用して、誤分類されたメールにマークを付けることもできます。



スパム レポートの暗号化の設定

スパム レポートの暗号化を有効または無効にするには、アカウントの config_{N} ファイルの「reporting」セクションで次の 2 つのオプションを設定します。

- [format]：レポートのフォーマットを定義します。次の値をサポートしています。
  - [encrypted]：送信前にレポートが暗号化されます。
  - [plain]：暗号化せずにレポートが送信されます。

デフォルトの値は encrypted です。

- [subject]：レポートの件名を定義します。「${reportType}」という文字列を含めると、件名にレポートタイプ（スパム、ハム、ウイルス、フィッシング、マーケティング）を含めることができます。

スパム レポートのトラッキングの設定

スパム、ウイルス、フィッシング、またはマーケティングとマークされたメッセージをトラッキングするには、アカウントの config_{N} ファイルで次のパラメータを設定します。

copyAddressInPlainFormat：スパム レポートのコピーがプレーン（.raw）形式でカスタム電子メール アドレスに送信されるように指定します。

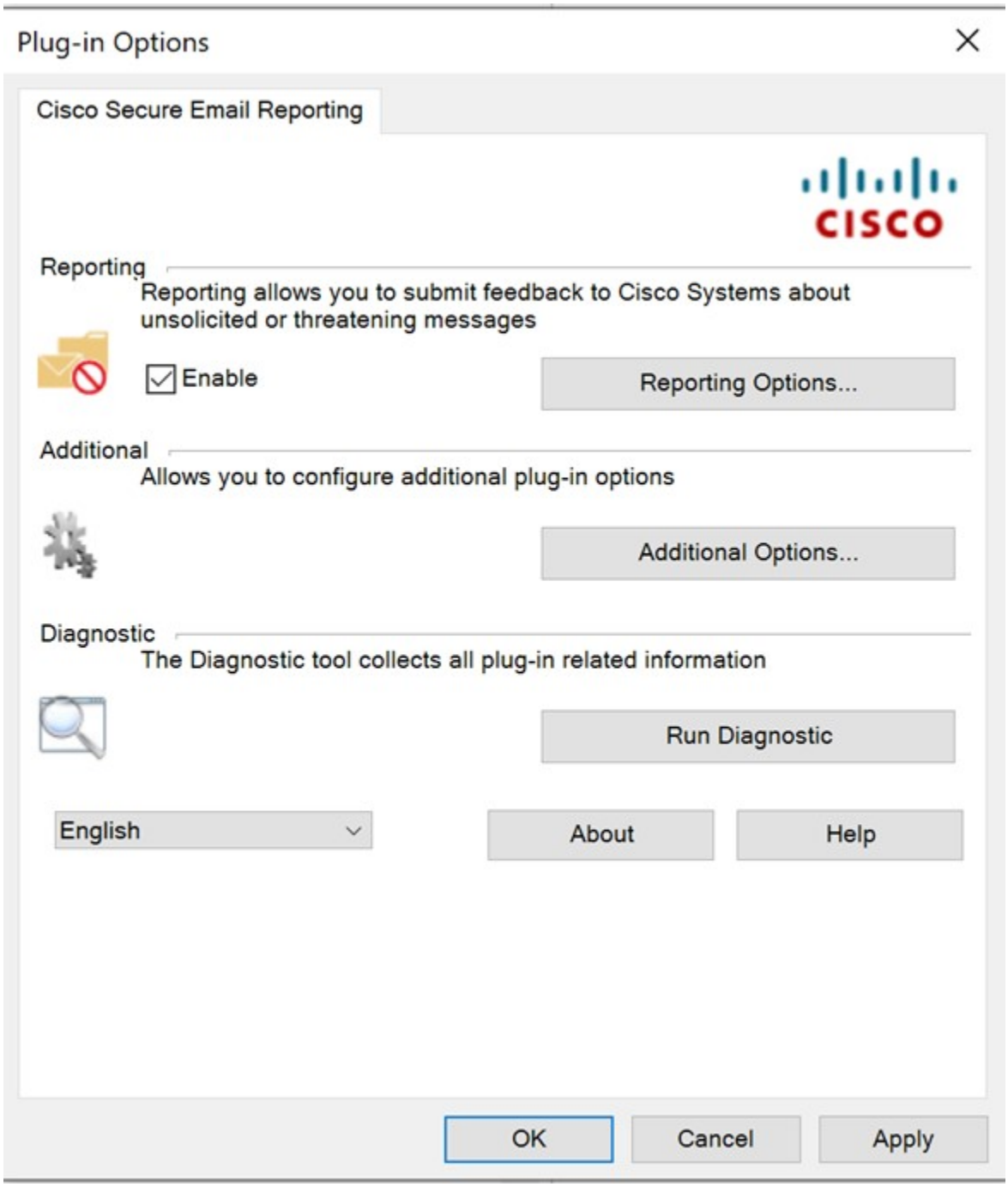
追加設定の変更

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 Reporting] 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 [プラグインオプション（Plug-in Options）] ボタンをクリックするか、[ファイル（File）] > [オプション（Options）] > [アドイン（Add-ins）] > [アドインオプション（Add-in Options）] > [Cisco Email Reporting] > [追加オプション（Additional Options）] を選択します。

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



[Logging] タブ

エンド ユーザは [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 Reporting Plug-in のロギングを有効にする場合に選択します。
Log file name	%ALLUSERSPROFILE%\Cisco\Cisco Email Reporting Plug-in\<username> に保存されているログファイルの名前を指定します。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	次のログレベル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 Reporting 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 [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	製品の改善に使用するデータを、Cisco Secure Email Reporting Plug-in が収集できるようにします。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 [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。

エラーとトラブルシューティング

この項では、Cisco Secure Email Reporting Plug-in for Outlook の使用中に発生し得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 Reporting Plug-in が機能しなくなった場合、エンド ユーザは修復プロセスを実行できます。Cisco Secure Email Reporting Plug-in for Outlook ファイルの修復 （18 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 Reporting 診断ツールの実行 （19 ページ）」を参照してください。

Outlook の起動時に発生するエラー

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、または %ALLUSERSPROFILE%\Cisco\Cisco Email Reporting Plug-in\<*username*> フォルダ内の一部のコンフィギュレーション ファイルが破損している場合に表示されます。

ソリューション

Cisco Secure Email Reporting Plug-in は、破損したコンフィギュレーション ファイルに含まれている一部のレポートオプションのデフォルト値を復元しません。代わりに、一部のレポート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 Reporting Plug-in for Outlook ファイルの修復 （18 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.

ソリューション

Cisco Secure Email Reporting Plug-in は、破損したコンフィギュレーション ファイルに含まれている一部のレポートオプションのデフォルト値を復元しません。代わりに、破損した値やタグをデフォルト値に設定します。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 Reporting Plug-in for Outlook ファイルの修復 （18 ページ）」を参照してください。

メッセージ報告エラー

Outlook が 1 つ以上の名前を認識しない

エンドユーザが Outlook で [Spam]、[Virus]、[Phish]、[Marketing] または [Not Spam] ボタンをクリックすると、次のメッセージが表示されることがあります。

There was error during email reporting. Description: Outlook does not recognize one or more names.

このエラーは、エンド ユーザがレポート プラグインを使用しており、電子メール メッセージの報告を試みているときに、Outlook がそのメッセージの形式を認識できない場合に発生します。エンドユーザは、スパムやフィッシング メールを報告できるように（および、正当なメールを「非スパム」と報告できるように）、レポート プラグイン ファイルを修復する必要があります。

ソリューション

修復プロセスを実行します。「Cisco Secure Email Reporting Plug-in for Outlook ファイルの修復 （18 ページ）」を参照してください。

サーバに接続できない

エンドユーザが Outlook で [スパム（Spam）]、[ウイルス（Virus）]、[フィッシング（Phish）]、[マーケティング（Marketing）] または [スパムではありません（Not Spam）] プラグイン ボタンをクリックし、IMAP プロトコルまたは「headers only」Outlook プロパティを使用すると、次のメッセージが表示されることがあります。

Error: The connection to the server is unavailable. Outlook must be online or connected to complete this action.

このエラーは、エンドユーザが部分的に（ヘッダーのみ）ダウンロードしたメッセージの報告を試み、メール サーバへの接続が切断された場合に発生します。レポート プラグインでは、部分的にダウンロードしたメッセージは報告できません。報告するメッセージ全体がダウンロードされるまで、メール サーバへの接続が試みられます。

ソリューション

ヘッダーだけのメッセージを報告するには、事前にOutlookをメールサーバに接続しておく必要があります。

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

Cisco Secure Email Reporting 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 Reporting Plug-in] を見つけて、[アンインストール/変更（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。

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 Reporting 診断ツールの実行 （19 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 Reporting 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 Reporting Plug-in に関する問題が発生した場合、エンドユーザ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 Reporting Plug-in for Outlook ファイルの修復 （18 ページ）またはCisco Secure Email Reporting 診断ツールの実行 （19 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 （16 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 Reporting 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。

- COM コンポーネントに関する登録情報
- 環境変数
- Cisco Secure Email Reporting 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
- その他の 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 Reporting 診断ツールの実行

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

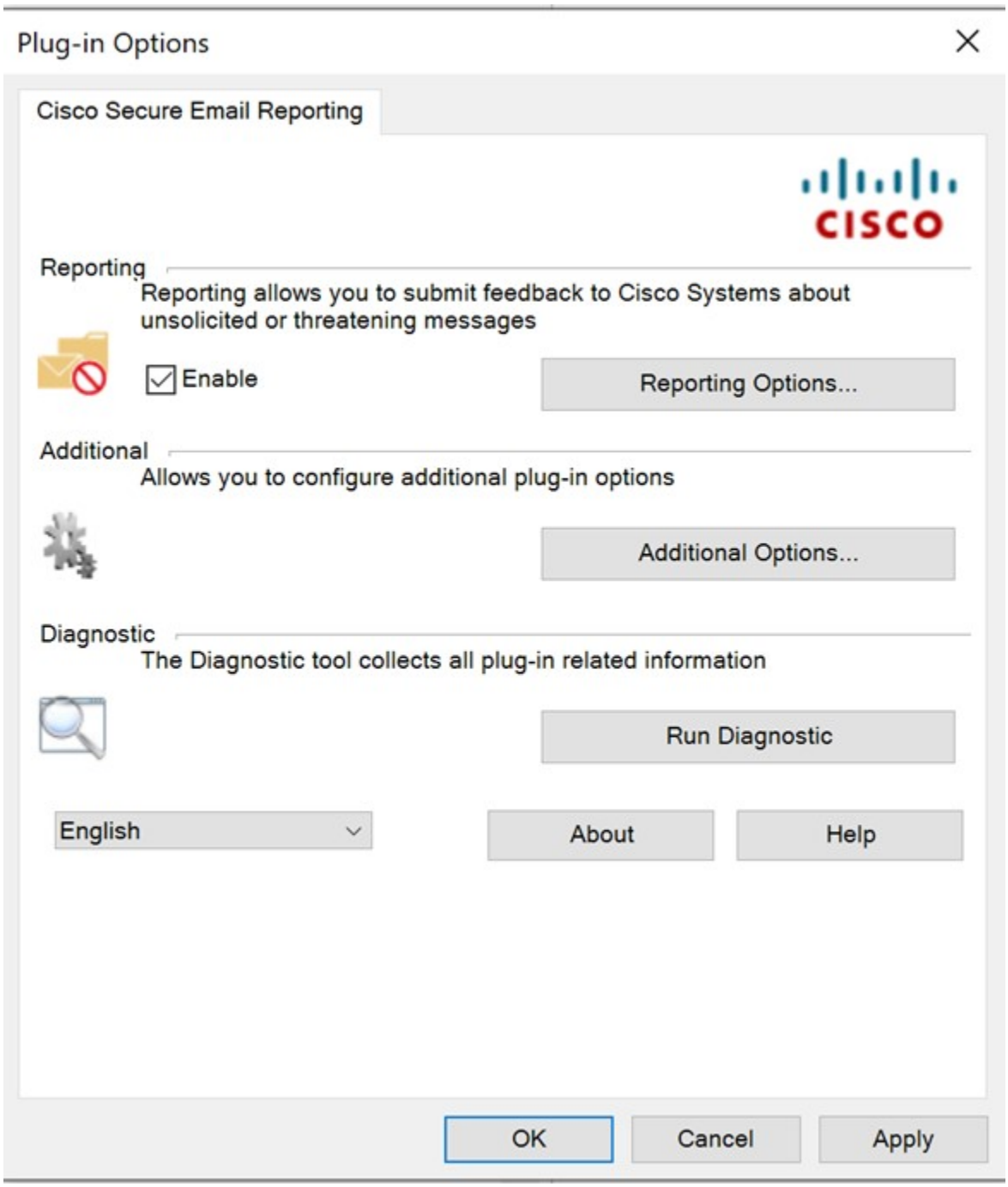
- Cisco Secure Email Reporting の [Options] タブから。通常は、Cisco Secure Email Reporting の [Options] タブから診断ツールを実行します。
- **Program Files**\Cisco Email Reporting Plug-in **フォルダ（通常は C:\Program Files\Cisco\Cisco Email Reporting Plug-in）から。**これは、Cisco Secure Email Reporting Plug-in がインストールされているフォルダです。
- [スタート（Start）] メニュー > [すべてのプログラム（All Programs）] > [Cisco Email Reporting Plug-in] > [Cisco Email Reporting Plug-in 診断（Cisco Email Reporting 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、Outlook 2010/2013/2016 ではリボンの [プラグインオプション（Plug-in Options）] ボタンをクリックするか、[ファイル（File）] > [オプション（Options）] > [アドイン（Add-ins）] > [アドインオプション（Add-in Options）] > [Cisco Email Reporting] > [診断の実行（Run Diagnostic）] を選択します。

Cisco Secure Email Reporting 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、*CiscoReportingDiagnosticReport.zip* ファイルが生成され、現在のユーザの **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、*CiscoReportingDiagnosticsReport.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。

- [スタート（Start）] > [プログラム（Programs）] > [Cisco Email Reporting Plug-in] > [Cisco Email Reporting Plug-in診断（Cisco Email Reporting Plug-in Diagnostic）] から診断ツールを実行します。

または

- Cisco Secure Email Reporting 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 Reporting Plug-in）に移動し、Cisco.EmailReporting.Framework.Diagnostic.exe ファイルをダブルクリックします。

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

Cisco Email Reporting Plug-in をアンインストールするには、[コントロールパネル（Control Panel）] > [プログラムの追加と削除（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
- [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いくつか。

（注） プラグインに関連するすべてのファイルが削除されるわけではありません。

- 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 Reporting 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。

Cisco Secure Email Reporting Plug-in for Outlook をアンインストールするには、次の 2 つの方法があります。

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 Email Reporting Plug-in] を選択し、[アンインストール/変更（Uninstall/Change）] > [次へ（Next）] > [削除（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、[削除（Remove）] オプションを選択して Cisco Secure Email Reporting Plug-in をアンインストールします。