Cisco IronPort Email Security Plug-in 7.3 管理者ガイド

2013 年 5 月 1 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

【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、米国シスコシステムズ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。

Cisco IronPort Email Security Plug-in 7.3 管理者ガイド

CONTENTS

CHAPTER 1

Cisco IronPort Email Security Plug-in の準備

この章の内容は、次のとおりです。

このリリースの新機能

このリリースには、次の新機能が含まれています。

- Cisco Ironport Email Security Plug-in の設定から、Cisco Ironport 暗号化アプライアンス（IEA）または Cisco Registered Envelope Service（CRES）をホステッド キー サーバとして使用するように指定可能。
- Outlook 2010 64 ビットのサポート。
- **自動設定。**Cisco Ironport Email Security Plug-in は、管理者から受信した XML 添付ファイルによって自動的に設定されます。
- **電子メール アカウントごとの設定。**Cisco Ironport Email Security Plug-in は、電子メール アカウントごとの設定を決定する 3 種類のモード（Decrypt Only、Flag、Encrypt）で展開されます。

- **デスクトップ暗号化のセキュア エンベロープ オプション**。
  - **暗号化された電子メールのロックまたはロック解除**。エンド ユーザは、暗号化された電子メールをロックまたはロック解除できます。また、暗号化された電子メールをロックする理由を設定したり変更したりすることができます。
  - **暗号化された電子メールの失効日時の設定** エンド ユーザは、失効日時を設定したりクリアしたりすることができます。

サポートされている構成

『*CCisco Encryption Compatibility Matrix*』にはサポートされているオペレーティング システムが掲載されており、次の URL からアクセスできます。

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

関連資料

暗号化プラグインを使用するには、暗号化プラグインと連携するように適切に設定された Cisco IronPort 暗号化アプライアンスを実行しているか、Cisco Registered Envelope Service（CRES）アカウントを所有している必要があります。Cisco IronPort Encryption アプライアンスの設定方法の詳細については、次のマニュアルを参照してください。

- *『IronPort Encryption Appliance Installation 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。次を参照してください。

http://www.cisco.com/en/US/products/ps10154/prod_installation_guides_list.html

Cisco IronPort Email Security の動作についての理解を深めるために、電子メールをスパム、ウイルス、または非スパムとして分類する方法に関する基本情報を確認することを推奨します。これらのテーマの詳細については、次のマニュアルを参照してください。

- *『Cisco IronPort AsyncOS for Email Configuration Guide』*。このマニュアルでは、スパムおよびウイルスからの保護について説明しています。ユーザは、スパムとウイルス用のプラグインを使用して SenderBase ネットワークの効率を向上させることができます。電子メールに「スパム」、「ウイルス」、または「非スパム」のマークを設定することによって、フィルタの効果を高め、すべての Cisco IronPort アプライアンスのパフォーマンスを向上させることができます。次を参照してください。

http://www.cisco.com/en/US/products/ps10154/products_user_guide_list.html

このマニュアルの使い方

このマニュアルは、Cisco IronPort Email Security Plug-in の機能について学習するためのリソースとして使用してください。マニュアルの内容は論理的な順序で構成されていますが、すべての章を読む必要はありません。目次およびこのマニュアルの構成（1-3 ページ）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バージョンは、Cisco IronPort カスタマー サポート ポータルで入手できます。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 では、[Tools] > [Options] > [Cisco Email Security] の順に移動します。Outlook で [Help] ボタンをクリックして、[Actions] > [Cisco Email Security] をクリックします。
- Outlook 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] > [Help] の順に移動します。

このマニュアルの構成

第 1 章「Cisco IronPort Email Security Plug-in の準備」では、Cisco IronPort セキュリティ プラグインの概要について説明し、ネットワーク セキュリティ設定で主要機能および役割を定義します。最新リリースの新機能、その他の情報リソース、およびサポート問い合わせ情報について説明します。

第 2 章「概要」では、レポート プラグインと暗号化プラグインについて紹介します。この項には各ツールの概要が示されています。

第 3 章「一括インストールの実行」では、一括インストールの実行方法について説明します。インストールを実行する手順が示されています。

第 4 章「Cisco IronPort Email Security Plug-in for Outlook の設定と使用」では、Cisco IronPort Email Security Plug-in for Outlook の設定手順について説明します。暗号化プラグインのインストール、暗号化された電子メールの送受信、セキュア メッセージの管理に関する手順も含まれています。

付録 A「Cisco IronPort Systems, LLC Software License Agreement」には、Cisco IronPort 製品の使用許諾契約に関する詳細な情報が掲載されています。

詳細情報の入手先

シスコでは、Cisco IronPort Email Security Plug-in について理解を深めるための次のリソースを用意しています。

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。登録と一般トレーニングに関しては、次の URL でアクセスしてください。

- http://training.ironport.com
- stbu-trg@cisco.com

認定。認定と認定試験に関しては、次の URL でアクセスしてください。

- http://training.ironport.com/certification.html
- stbu-trg@cisco.com

ナレッジ ベース

次の URL から Cisco IronPort カスタマー サポート サイトの Cisco IronPort ナレッジ ベースにアクセスできます。

http://www.cisco.com/web/ironport/knowledgebase.html

ナレッジ ベースには、Cisco IronPort 製品に関するトピックについて豊富な情報が用意されています。

通常、記事は次のカテゴリのいずれかに分類されています。

- **手順:** 手順の項目では、Cisco IronPort 製品を使用して何かを実行する方法について説明します。たとえば、How-To の記事では、アプライアンス用データベースのバックアップをとり、復元する手順について説明します。
- **問題と解決策:** 問題と解決策の項目では、Cisco IronPort 製品の使用時に発生する可能性があるエラーや問題に対処します。たとえば、Problem-and-Solution の記事では、製品の新バージョンへのアップグレード時に特定のエラーメッセージが表示された場合の対応方法について説明します。
- **参考資料:** Reference の記事は、通常、特定のハードウェアに関連するエラー コードなど情報のリストを提供します。
- **トラブルシューティング:** トラブルシューティングの項目では、Cisco IronPort 製品に関連する一般的な問題を分析し、解決する方法について説明します。たとえば、Troubleshooting の記事は、DNS で問題が発生した場合に従う手順を提供します。

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。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 ユーザや Cisco IronPort ユーザと情報を共有したりできます。

シスコ サポート コミュニティには次の URL からアクセスできます。

https://supportforums.cisco.com

Cisco 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。Cisco IronPort 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 Cisco カスタマーサポートにお問い合わせください。

- Cisco サポート ポータル：http://www.cisco.com/support
- 電話サポート：800-553-2447（米国/カナダ国内）または Worldwide Phone Numbers 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 Content Security にコメントをお寄せください

Cisco Content Security テクニカル マニュアル チームは、製品ドキュメントの向上に努めています。コメントおよびご提案をお待ちしています。コメントは次の電子メール アドレス宛に送信できます。

contentsecuritydocs@cisco.com

Cisco IronPort Email Security Plug-in の概要

Cisco IronPort Email Security Plug-in では、Outlook 電子メール プログラムにレポートと暗号化のメニューがインストールされます。レポート プラグインを使用すると、受信したメールの種類についてフィードバックを送信できます（たとえば、スパム、フィッシング、ウイルスなどが含まれている電子メールを報告できます）。また、暗号化プラグインをインストールすると、ツールバーに [Encrypt Message] ボタンが表示されます。ユーザはこのボタンを使って、電子メール プログラムから暗号化した電子メールを送信したり、組織外に送信する前に暗号化する電子メールにフラグを設定することができます。

Cisco IronPort Email Security Plug-in をインストールすると、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。この単一のインターフェイスを使って、エンドユーザは電子メールをシームレスに報告したり、暗号化された電子メールを送信することができます。エンド ユーザは、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。これらのプラグインを組み合わせると、インストールが簡単になり、ユーザと管理者は 1 つのインターフェイスからインストールや変更を行うことができるようになります。

レポート プラグインおよび暗号化プラグインは、ツールバー ボタンと右クリック コンテキスト メニューを使用してフィードバックおよび暗号化されたメッセージを送信できる便利なインターフェイスです。レポート プラグインを使用してメッセージを報告すると、メッセージが送信されたことを示すダイアログボックスが表示されます。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、送信者は暗号化されたメッセージを簡単に送信できます。暗号化プラグインを使用するには、適切に設定された Cisco IronPort 暗号化アプライアンスが存在しているか、または、Cisco Registered Envelope Service（CRES）のアカウントを所有している必要があります。

CHAPTER 2

概要

Cisco IronPort Email Security Plug-in は、レポート プラグインや暗号化プラグインなど、複数の Cisco IronPort Email Security Plug-in をサポートするフレームワークです。

この章の内容は、次のとおりです。

Cisco IronPort Email Security Plug-in

Cisco IronPort Email Security Plug-in は、よく使用される 2 つの電子メール セキュリティ プラグイン（レポート プラグインと暗号化プラグイン）から構成されています。Cisco IronPort Email Security Plug-in は Outlook 電子メール プログラムに導入できます。Cisco IronPort Email Security Plug-in を導入すると、次のアプリケーションのいずれか（または両方）がインストールされます。

- **Reporting Plug-in**：レポート プラグインを使用すると、Outlook ユーザは、スパム、ウイルス、フィッシング メッセージなど、一方的に送りつけられる不要な電子メール メッセージについて Cisco IronPort Systems にフィードバックを送信できます。詳細については、レポート プラグイン（2-2 ページ）を参照してください。
- **Encryption Plug-in**：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、送信者は暗号化が必要なメッセージを簡単にマークできます。詳細については、暗号化プラグイン（2-3 ページ）を参照してください。

レポート プラグイン

レポート プラグインを使用すると、Outlook ユーザは、スパム、ウイルス、フィッシング メッセージなど、一方的に送りつけられる不要な電子メール メッセージについて Cisco IronPort Systems にフィードバックを送信できます。Cisco IronPort では、このフィードバックを活用してフィルタを更新し、不要なメッセージが受信トレイに配信されないようにします。

さらに、[Not Spam] ボタンを使用して、誤検出（誤ってスパムとしてマークされた正当な電子メール メッセージ）を IronPort Systems に報告することもできます。正当な電子メール メッセージは「ハム」とも呼ばれます。シスコでは、誤検出に関するレポートを活用してスパム フィルタを調整し、今後、正当な電子メールが誤分類されないようにします。あらゆる正当な電子メールを「**非スパム**」として報告できるので、フィルタの効率向上に役立ちます。

このプラグインは、ツールバー ボタンと右クリック コンテキスト メニューを使用してフィードバックを送信できる便利なインターフェイスです。メッセージを報告すると、メッセージが送信されたことを示すダイアログ ボックスが表示されます。送信したメッセージ データは、Cisco IronPort フィルタを改善するために自動システムによって使用されます。メッセージ データを提出することで、受信ボックスに一方的に送りつけられるメールの量を削減できます。

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、暗号化する電子メールにフラグを設定できます。電子メールは、Cisco IronPort 暗号化アプライアンスまたは電子メール セキュリティ アプライアンスによって暗号化されてから、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、Cisco IronPort 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 IronPort 暗号化アプライアンス、または Cisco IronPort 電子メール セキュリティ アプライアンス（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。

プラグインのインストール

ユーザ グループ向けに Cisco IronPort Email Security 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、第 3 章「一括インストールの実行」を参照してください。

コンフィギュレーション モード

Cisco IronPort Email Security Encryption Plug-in は 3 種類のコンフィギュレーション モードで導入されます。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 ユーザの電子メール アカウントに *BCE_Config_signed.xml* 添付ファイルを送信します。エンド ユーザはこのファイルを *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） デフォルトのエンベロープ名は *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エンベロープに反映されます。

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。フラグ オプションを使用すると、エンド ユーザは暗号化が必要な電子メールにフラグを設定できます。電子メールは、Cisco IronPort 暗号化アプライアンスまたは電子メール セキュリティ アプライアンスによって暗号化されてから、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で復号化できるようサーバ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
電子メールのロックおよびロック解除			X

機能	Decrypt Only	Decrypt and Flag	Decrypt and Encrypt
電子メールの有効期限			X
電子メールの診断（レポート プラグインと暗号化プラグインで使用）	X	X	X
開封確認			X
エンベロープ設定			X
設定	X	X	X

Cisco Registered Envelope Service（CRES）キー サーバ用の Cisco IronPort Email Security Plug-in の導入

Cisco IronPort Email Security Plug-in を Cisco Registered Email Service（CRES）キー サーバで直接使用できるようにするには、次の手順に従って導入します。

まず、https://res.cisco.com/admin で CRES アカウントにログインし、[Accounts] タブに移動します。Email Security 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 1　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 サーバが CRES の場合に選択します。
  - [SecureCompose]：CRES トークンとしてこのオプションを選択しないでください。
  - [Token <Account number>]：CRES トークンとしてこのオプションを選択します。

ステップ 2　[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 3　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 4　[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 5　同時に多数のエンド ユーザ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。

a. ステップ 4 で作成した *BCE_Config_signed.xml* ファイルの場所を参照します。

b. エンド ユーザの電子メール 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。

c. 必要に応じて電子メールの件名を変更します。

d. [Distribute Config] をクリックします。

（注）　XML コンフィギュレーション ファイルが他のエンド ユーザに転送された場合は、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、エラーが返されます。

（注）　メーリング リスト宛てに *BCE_Config_signed.xml* ファイルを送らないでください。CRES はメーリング リストに対応していません。

IronPort 暗号化アプライアンス（IEA）キー サーバ用の Cisco IronPort Email Security Plug-in の導入

IEA キー サーバのトークンのダウンロード

設定に署名するプロセスでは IEA トークンを使用する必要があります。コンフィギュレーション ファイルに署名する前に、ローカル マシンにトークンをダウンロードします。

IEA キー サーバからトークン ファイルをダウンロードするには、次の手順を実行します。

ステップ 1　IEA 管理コンソールにログインします：https://<IEA_hostname>/admin。管理コンソールが表示されます。

ステップ 2　[Accounts] タブに移動します。プラグインのインストールに使用するアカウントに移動します。通常、これは **Users** アカウントです。

ステップ 3　[Tokens] タブに移動します。トークンの右側にある [Save Token] アイコン（下矢印が付いた円形のアイコン）をクリックし、トークンをローカル マシンに保存します。

コンフィギュレーション ファイルのカスタマイズと署名

IEA トークン ファイルをダウンロードすると、コンフィギュレーション ファイルをカスタマイズして署名できるようになります。Cisco Registered Envelope Service（CRES）は、Cisco IronPort 暗号化テクノロジーをサポートするホスト サービスです。プラグイン コンフィギュレーション ファイルの署名の検証は CRES システムによって行われるため、キー サーバとして IEA を使用しているユーザが Cisco IronPort Email Security Plug-in を導入する場合は、CRES の管理者アカウントも必要です。専用に作成された CRES 管理者アカウントが必要な場合は、次の Cisco IronPort カスタマー サポートにお問い合わせください：http://www.cisco.com/web/ironport/index.html

IEA キー サーバで使用する署名済みコンフィギュレーション ファイルを作成するには、次の手順を実行します。

ステップ 1　CRES アカウントにログインします：https://res.cisco.com/admin。管理コンソールが表示されます。

ステップ 2　[Accounts] タブに移動し、Email Security 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　トークン タイプとして [IEA] を選択し、前に IEA からダウンロードした IEA トークンをアップロードします。

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。

（注）　IEA をキー サーバとして使用する場合は、BCE 設定タブ [Distribute Signed Configuration File to Bulk List]（オプション）で ステップ 5 を実行しないでください。このオプションは CRES にのみ適用され、今後のリリースで削除される予定です。

エンド ユーザへのコンフィギュレーション ファイルの展開

エンド ユーザにコンフィギュレーション ファイルを展開するには、IEA で暗号化した電子メールによって、署名済みコンフィギュレーション ファイルを各エンド ユーザに送信します。メッセージは、IEA と CRES アカウントで管理者として示される電子メール アドレスから送信する必要があります。

（注） XML コンフィギュレーション ファイルが他のエンド ユーザに転送された場合は、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、エラーが返されます。

（注） メーリング リスト宛てに *BCE_Config_signed.xml* ファイルを送らないでください。CRES はメーリング リストに対応していません。

BCE_Config_signed.xml ファイルを使用して一括インストールを実行するには、BCE_Config.xml ファイルを使用した一括インストール（3-18 ページ）を参照してください。

Cisco IronPort Email Security Plug-in の設定

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

- Outlook 2010 では、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] の順に移動します。
- Outlook 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] の順に移動します。

レポート プラグインのインストールまたは暗号化プラグインのインストールに変更を加えることができます。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 IronPort Email Security Encryption Plug-in のロギングを有効化または無効化したり、特定の暗号化モードのオプションを変更することができます。

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、それらの設定は Cisco IronPort 暗号化アプライアンスと互換性がなければなりません。

Outlook で設定を変更する場合は、第 4 章「Cisco IronPort Email Security Plug-in for Outlook の設定と使用」を参照してください。

Cisco IronPort Email Security Plug-in に必要な TCP/IP サービス

Cisco IronPort Email Security Plug-in では、次の TCP/IP サービスと関連ポートを使用する必要があります。これらのポートは、TCP/IP サービスで使用できる状態のままにしておく必要があります。

- DNS（ドメイン ネーム システム）。

  DNS サービスは、インターネット ドメイン名とホスト名を IP アドレスに変換します。DNS は、Web ブラウザのアドレス バーに入力された名前を、それらのサイトをホストしている Web サーバの IPアドレスに自動的に変換します。

  ポート番号：53（TCP/UDP）

  詳細については、次のサイトを参照してください。
  http://en.wikipedia.org/wiki/Domain_Name_System

  影響：大

  処置：このサービスは、すべてのエンド ユーザに対してアクセス可能にする必要があります。

- SMTP（Simple Mail Transfer Protocol）

  Simple Mail Transfer Protocol（SMTP）は、インターネット プロトコル（IP）ネットワークを介して電子メール（E メール）を伝送するためのインターネット標準です。

  ポート番号：25、587、465、475、2525（TCP）

  詳細については、次のサイトを参照してください。
  http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

  影響：大

処置：このサービスは、すべてのエンド ユーザに対してアクセス可能にする必要があります。

- DHCP（ダイナミック ホスト コンフィギュレーション プロトコル）

  DHCP は、ネットワーク（ホスト）に接続するデバイスの設定に使用されるネットワーク プロトコルです。これによって、デバイスはインターネット プロトコル（IP）を使用してネットワーク上で通信できるようになります。

  ポート番号：67、68（TCP/UDP）

  詳細については、次のサイトを参照してください。
  http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

  影響：大

  処置：このサービスは、DHCP サーバから IP アドレスを自動取得するエンド ユーザ全員に対してアクセス可能にする必要があります。

- Net BIOS over TCP/IP

  NetBIOS over TCP/IP（NBT または NetBT）は、NetBIOS API を利用しているレガシー コンピュータ アプリケーションで最新の TCP/IP ネットワークを使用できるようにするネットワーク プロトコルです。

  ポート番号：137（UDP）（ネーム サービス）、138（UDP）（データグラム サービス）、139（TCP）（セッション サービス）

  詳細については、次のサイトを参照してください。
  http://en.wikipedia.org/wiki/NetBIOS_over_TCP/IP

  影響：大

  処置：このサービスは、すべてのエンド ユーザに対してアクセス可能にする必要があります。

- HTTP（Hypertext Transfer Protocol）

  Hypertext Transfer Protocol（HTTP）は、コラボレーション ハイパーメディア分散情報システム用のアプリケーション プロトコルです。

  ポート番号：80、8080（TCP）

  詳細については、次のサイトを参照してください。
  http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

  影響：大

  処置：このサービスは、すべてのエンド ユーザに対してアクセス可能にする必要があります。

- HTTPS（Hypertext Transfer Protocol Secure）

  HTTPS は、コンピュータ ネットワーク上で安全に通信するための通信プロトコルであり、特にインターネット全体にわたって展開されています。

  ポート番号：443（TCP）

  詳細については、以下を参照してください。
  http://en.wikipedia.org/wiki/HTTP_Secure

  影響：大

  処置：このサービスは、すべてのエンド ユーザに対してアクセス可能にする必要があります。

- IMAP（Internet Message Access Protocol）

  Internet Message Access Protocol によって、電子メール クライアントはリモート メール サーバ上の電子メールにアクセスできます。

  ポート番号：143、993（TCP）

  詳細については、次のサイトを参照してください。
  http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

  影響：大

  処置：このサービスは、すべてのエンド ユーザに対してアクセス可能にする必要があります。

- POP3（Post Office Protocol）

  Post Office Protocol は、TCP/IP 接続を介してリモート サーバから電子メールを取得するために、電子メール クライアントによって使用されます。

  ポート番号：110、995（TCP）

  詳細については、次のサイトを参照してください。
  http://en.wikipedia.org/wiki/Post_Office_Protocol

  影響：大

  処置：このサービスは、すべてのエンド ユーザに対してアクセス可能にする必要があります。

CHAPTER 3

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を実行する方法について説明します。内容は次のとおりです。

インストールの実行

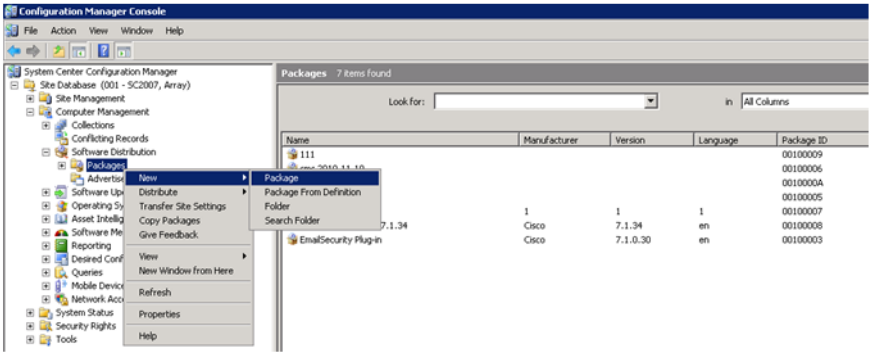
インストールを実行するには、次の手順を実行して、ネットワーク共有フォルダ、配布パッケージ、新しいパッケージのウィザード、新しいプログラムのウィザードを作成します。

インストールを実行するには次の手順を実行します。

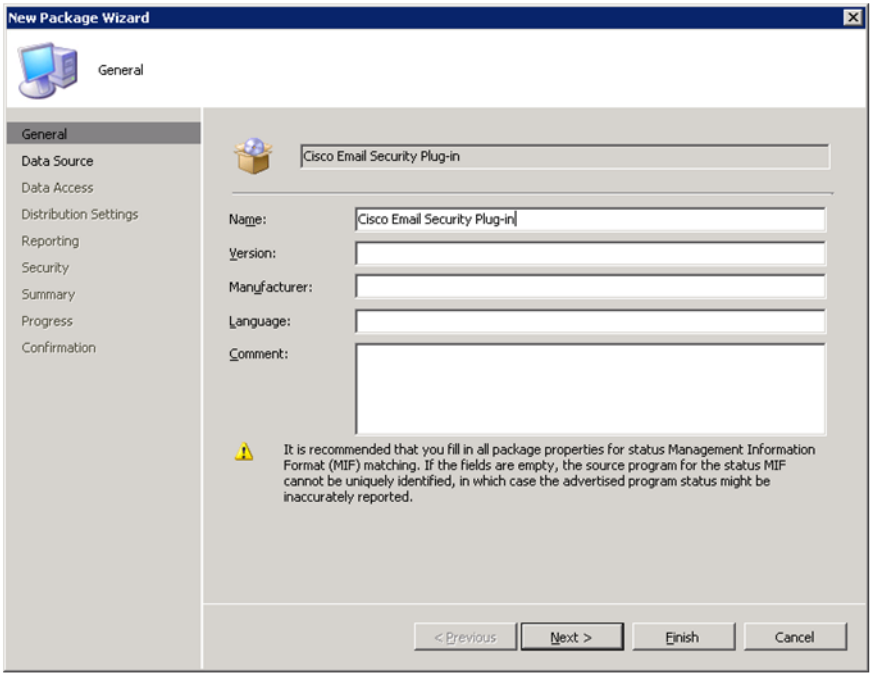
ステップ 1 インストール パッケージを含むネットワーク共有フォルダを作成し、ユーザに対して共有フォルダへのアクセス権限を付与します。

ステップ 2 SCCM 管理ツールを開きます。

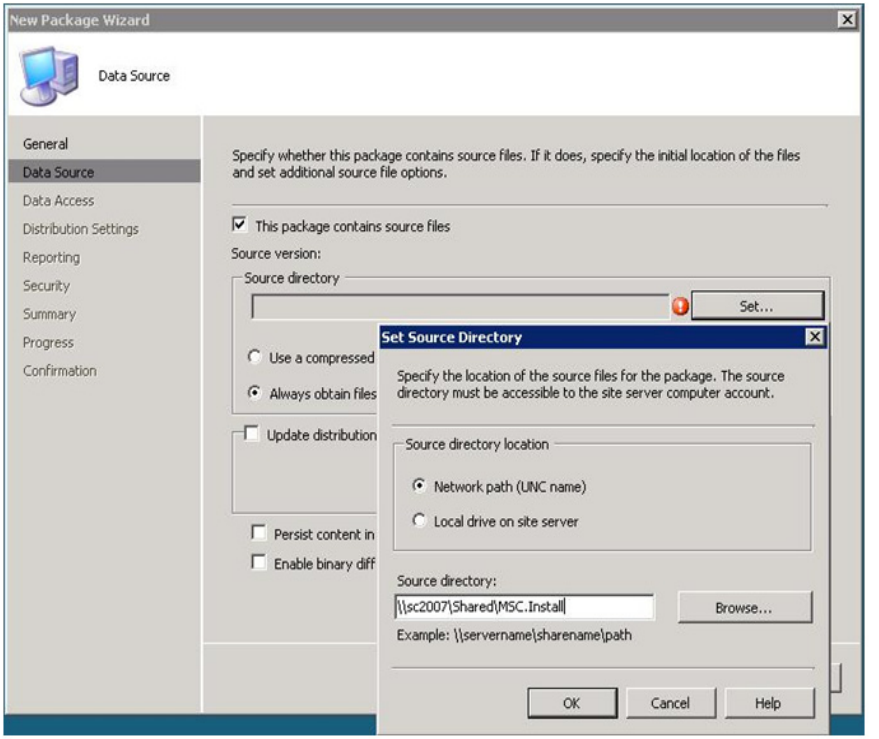
ステップ 3　新しいソフトウェア配布パッケージを作成します。



ステップ 4　パッケージの名前を入力し、[Next] をクリックします。

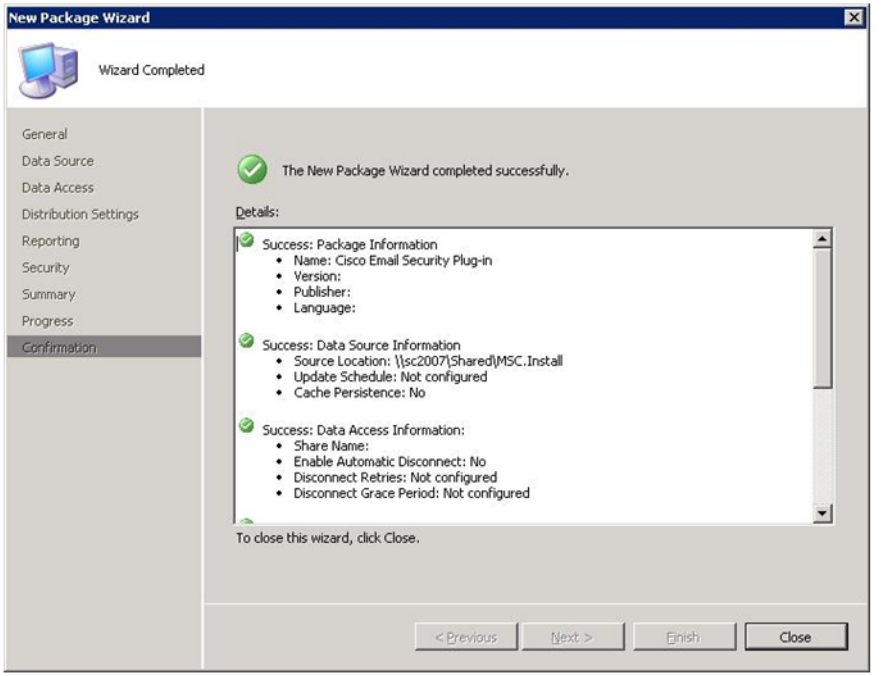


ステップ 5　ネットワーク共有フォルダへのパスを入力して、ステップ 1 で作成したネットワーク ソース ディレクトリを指定します。フォルダへのパスを入力するか、フォルダを参照します。[Next] をクリックします。

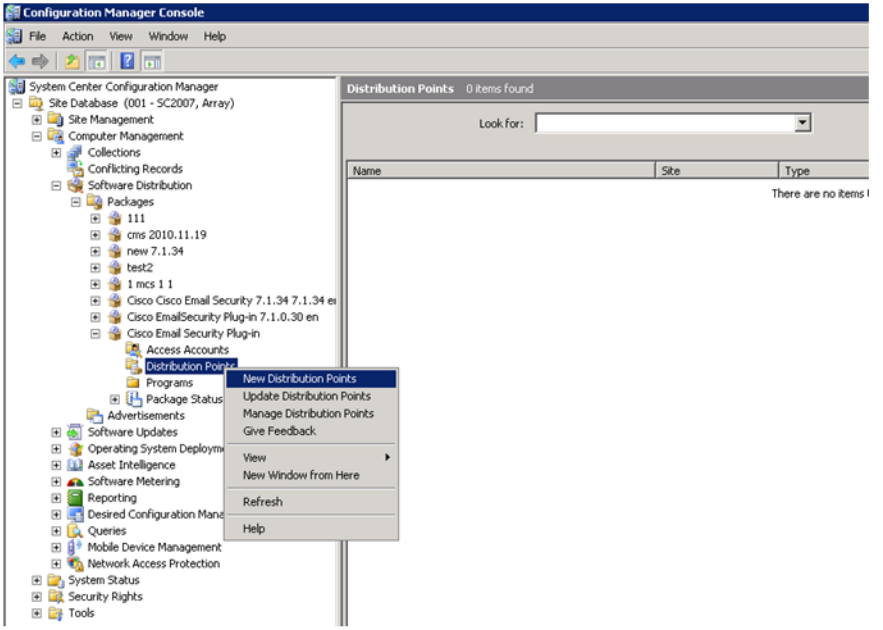


ステップ 6　[New Package Wizard] で次のステップに進み、[Next] をクリックします。

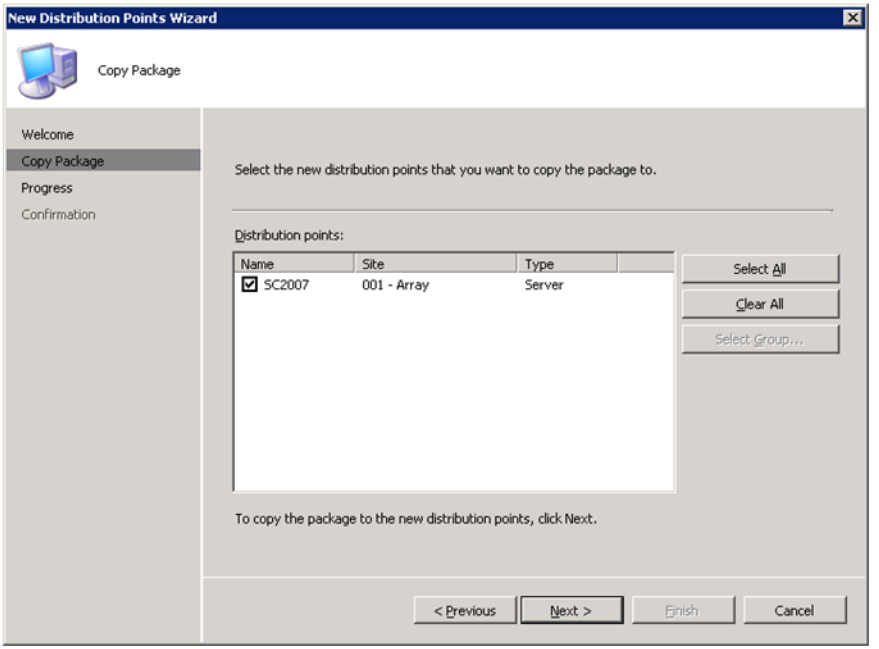
ステップ 7　[New Package Wizard] が正常に完了したことを確認して、[Close] をクリックします。



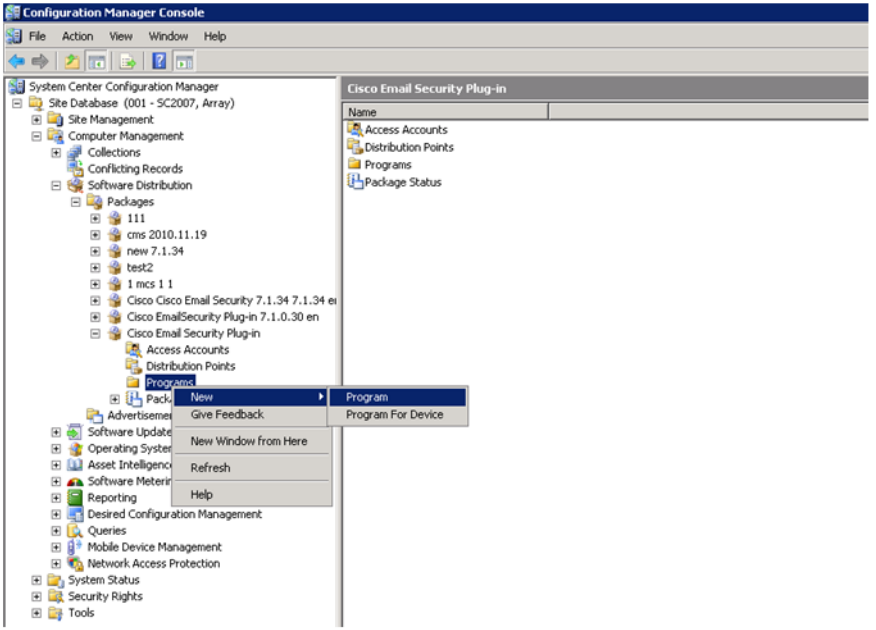
ステップ 8　新しい分散ポイントを作成し、[Welcome] ページの [Next] をクリックします。



ステップ 9　新しい分散ポイントを選択します。[New Distribution Points Wizard] で以降のページをクリックして、[Close] をクリックします。

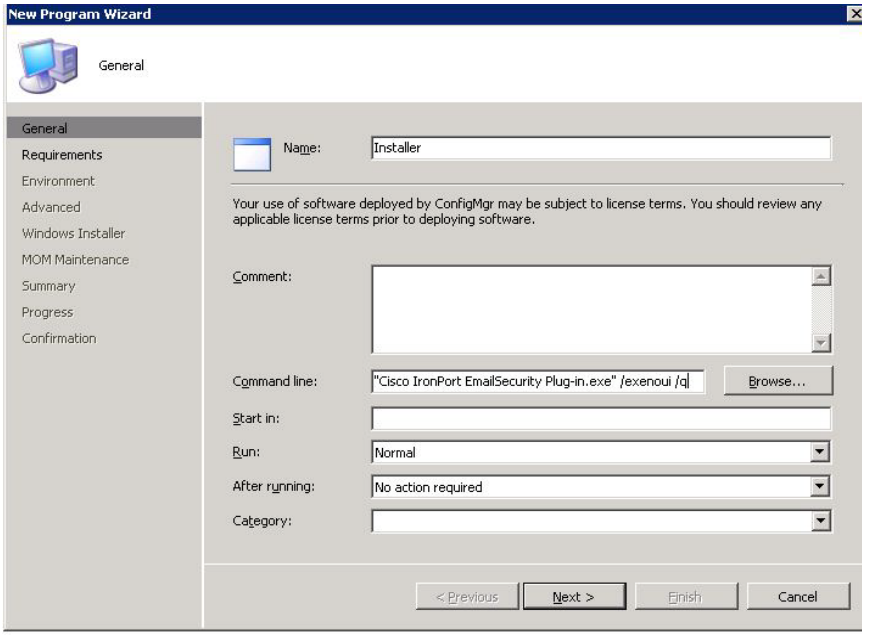


ステップ 10　新しいプログラムを作成します。



ステップ 11　コマンドライン フィールドに、次のコマンドを入力します。*{共有のネットワーク パス}\Cisco IronPort Email Security Plug-in.exe /exenoui /qn*

例：*\\sc2007\Shared\Cisco IronPort Email Security Plug-in.exe /exenoui /qn*
\\sc2007\Shared\Cisco IronPort Email Security Plug-in.exe はネットワーク共有フォルダ内の .exe ファイルへのフル ネットワーク パスです。



（注）　カスタマイズされたコンフィギュレーション ファイルを使用する場合は、カスタマイズされたファイルをインストールで使用できるようにする特別なキーをこのステップで追加する必要があります。次の構文を使用して、コマンドラインから（= 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して）特別なキーを追加します。

```
Cisco IronPort Email Security Plug-in.exe /exenoui /qn
UseCustomConfig="\\sc2007\Shared\config\"
```

コンフィギュレーション ファイルのカスタマイズの詳細については、カスタム コンフィギュレーション ファイルの使用（3-15 ページ）を参照してください。

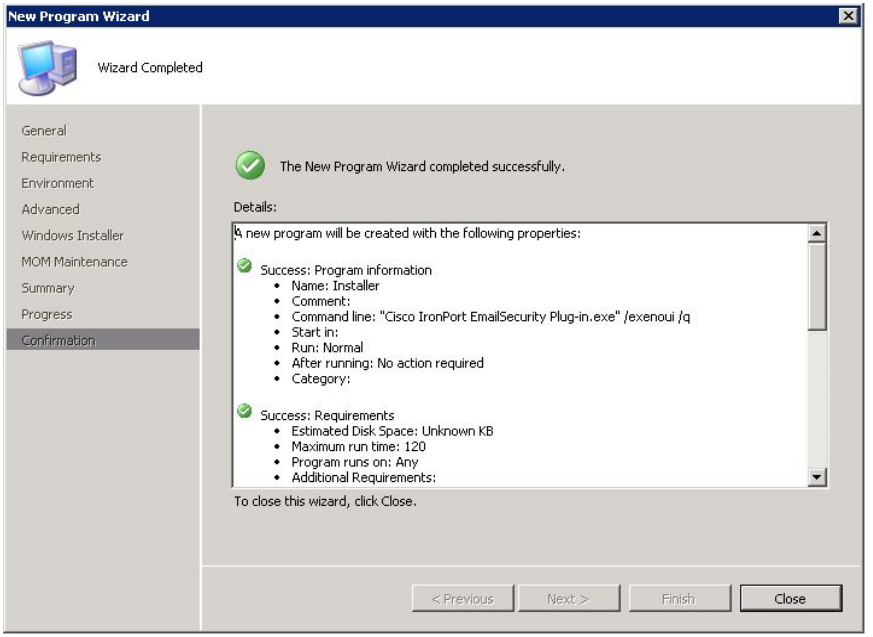
ステップ 12　[Run] フィールドで [Hidden] を選択し、[Next] をクリックします。

ステップ 13　要件ページをクリックして、[Next] をクリックします。

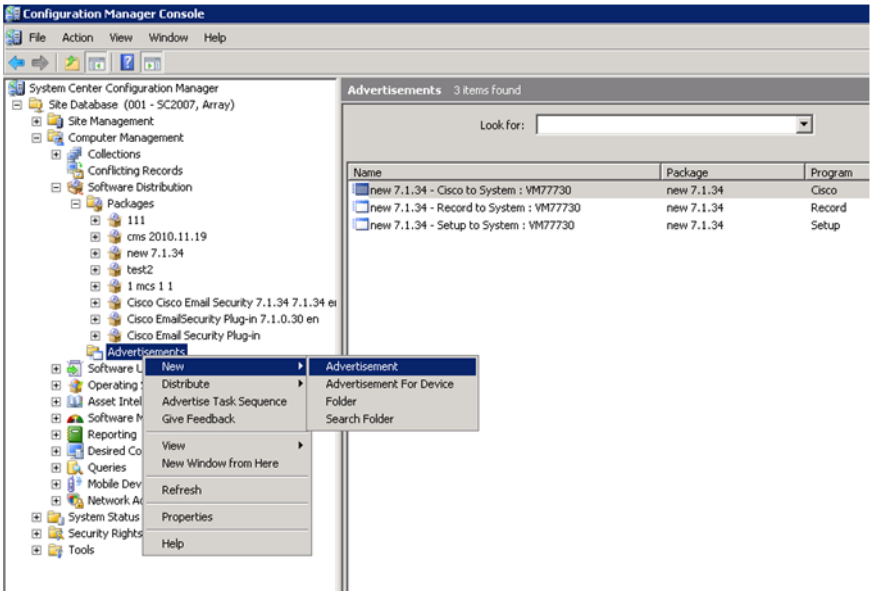
ステップ 14　次の環境オプションを選択します。

- [Program can run]：ユーザのログイン時に限ります。実行モードに管理者権限が設定されている場合は、[Program can run]を [Whenever the user is logged on] に設定できます。
- [Run mode]：ユーザの権限で実行するか、またはユーザが新しいソフトウェアのインストールに必要な権限を持っていない場合は管理権限で実行します。

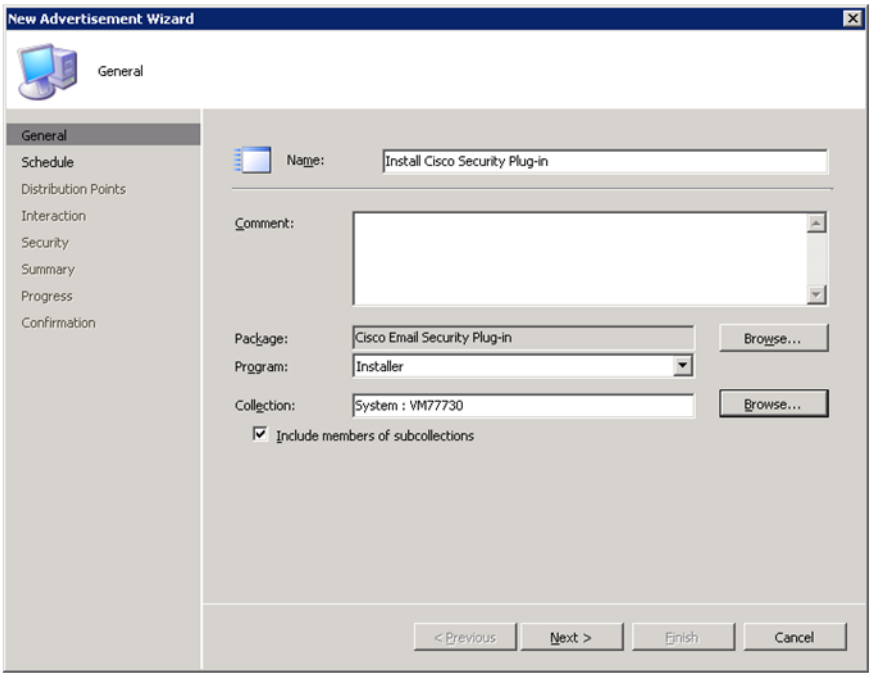
ステップ 15　[New Program Wizard] が正常に完了したことを確認して、[Close] をクリックします。



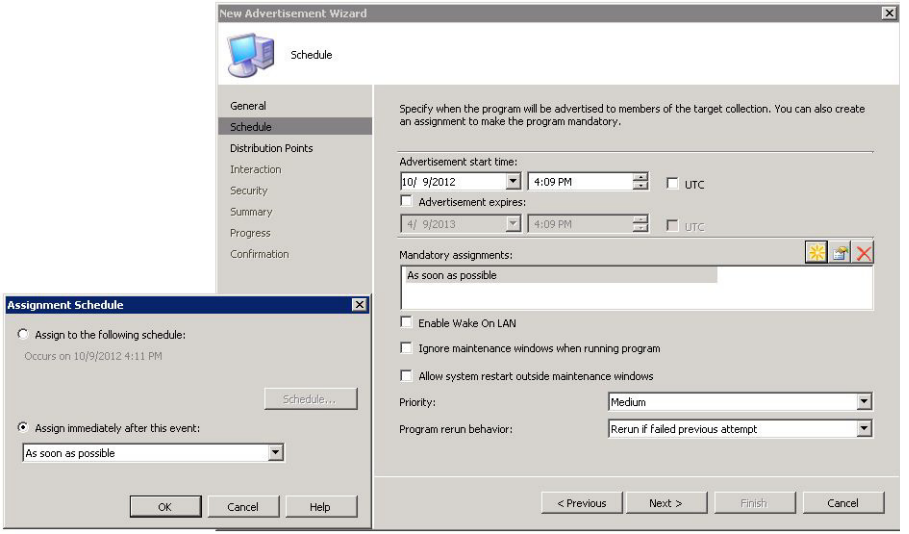
ステップ 16　新しいアドバタイズメントを作成します。



ステップ 17　名前を入力し、作成したパッケージとプログラムを選択します。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る収集を選択して、[Next] をクリックします。



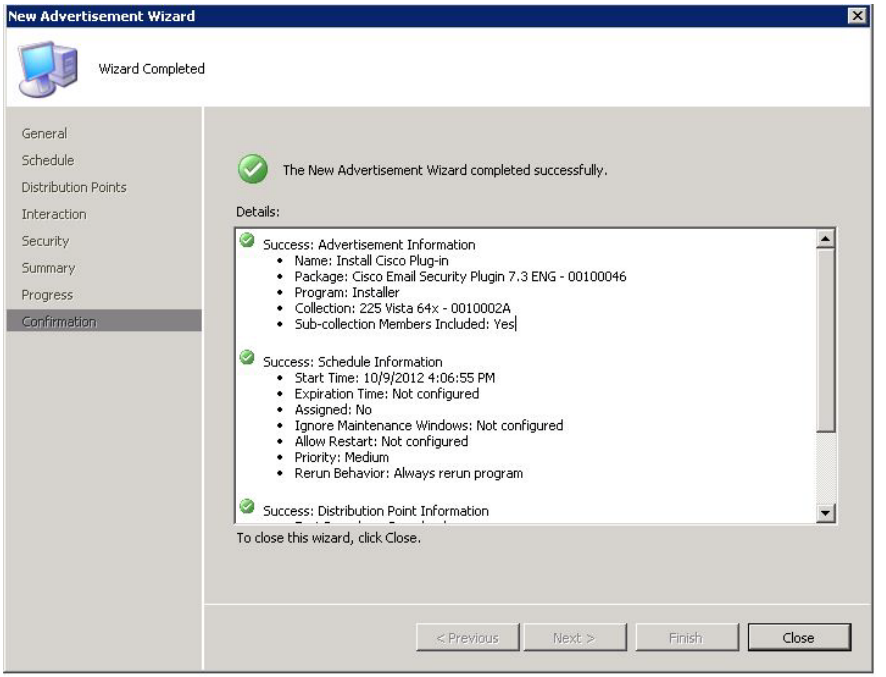
ステップ 18　割り当てを必須として設定します。[Next] をクリックします。



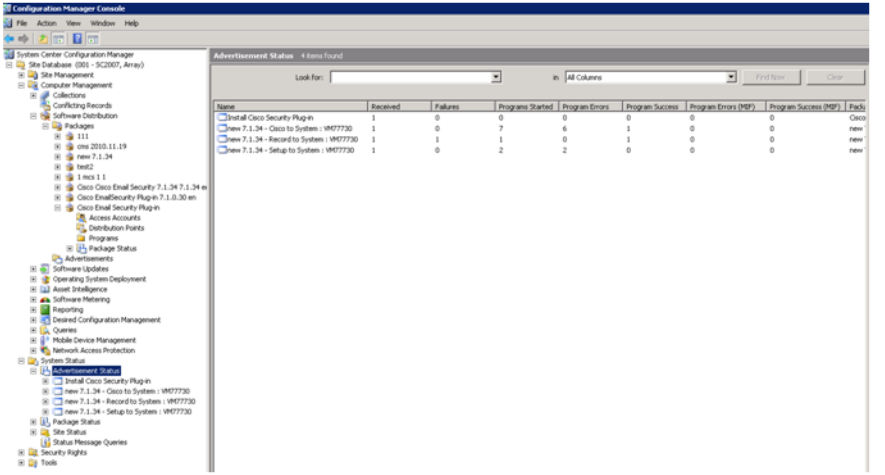
ステップ 19　ユーザ設定に基づいてスイッチを選択します。少なくとも 1 つの必須割り当てを設定する必要があります。[Do Not Run Program] を選択すると、接続速度が遅い場合にプログラムが開始されないため、これを選択しないでください。[Next] をクリックします。

ステップ 20　[New Advertisement Wizard] をクリックし、[Next] をクリックします。

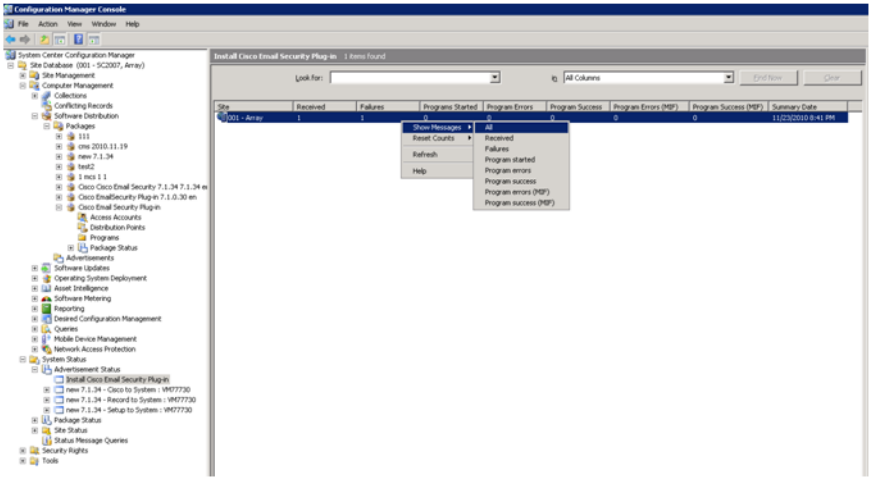
ステップ 1　[New Advertisement Wizard] が正常に完了したこと示す確認を表示して、[Close] をクリックします。



ステップ 2　[Advertisement Status] ウィンドウで [Advertisement Status] を表示します。



ステップ 3　アドバタイズメント レポートを作成して詳細を表示するには、コンテキスト メニューで **[Show message] > [All]** を選択します。エラーが発生した場合は、レポートを調べてエラーが発生した場所を確認できます。



カスタム コンフィギュレーション ファイルの使用

Cisco IronPort Email Security 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、暗号化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)。また、レポート コンフィギュレーション ファイルで、報告用の最大メール サイズ、報告後にファイルのコピーを保持するかどうかなどのデフォルト オプションの一部を変更できます。ボタン名をカスタマイズすること、さらに、ユーザ インターフェイスで使用されてい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 ファイルを変更および展開するには、次の手順を完了します。

ステップ 1　**\\%allusersprofile%\Cisco\Cisco IronPort Email Security 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)　正当性を維持するため、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 IronPort Email Security プラグインのディレクトリで始まる構造を維持していること、コンフィギュレーション ファイルと一緒にすべてのファイルを含めたことを確認します。

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 ファイルに含まれた XML ファイルを変更することをお勧めします。これらのファイルを変更する方法については、XML コンフィギュレーション ファイルの編集(3-16 ページ)を参照してください。

ステップ 3　インストールの実行（3-1 ページ）に説明されている方法で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（3-19 ページ）に説明されている方法でカスタマイズされた 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 IronPort Email Security 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、プラグインにより、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 IronPort Email Security Plug In
```

XML ファイルは、次のデフォルトの場所に配置されます。

- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\CommonEncryptionConfig.xml**：Desktop Encryption プラグインに関連する構成データが含まれます。
- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\config_1.xml, config_{N}.xml**：この番号はユーザ アカウントの数によって異なります。
- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\CommonConfig.xml**：ログ ファイルの場所や、ローカリゼーション ファイルの名前（デフォルトのローカリゼーション ファイルは en-US.xml）など、レポート プラグインと暗号化プラグインの両方に共通する基本的な構成データが含まれます。電子メール プログラムの設定情報を使用してログ ファイルの場所を変更し、一括インストール プログラムと一緒にその設定情報を展開できます。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参照する必要があります。
- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\Reporting.xml**：報告可能な最大メール サイズなど、Reporting Plug-in に関連する設定データが保存されます。このファイルを変更することはお勧めしません。

- **\\%allusersprofile%\Cisco\Cisco IronPort Email Security Plug-In\Common\Localization\en-US.xml**：ローカル言語に関連するデータが含まれます。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-CN.xml を含め、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 ファイルの対象ではない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 ファイルの中で参照できます。

警告　<または > 記号の内側にあるどの文字列 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。

例

次の例は、*en-US.xml* ファイルに変更を加える例を示しています。

レポート ツールバー内のテキストを変更するには、*en-US.xml* という xml ファイルの次のセクションを参照し、太字で表記されているテキストを編集します。

```
<group name="Mso.Report.Button.Cations">
 <string id="blockSender">Block Sender</string>
 <string id="spam">Spam</string>
 <string id="ham">Not Spam</string>
 <string id="virus">Virus</string>
 <string id="phish">Phish</string>
</group>
```

タイトルに説明を追加する場合は、たとえば、次のようにテキストを変更できます。

```
<group name="Mso.Report.Button.Cations">
 <string id="blockSender">Outlook を使用して送信者をブロック</string>
 <string id="spam">スパムとしてレポート</string>
 <string id="ham">スパムでないとレポート</string>
 <string id="virus">ウイルスとしてレポート</string>
 <string id="phish">フィッシング攻撃としてレポート</string>
</group>
```

BCE_Config.xml ファイルを使用した一括インストール

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

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

ステップ 2　*config_1.xml file* があれば、これを削除します。

ステップ 3　*BCE_Config_signed.xml* ファイルをこのディレクトリにコピーして、ファイル名を *config_1.xml* に変更します。

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

ステップ 5　*CommonEncryptionConfig.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。

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

（注）　特定のドメイン内の選択されたユーザ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して、*CommonEncryptionConfig.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、次のように変更します。

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

が、次のように変わります。

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

`accountFileName` タグを複数指定する場合は、`filePath` を config_2.xml, config_3.xml などとします。

次に例を示します。

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

ステップ 6　インストールの実行（3-1 ページ）に説明されている方法で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（3-19 ページ）に説明されている方法でカスタマイズされた XML ファイルを展開します。

（注）　**\\%allusersprofile%\Cisco\Cisco IronPort Email Security 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。{CONFIG_FOLDER} に Common フォルダが存在している必要があります。UseCustomConfig コマンド パラメータにより、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るようになります。

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後、展開時に特別なキーを追加し、変更後のカスタム コンフィギュレーション ファイルがインストーラによって使用されるようにする必要があります。**UseCustomConfig** コマンド ライン パラメータを使用すると、インストールでカスタム コンフィギュレーション ファイルを使用し、インストール時に使用する必要のあるコンフィギュレーション ファイルを格納しているフォルダへのパスを指定できます。

一括インストールのステップ 11 で、次の構文を使用してコマンド ラインから **UseCustomConfig** キーを追加（インストールの実行（3-1 ページ）を参照）します。

```
Cisco IronPort Email Security Plugin.exe /exenoui /qn
UseCustomConfigs="\\{SHARED_DIR}\{CONFIG_FOLDER}
```

= の後に、カスタマイズされたコンフィギュレーション ファイルへのパスを指定します。

その他のコマンド

UseCustomConfig 以外に、次のコマンドを使用できます。

- AppDir="C:\CustomInstallDir"：カスタム ターゲット ディレクトリを指定します。
- SkipReporting="TRUE"：次のインストールのレポート プラグインを無効にします。
- SkipEncryption="TRUE"：次のインストールの暗号化プラグインを無効にします。

CHAPTER 4

Cisco IronPort Email Security Plug-in for Outlook の設定と使用

この章では、Cisco IronPort Email Security Plug-in for Outlook で使用可能な機能について説明します。Cisco IronPort Email Security Plug-in には、Outlook 電子メール プログラムと連動する数種類のセキュリティ プラグインが用意されています。この章の内容は、次のとおりです。

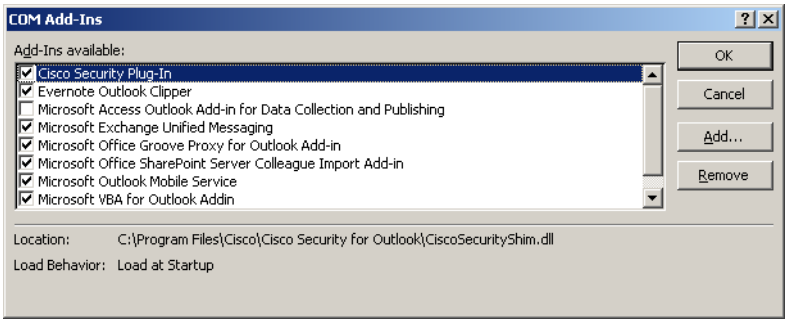
Cisco IronPort Email Security Plug-in For Outlook の全般的な設定

Cisco IronPort Email Security Plug-in は、暗号化プラグインやレポート プラグインなど、複数の Cisco プラグインをサポートするプラットフォームです。Cisco IronPort Email Security Plug-in の一般的な設定は [Options] ページから行うことができます。

Enable または Disable

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

- Outlook 2010 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 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] の順に移動します。



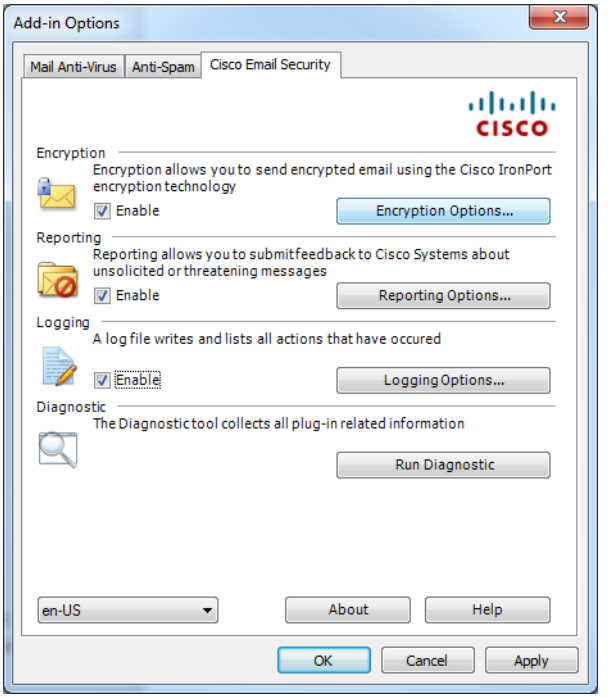
[COM Add-Ins] ウィンドウで、Cisco IronPort Email Security Plug-in のチェックボックスをオフにして [OK] をクリックします。

Outlook プラグインの基本設定

エンド ユーザは [Cisco Email Security] タブで基本的な設定項目を設定できます。

- Outlook 2010 では、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] の順に移動します。
- Outlook 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] の順に移動します。

[Cisco Email Security] タブ



エンド ユーザは、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、レポート、ロギングを有効にできます。さらに設定を行うには、[Encryption Options...]、[Reporting Options...]、または [Logging 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 IronPort Email Security 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。

不要な電子メールによるスパム、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、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 IronPort Email Security Reporting Plug-in for Outlook は、Outlook の [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。

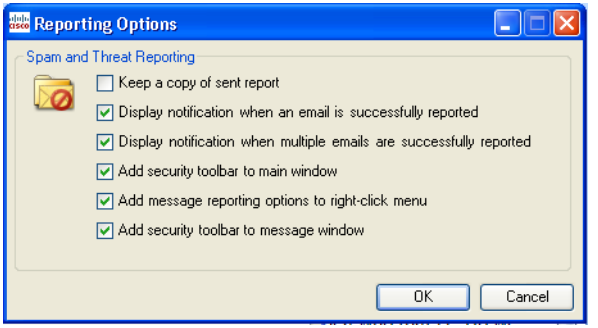
- Outlook 2010 では、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] の順に移動します。[Cisco Email Security] タブで、[Reporting] フィールドの [Enable] チェックボックスをオンにします。
- Outlook 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] タブの順に移動します。[Cisco Email Security] タブで、[Reporting] フィールドの [Enable] 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 Email Security] 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 では、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] の順に移動し、[Reporting Options] ボタンをクリックします。
- Outlook 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] タブの順に移動し、[Reporting Options] ボタンをクリックします。

[Reporting Options] ページ:



オプション

ここでは、エンド ユーザが設定できるレポート オプションについて説明します。

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 an 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。

オプション	説明
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 security toolbar to main window	デフォルトでは、エンド ユーザが Cisco IronPort Email Security 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。
Add message reporting options to right-click menu	デフォルトでは、Cisco IronPort Email Security 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 security toolbar to message window	デフォルトでは、エンド ユーザが Cisco IronPort Email Security 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。

Reporting Plug-in for Outlook の使用方法

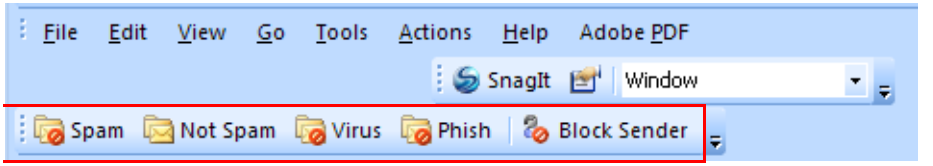
概要

Cisco IronPort Email Security Plug-in for Outlook では、エンド ユーザは、受信トレイで受信したスパム、ウイルス、フィッシ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。

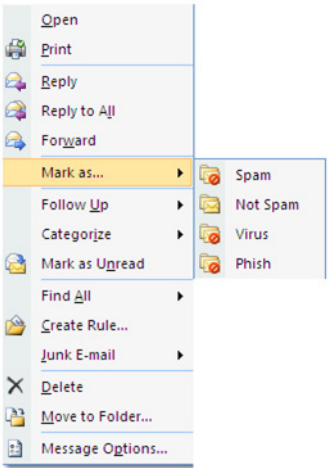
シスコへのフィードバック

このプラグインをインストールすると、Outlook に新たにツールバーが追加されます。このツールバーには、[Spam]、[Not Spam]、[Virus]、[Phish]、[Block Sender] ボタンが含まれています（[Block Sender] はエンド ユーザの迷惑メール ボックスに届く電子メールをブロックしません）。

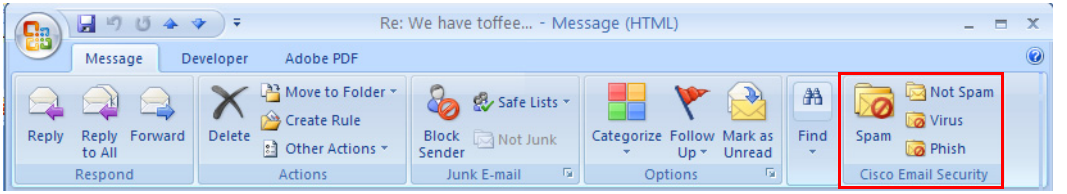


これらのボタンを使用して、スパム、ウイルス、フィッシングのメールを報告します(フィッシング攻撃とは、「不正な」偽装 Web サイトにリンクしている電子メールを送りつける攻撃です。これらの Web サイトは、クレジット カード番号、口座の名義人名とパスワード、社会保障番号など、個人の金融情報を受信者に漏洩させることを目的としています。たとえば、個人の銀行口座情報を不正に要求する電子メールが *infos@paypals.com* から送信されてくることがあります)。さらに、エンド ユーザは [Block Sender] ボタンをクリックすることもできます。このボタンをクリックすると、Outlook の迷惑メール対策アクションである「送信者を受信拒否リストに追加」する機能が作動します。この機能の詳細については、Microsoft のドキュメントを参照してください。

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、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、またはフィッシ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、フィッシングとして電子メール 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。

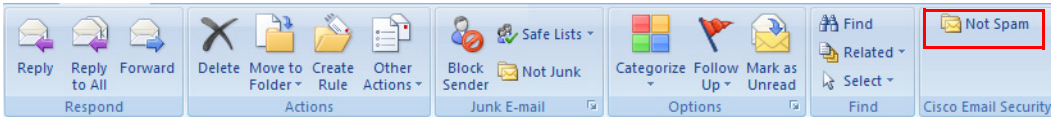
受信トレイのメッセージ:

- スパム、ウイルス、またはフィッシ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。
- 「非スパム」と報告された受信トレイのメッセージは、[受信トレイ] フォルダに残されます。

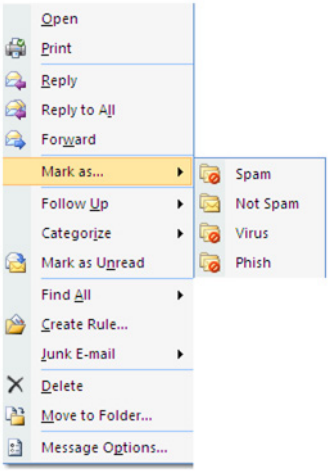
迷惑メッセージ:

- スパム、ウイルス、またはフィッシ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。
- 「非スパム」と報告された迷惑メッセージは、[受信トレイ] フォルダに移動されます。

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、今後この送信者からのメールはスパムとして分類されないようになります。



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。

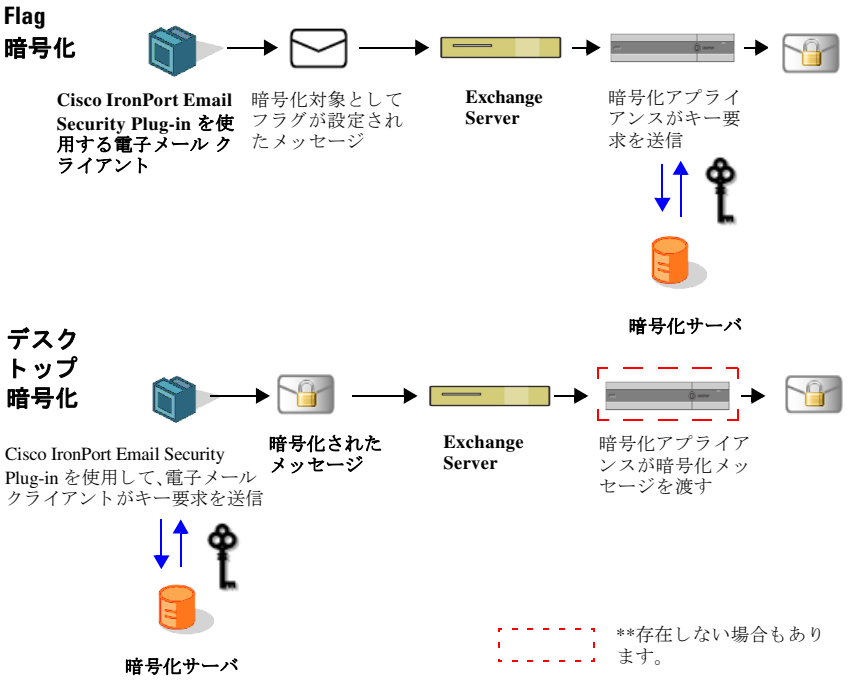


電子メールの暗号化

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、暗号化が必要な電子メールにフラグを設定できます。この電子メールは、Cisco IronPort 暗号化アプライアンスによって暗号化されてから、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 IronPort 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 4-1　　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 アカウントからの *BCE_Config_signed.xml* 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 ユーザは、管理者から更新済みの *BCE_Config_signed.xml* 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 *BCE_Config_signed.xml* 添付ファイルが含まれている場合は、エンド ユーザがそのコンフィギュレーション 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 IronPort 暗号化アプライアンスまたは Cisco Registered Envelope Service（CRES）は、キー サーバとして使用されます。エンド ユーザ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。フラグ オプションを使用すると、エンド ユーザは暗号化が必要な電子メールにフラグを設定できます。この電子メールは、Cisco 電子メール セキュリティ アプライアンスによって暗号化されてから、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で復号化できるようサーバ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。

Email Security Plug-in のコンフィギュレーション ファイルの起動

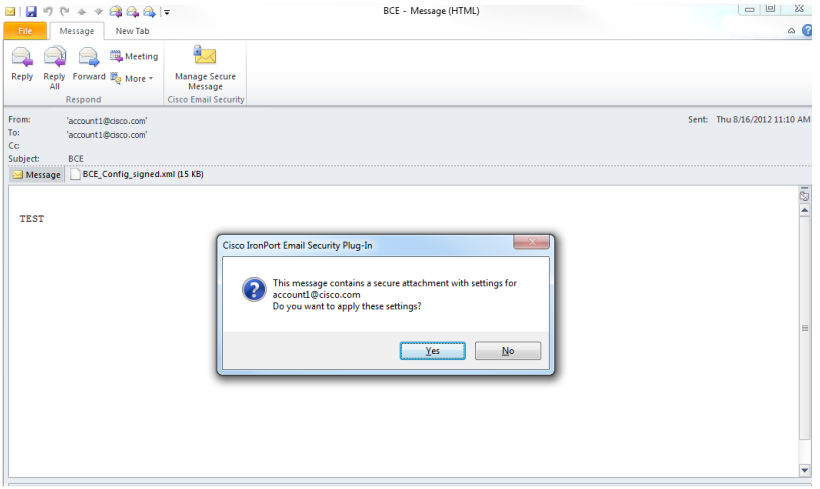
エンド ユーザは、Outlook 電子メール アカウントからの *BCE_Config_signed.xml* 添付ファイルを復号化することによって、Outlook 電子メール アカウントの暗号化を有効化したり設定することができます。エンド ユーザの受信トレイに添付ファイル付きの通知メールがない場合は、スパム メールまたは迷惑メールのフォルダを調べてください。

コンフィギュレーション ファイルを起動すると、*BCE_Config_signed.xml* 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。

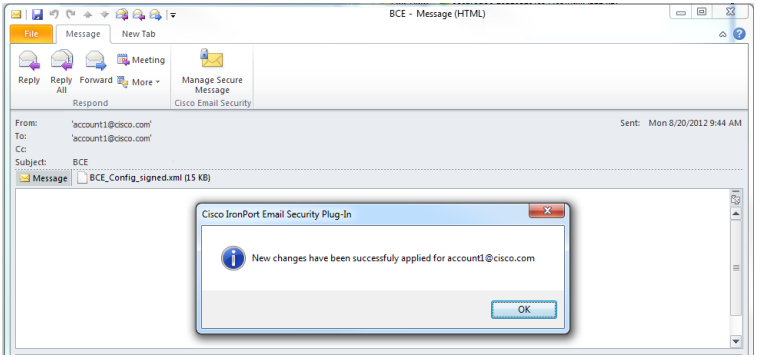
注　通常は、プラグインのインストール時に Jave Runtime Environment（JRE）が自動的にインストールされます。インストールされなかった場合は、最新のバージョン 1.6 をインストールしてプラグインで使用してください。

Outlook 電子メール アカウントに対してセキュリティ プラグインを有効化して設定するには、次の手順を実行します。

ステップ 1　*BCE_Config_signed.xml* 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 IronPort Email Security 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。



Flag 暗号化

Flag 暗号化オプションを使用すると、エンド ユーザは暗号化が必要な電子メールにフラグを設定できます。この電子メールは、Cisco IronPort 暗号化アプライアンスまたは電子メール セキュリティ アプライアンスによって暗号化されてから、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。

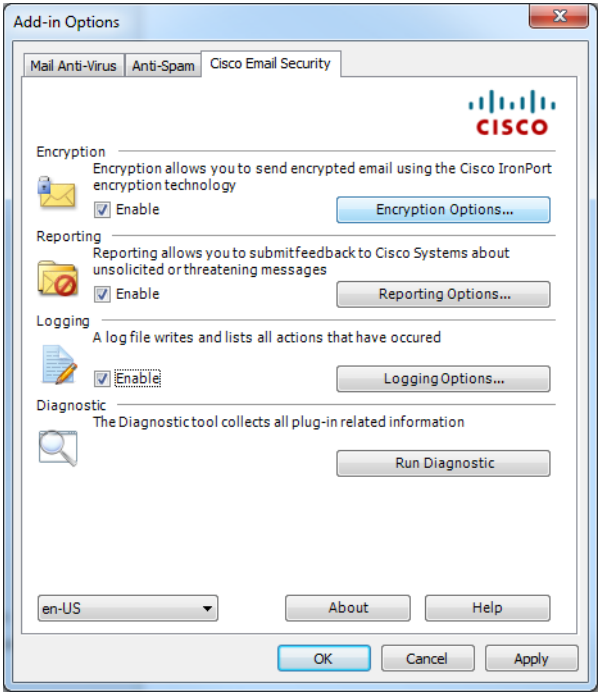
Flag 暗号化の設定は [Cisco Email Security] ページにあります。Flag 暗号化の設定を変更するには、次の手順を実行します。

- Outlook 2010 では、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] > [Encryption Options] の順に移動します。
- Outlook 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] > [Encryption Options] の順に移動します。

暗号化プラグインを有効化または無効化するには、[Cisco Email Security] 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 Email Security の [Add-in Options] ページ:

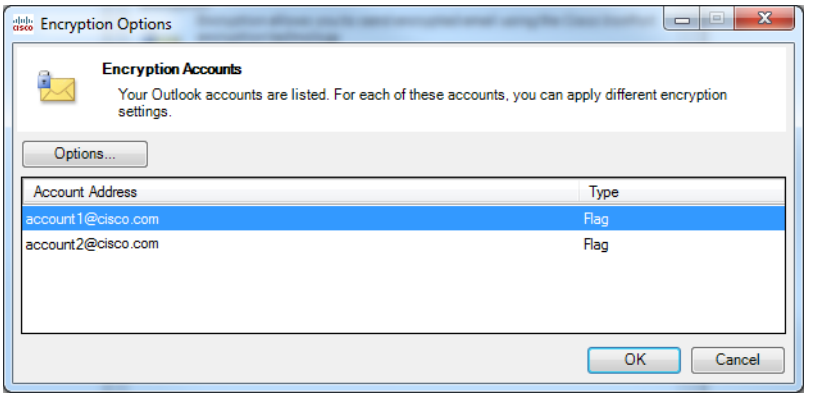


Flag 暗号化のオプション

暗号化アカウント

[Encryption Accounts] ページには、Flag 暗号化プラグインの対象となるすべての電子メール ユーザ アカウントが表示されます。各行は 1 つのアカウントに対応しており、アカウントの電子メール アドレスと暗号化タイプが表示されます。[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

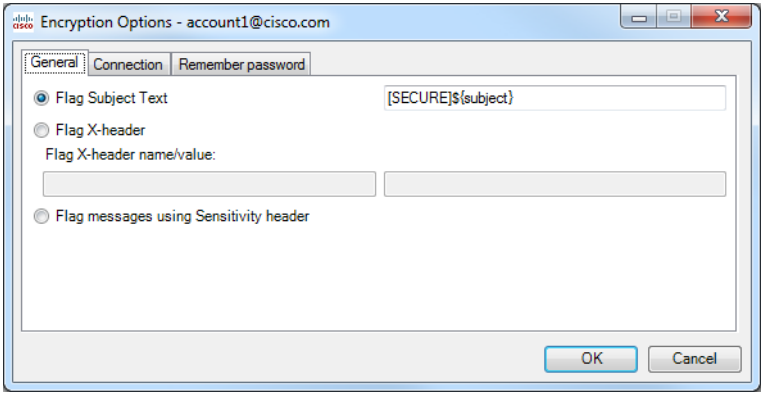
エンド ユーザが送信メールの暗号化を必要としている場合、管理者はその電子メールに暗号化のマーク（「フラグ」）を設定する必要があります。これにより、管理者が作成したフィルタを使って暗号化が必要なメッセージを識別できます。

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

次の図は、[Flag Encryption Options] の [General] タブを示しています。



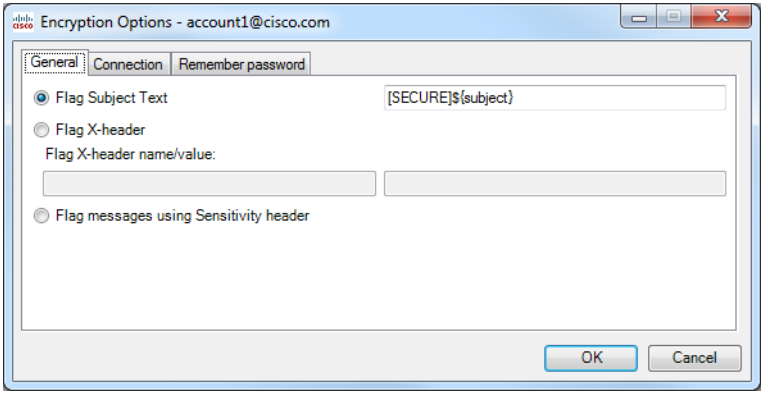
次の [General] のオプションから選択できます。

[General] のオプション	値
Flag Subject Text	送信メールの [Subject] フィールドにテキストを追加して、電子メールに暗号化のフラグを付けることができます。[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]*）。

[General] のオプション	値
Flag X-header name/value	送信メールに x ヘッダーを追加して、電子メールに暗号化のフラグを付けることができます。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」を入力すると、指定した x ヘッダーが付いたメッセージが暗号化されます（デフォルト値は「true」）。
Flag messages using Sensitivity header	Outlook では、秘密度に関するヘッダーを追加して電子メールの暗号化を示すフラグをメッセージに付けることができます。この方法を選択すると、Outlook の秘密度に関するヘッダーを使用して電子メールに暗号化のマークを付けることができます。

[Connection] タブ

次の図は、[Flag Encryption Options] の [Connection] タブを示しています。

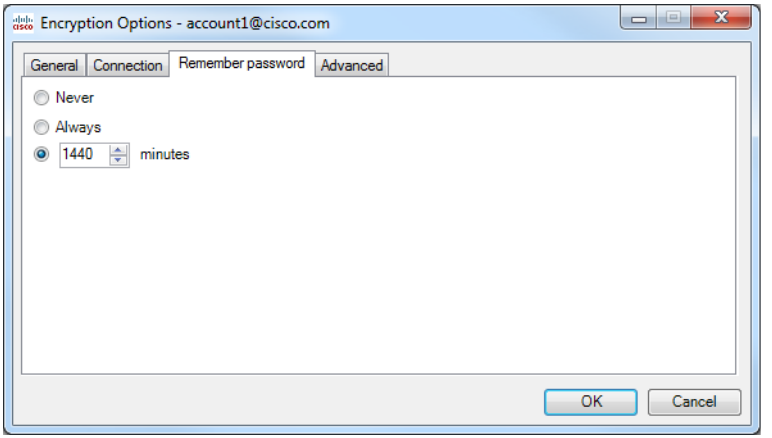


次の [Connection] のオプションから選択できます。

[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	特定のプロキシの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は、[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 サーバのポートを指定します。
Username	サーバでユーザ名が必要な場合に、ユーザ名を入力します。
Password	システムまたはプロキシ サーバに対して入力したユーザ名に関連するパスワードを入力します。

[Remember Password] タブ

次の図は、[Flag Encryption Options] の [Remember password] タブを示しています。



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。

デスクトップ暗号化

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。

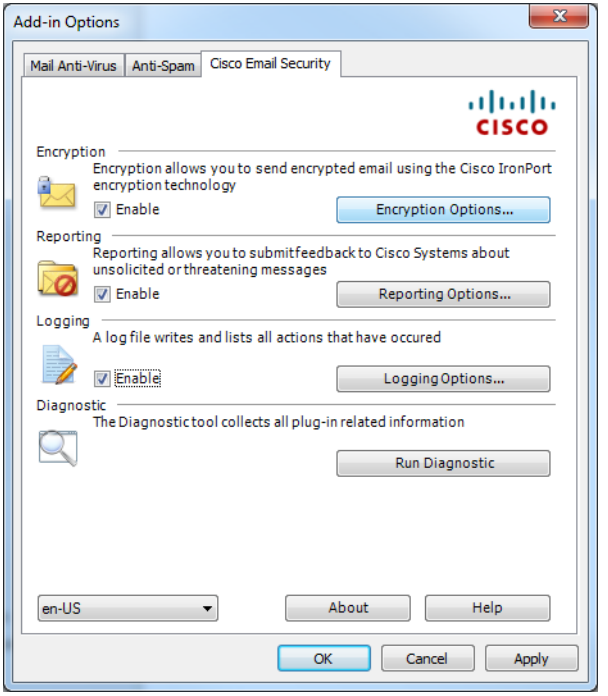
デスクトップ暗号化の設定は [Cisco Email Security] ページにあります。デスクトップ暗号化の設定を変更するには、次の手順を実行します。

- Outlook 2010 では、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] > [Encryption Options] の順に移動します。
- Outlook 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] > [Encryption Options] の順に移動します。

エンド ユーザは、[Cisco Email Security] 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することで、暗号化プラグインを有効化または無効化できます。[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 ユーザは [Cisco Email Security] 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。

Cisco Email Security の [Add-in Options] ページ:

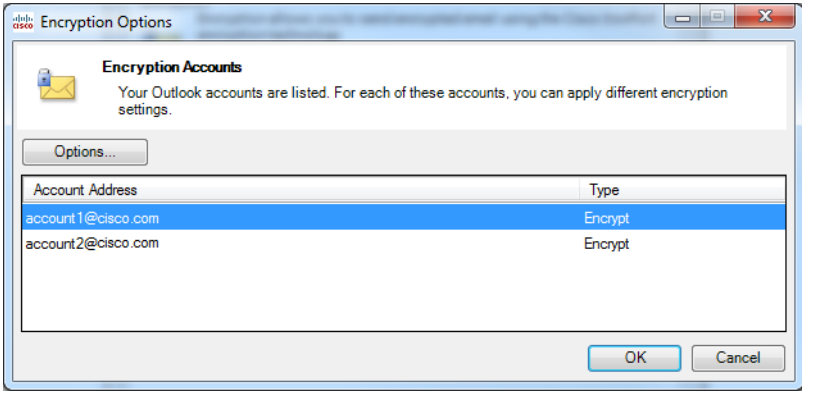


デスクトップ暗号化のオプション

暗号化アカウント

[Encryption Accounts] ページには、デスクトップ暗号化プラグインの対象となるすべての電子メール ユーザ アカウントが表示されます。各行は 1 つのアカウントに対応しており、アカウントの電子メール アドレスと暗号化タイプが表示されます。[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：

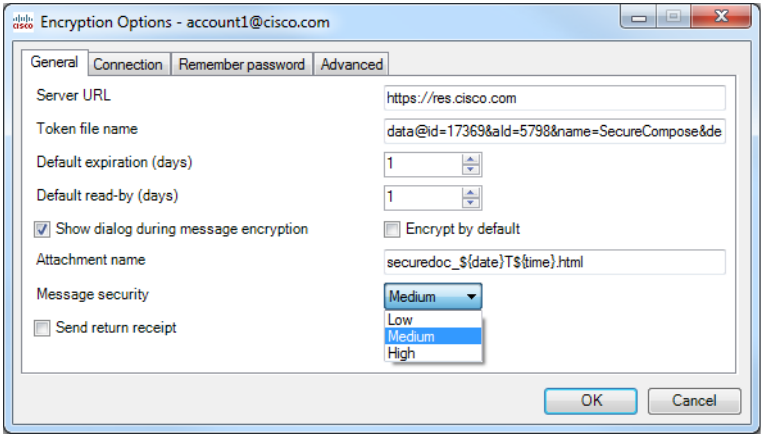


注　Outlook の新規アカウントは [Encryption Accounts] リストに自動的に追加されます。Outlook アカウントが削除されると、そのアカウントは [Encryption Accounts] リストから自動的に削除されます。

[General] タブ

次の図は、[Desktop Encryption Options] の [General] タブを示しています。

注　スクリーンショットと表には [General] タブの使用可能なオプションがすべて示されていますが、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。



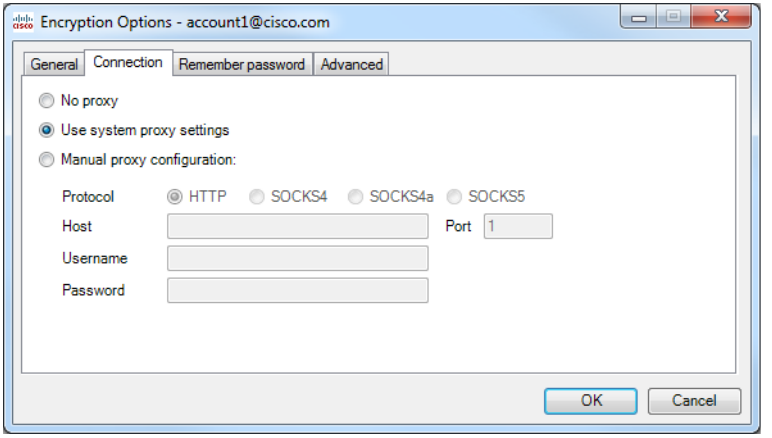
次の [General] のオプションから選択します。

[General] のオプション	値
Server URL	暗号化サーバの URL を入力します。
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。
Default read-by (days)	受信者が暗号化されたメッセージを読むと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。
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。

[General] のオプション	値
Encrypt by default	このオプションを選択すると、送信するすべての電子メール メッセージがデフォルトで暗号化されます。
Attachment name	デフォルトのエンベロープ名は *securedoc.html* です。添付ファイル名の値は変更でき、指定した新しい名前がエンベロープに反映されます。
Message Security	ドロップダウン リストから、暗号化する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* ファイルで設定された値です。 **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]: 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。
Send return receipt	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。

[Connection] タブ

次の図は、[Flag Encryption Options] の [Connection] タブを示しています。



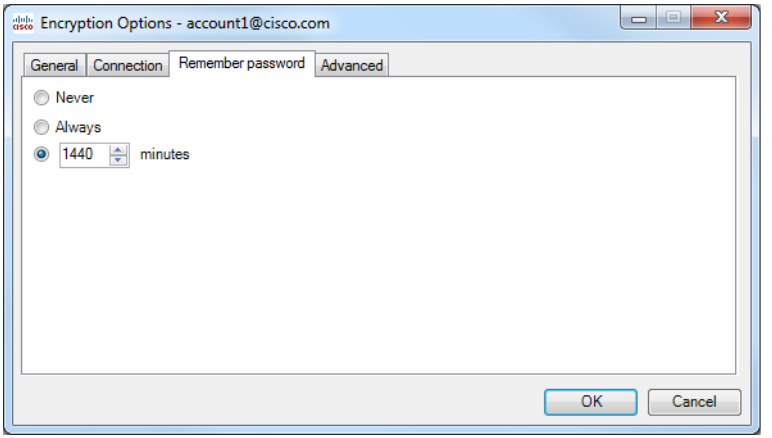
次の [Connection] のオプションから選択します。

[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	特定のプロキシの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は、[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 サーバのポートを指定します。

[Connection] のオプション	値
User Name	サーバでユーザ名が必要な場合に、ユーザ名を入力します。
Password	システムまたはプロキシ サーバに対して入力したユーザ名に関連するパスワードを入力します。

[Remember Password] タブ

次の図は、[Flag Encryption Options] の [Remember password] タブを示しています。



次の [Remember Password] のオプションから選択します。

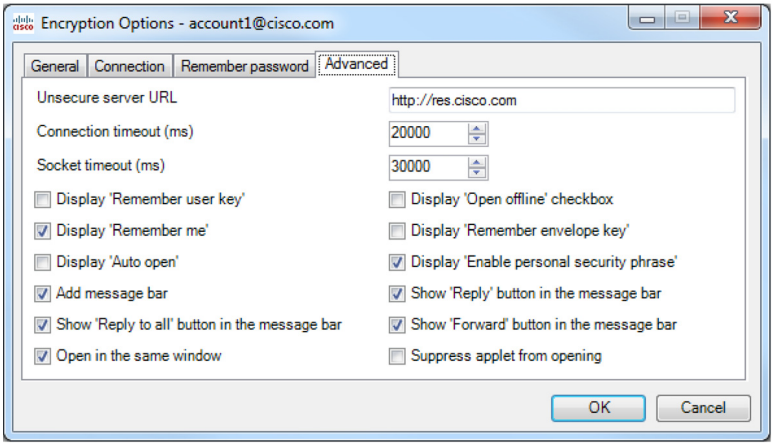
パスワードのオプション	値
Never	このオプションを選択すると、電子メールを復号化または暗号化するときに、常に暗号化パスワードが必要になります。

パスワードのオプション	値
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。ドロップダウンから、キャッシュしておく期間（分数）を選択します。指定した時間が経過すると、エンド ユーザは、電子メールを復号化したり暗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

次の図は、[Flag Encryption Options] の [Advanced] タブを示しています。

注　スクリーンショットと表には [General] タブの使用可能なオプションがすべて示されていますが、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。



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非セキュア ベース 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に待機する時間の長さ。
Socket timeout	キー サーバ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、エンベロープに [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、エンベロープに [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、エンベロープに [Enable personal security phrase] チェックボックスが表示されます。
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。
Suppress applet for open	アプレットでエンベロープが開かれないようにする場合に選択します。
Display "Remember me"	このオプションを選択すると、エンベロープに [Remember me] チェックボックスが表示されます。
Display "Auto open"	このオプションを選択すると、エンベロープに [Auto open] 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。

[Advanced] のオプション	値
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。
Open in the same window	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。

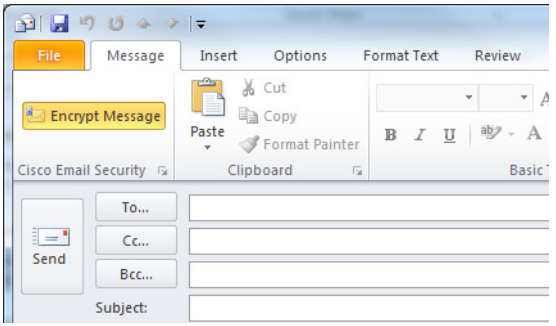
暗号化された電子メールの送信

注　添付前の暗号化電子メールのデフォルトの最大サイズは 7 MB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。

エンド ユーザ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。

次の図は、[Mail Compose] ページの [Encrypt Message] ボタン、および [Encryption Mail Options] トグル ボタンを示しています。



[Encryption Mail Options] ページを表示するには、右下隅にある [Cisco Email Security] ランチャをクリックします。

[Encryption Mail Options] ページ:

注　スクリーンショットと表には [Encryption Mail Options] の使用可能なオプションがすべて示されていますが、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。

[Encryption Mail Options]	説明
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。
Message Security	ドロップダウン リストから、暗号化する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* ファイルで設定された値です。 **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]: 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。

[Encryption Mail Options]	説明
Expiration	ドロップダウン リストで、暗号化した電子メールの有効期限（日時）を指定します。有効期限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。
Read By	ドロップダウン リストで、受信者が暗号化されたメッセージを読むと予想される期限の日時を指定します。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 ユーザが [Send] をクリックすると [Secure Envelope Options] ページが表示されます。エラーおよびトラブルシューティング（4-52 ページ）を参照してください。

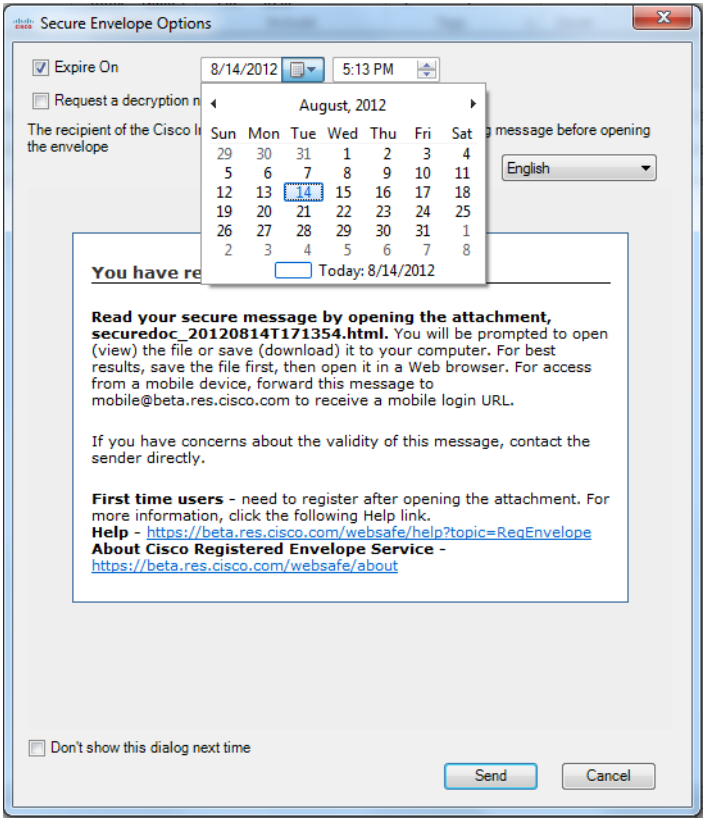
返信オプションの伝播

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。
- *BCE_Config_signed.xml* 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。

[Secure Envelope Options] ページ:



エンド ユーザは次の [Secure Envelope Options] から選択できます。

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

[Manage Secure Messages] ページには、送信済みの暗号化電子メールが表示されます。エンド ユーザはこのオプションを使用して、送信済みの暗号化電子メールに対して次の操作を実行できます。

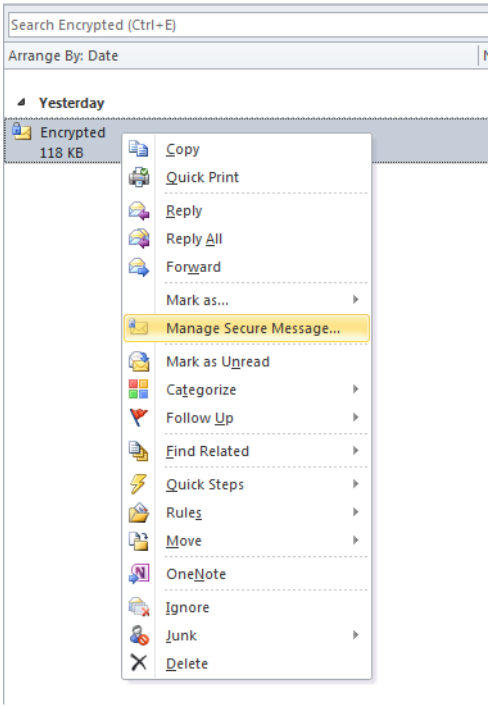
- **電子メールのロック**。エンド ユーザは、以前に送信した暗号化電子メールをロックできます。また、ロックの理由を設定したり、メッセージがすでにロックされている場合はロックの理由を更新できます。受信者はロックされた電子メールを開くことができなくなります。
- **電子メールのロック解除**。エンド ユーザは、以前に送信した暗号化電子メールのロックを解除できます。これによって、受信者はその電子メールを復号化できるようになります。
- **有効期限の更新**。エンド ユーザは、送信した暗号化電子メールに対して有効期限を設定、更新、クリアすることができます。暗号化された電子メールが期限切れになる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

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] メニューを表示します。

また、エンド ユーザは、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。

[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。エンド ユーザのパスワードがキャッシュされていない場合は、パスワードの入力を求めるメッセージが表示されます。

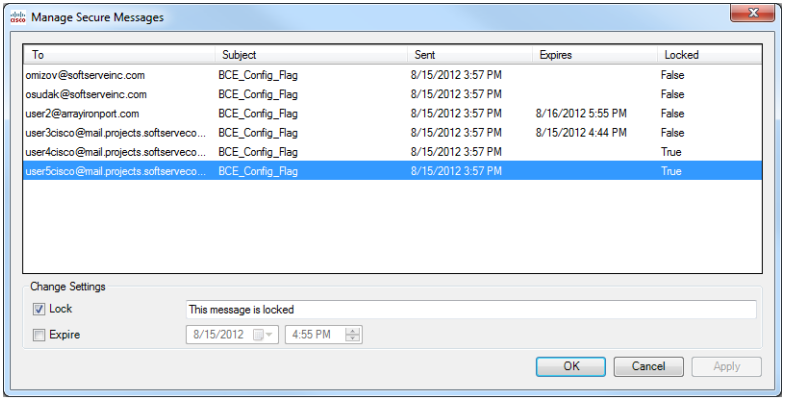
ステップ 3　受信者ごとにロックや有効期限のオプションを設定するには、送信済みの暗号化電子メール メッセージを選択して右クリックし、[Manage Secure Messages] を選択します。

または

送信済みの暗号化電子メール メッセージを複数選択して右クリックし、[Manage Secure Messages] を選択して、選択した暗号化電子メール メッセージをすべてロックします。

注　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] ページ：

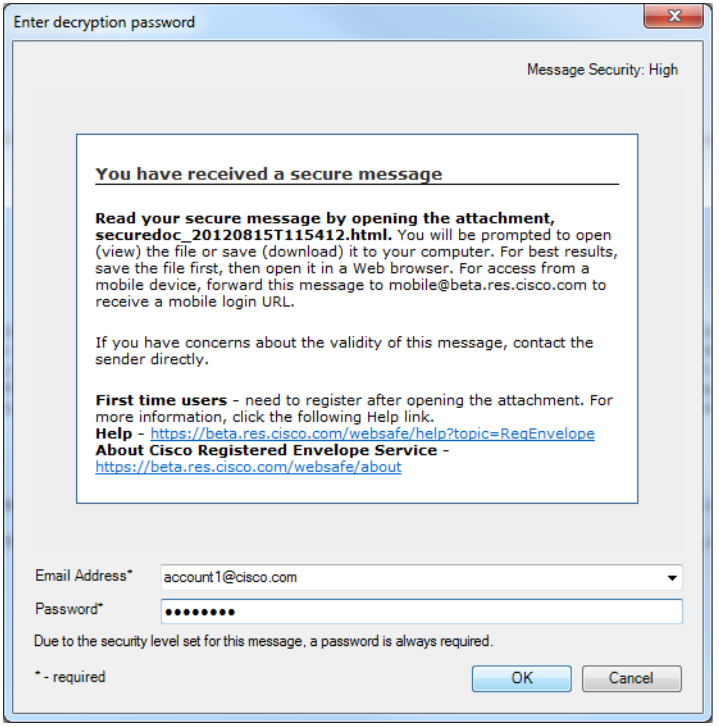


安全な電子メールの受信

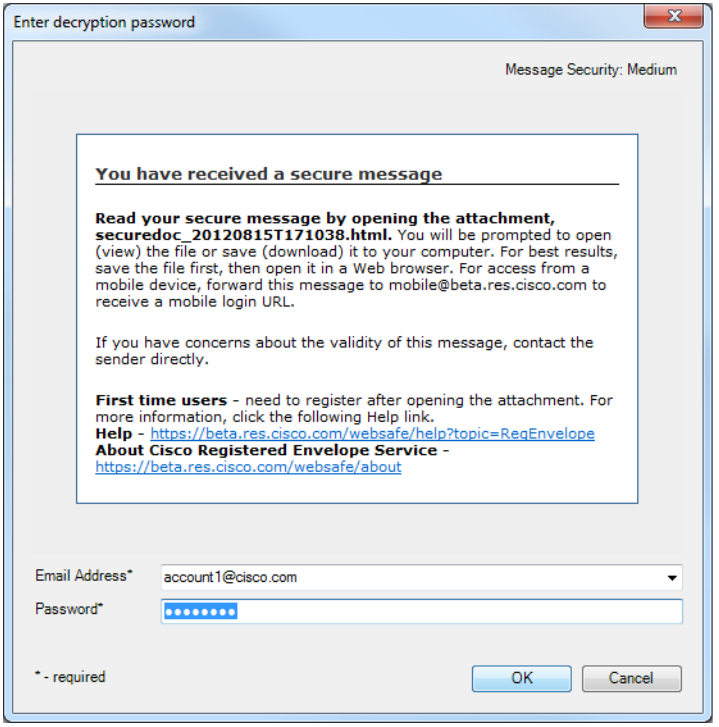
デスクトップ暗号化プラグインは安全な電子メールを自動的に検出し、Outlook 内でそれらの復号化を試みます。エンド ユーザが暗号化されたメッセージを受信した場合は、通常、エンベロープを開封するために暗号化パスワードを入力する必要があります。セキュア メッセージには、[High]、[Medium]、または [Low] のメッセージ セキュリティを設定できます。

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 ユーザは、そのメッセージを開封するために、Cisco Registered Envelope Service（CRES）にユーザ 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、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（4-45 ページ）を参照してください。

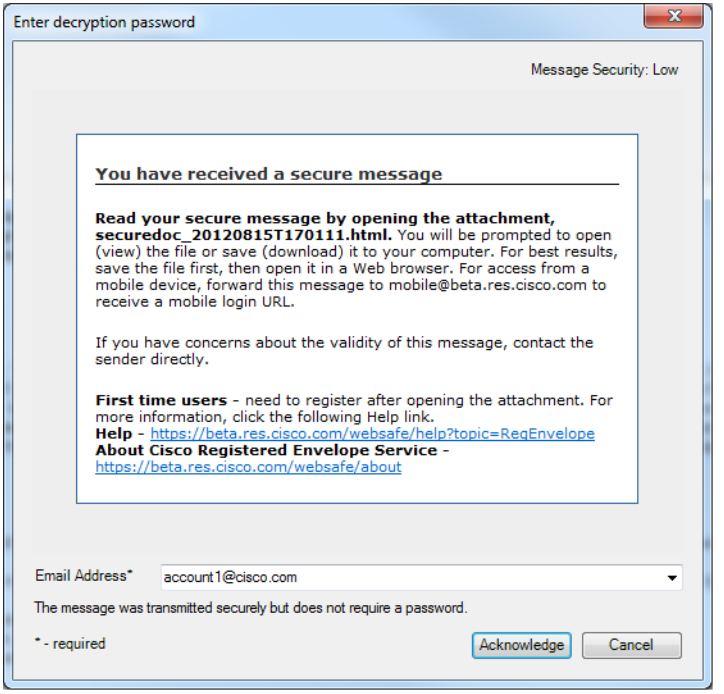
[Message Security High] ページ:



[Message Security Medium] ページ:



[Message Security Low] ページ：

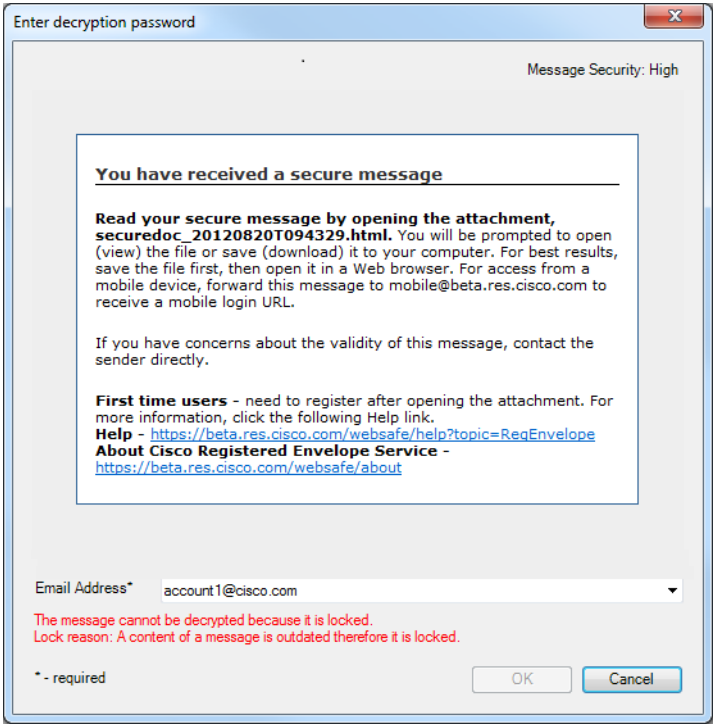


次の表は、メッセージ セキュリティのオプションを示しています。

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。

メッセージ セキュリティのオプション	説明
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。


Enter decryption password
Message Security: High
You have received a secure message
Read your secure message by opening the attachment, securedoc_20120820T094329.html. You will be prompted to open (view) the file or save (download) it to your computer. For best results, save the file first, then open it in a Web browser. For access from a mobile device, forward this message to mobile@beta.res.cisco.com to receive a mobile login URL.
If you have concerns about the validity of this message, contact the sender directly.
First time users - need to register after opening the attachment. For more information, click the following Help link.
Help - https://beta.res.cisco.com/websafe/help?topic=RegEnvelope
About Cisco Registered Envelope Service - https://beta.res.cisco.com/websafe/about
Email Address*
account1@cisco.com
The message cannot be decrypted because it is locked.
Lock reason: A content of a message is outdated therefore it is locked.
* - required
OK
Cancel

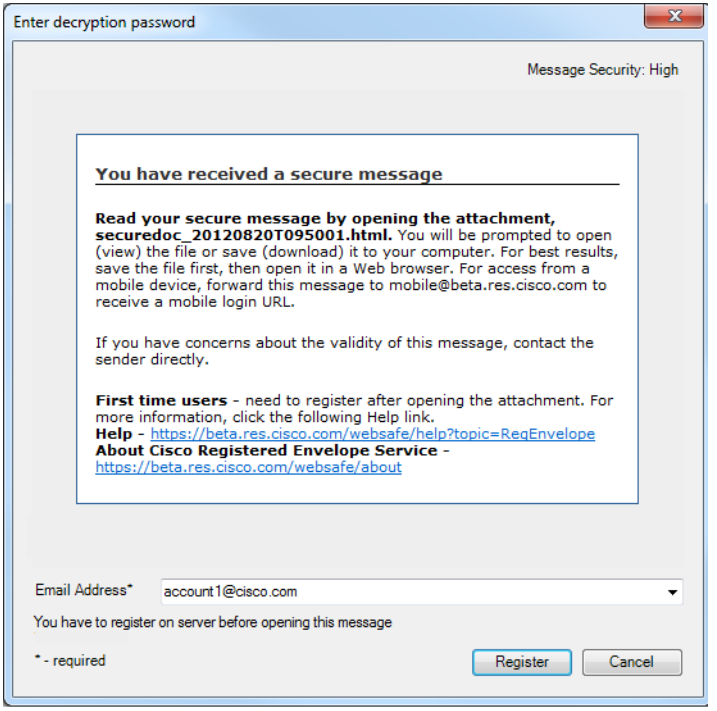
暗号化されたセキュア メッセージを初めて開封する場合

暗号化されたセキュリティ メッセージを受信した場合、エンド ユーザは、そのメッセージを開封するために、Cisco Registered Envelope Service（CRES）にユーザ 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、受信するすべての暗号化されたセキュア メッセージを開封できます。

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は、次の手順を実行します。

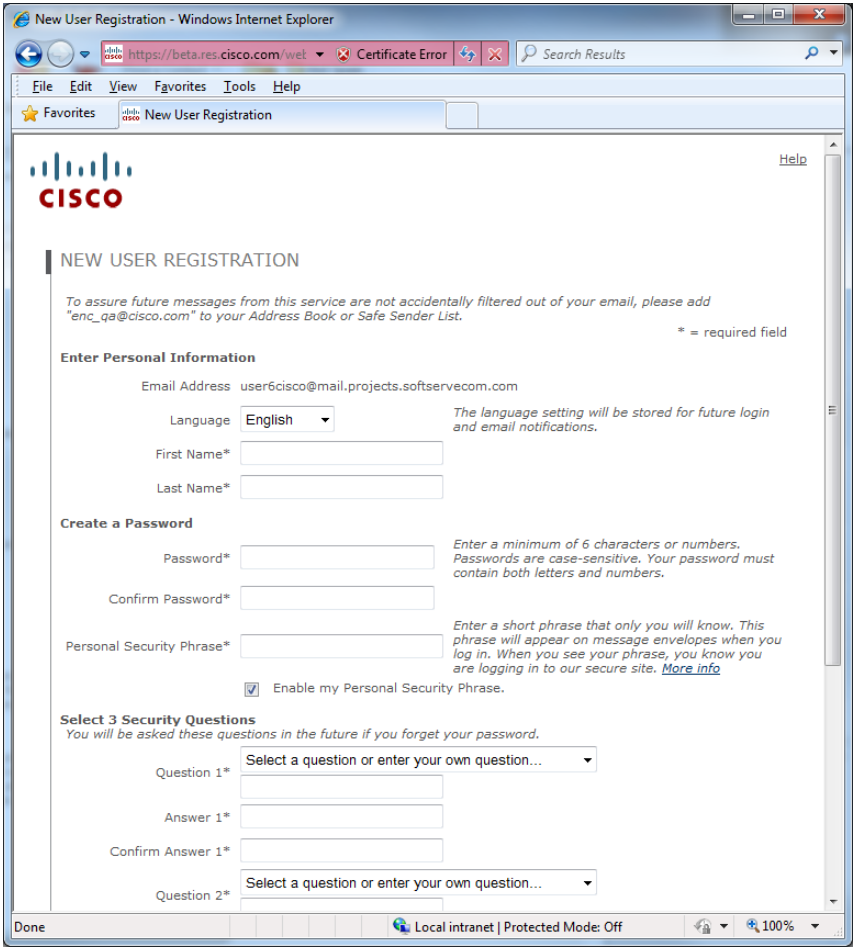
ステップ 1　メールボックス内の安全な電子メール メッセージをダブルクリックします。登録ボタンが付いた復号化ダイアログが表示されます。

ステップ 2　[Register] をクリックして、Cisco Registered Envelope Service（CRES）に登録します。



ステップ 3　CRES の [New User Registration] ページに情報を入力して、オンライン登録フォームを完了させます。

CRES の [New User Registration] ページ:



[New User Registration] 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、CRES アカウントで使用する言語を選択します。デフォルトでは、登録ページは英語で表示されますが、エンド ユーザは日本語、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。CRES ユーザアカウントの名を入力します。
Last Name	必須です。CRES ユーザアカウントの姓を入力します。
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 6 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。 **注**　パスワードを忘れた場合、エンド ユーザはセキュリティに関する質問に正しく答えることによって、パスワードをリセットできます。

フィールド	説明
Personal Security Phrase	必須です。個人セキュリティ フレーズを入力します。個人セキュリティ フレーズは、パスワード フィッシングの脅威からエンド ユーザを保護する上で役立ちます。登録時に、エンド ユーザは自分とサービスだけが知っている短い個人セキュリティ フレーズを指定できます。この個人セキュリティ フレーズは、エンド ユーザが受信した登録済みエンベロープのパスワード フィールドをクリックすると表示されます。表示されない場合は、詳細情報のリンクをクリックして確認します。 **注**　エンド ユーザが [Remember me on this computer] をオンにしていない場合、個人セキュリティ フレーズは表示されません。
Enable Personal Security Phrase	オプション。個人セキュリティ フレーズを有効にするには、このチェックボックスをオンにします。
Security Questions	必須です。エンド ユーザは 3 つのセキュリティに関する質問を選択し、質問への回答を入力して確認する必要があります。これらの質問は、エンド ユーザがパスワードを忘れた場合にパスワードをリセットするために使用されます。

ステップ 4　フォームの下部にある [Register] をクリックし、ユーザ アカウントを作成します。

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、エンド ユーザは複数のユーザ アカウントを設定する必要があります。各アドレスごとに個別のユーザ アカウントが必要です。

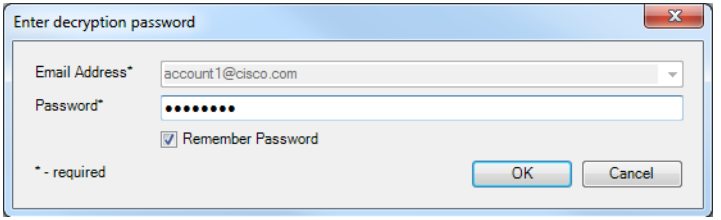
ステップ 5　電子メール アカウントの受信トレイをチェックして、アカウントのアクティベーション メッセージが届いていることを確認します。アクティベーション用電子メール メッセージ内の [Click here to activate this account] リンクをクリックします。メッセージが表示され、アカウントのアクティベーションが確認されたこと、および登録済み電子メール アドレスに送信された暗号化電子メールをエンド ユーザが表示できるようになったことが示されます。

ステップ 6　元の電子メールに戻り、*securedoc_date_time.html* 添付ファイルをクリックします。

ステップ 7　[Open] をクリックします。安全な電子メールが復号化され、そのメッセージが表示されます。

注　エンド ユーザのコンフィギュレーション ファイルの設定によっては、一部の機能が使用できないことがあります。たとえば、メッセージの返信、全員に返信、または転送ができない場合があります。

パスワードは Outlook セッション中に保存されます。ただし、Outlook を再起動したときに、エンド ユーザはパスワードを再入力する必要があります。



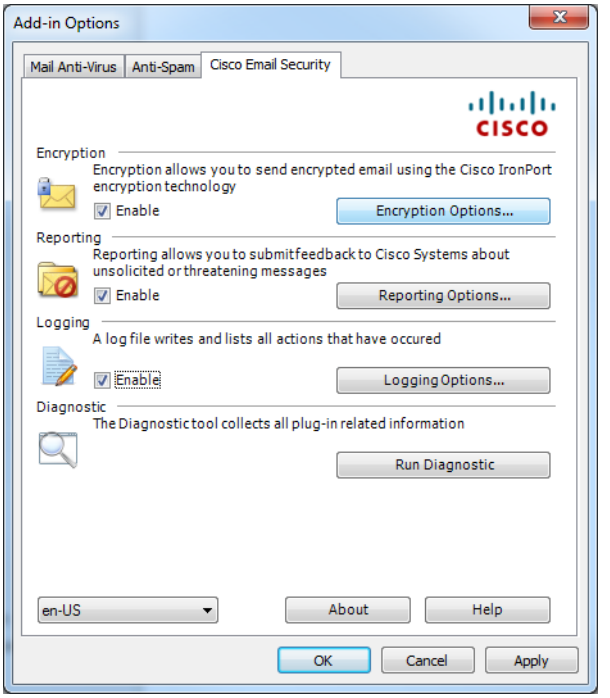
ログ設定の変更

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。

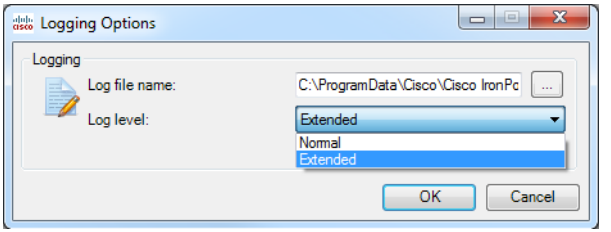
ロギング オプションは [Cisco Email Security] ページにあります。ロギング オプションを変更するには、次の手順を実行します。

- Outlook 2010 では、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] > [Logging Options] の順に移動します。
- Outlook 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] > [Logging Options] の順に移動します。

Cisco Email Security の [Add-in Options] ページ:



暗号化の [Logging Options] ページ:



ロギング オプション

エンド ユーザは [Logging] メニューで次のオプションを設定できます。

オプション	説明
Log file name	エンド ユーザは ログ ファイル（%ALLUSERSPROFILE%\Cisco\Cisco IronPort Email Security Plug-in\<username> に保存）の名前を指定できます。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	• [Normal]。デフォルトで、このオプションは有効になっています。Normal ロギングには、致命的エラー、回復可能エラー、警告、役立つ情報が記載されます。 • [Extended]。Extended ロギングでは、Normal ログ メッセージに加えて、デバッグ ログ メッセージを使用できます。

エンド ユーザは、特定の状況に応じた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 IronPort Email Security Plug-in に関する問題が発生した場合、エンド ユーザがログ レベルを [Extended] に設定すると管理者に最大限の情報を提供できるので、開発者は問題を再現して診断を実行することができます。

エラーおよびトラブルシューティング

ここでは、Cisco IronPort Email Security Plug-in for Outlook の使用時に発生する可能性があるいくつかの一般的なエラー、およびそれらのエラーの修正に役立つトラブルシューティングのヒントを示します。

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 IronPort Email Security 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 Email Security Plug-in for Outlook ファイルの修復（4-57 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 IronPort Email Security 診断ツールの実行（4-59 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 IronPort Email Security 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 IronPort Email Security 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 Email Security Plug-in for Outlook ファイルの修復（4-57 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 IronPort Email Security 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 Email Security Plug-in for Outlook ファイルの修復（4-57 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]、または [Not Spam] ボタンをクリックしたときに、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 Email Security Plug-in for Outlook ファイルの修復（4-57 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 [Spam]、[Virus]、[Phish]、または [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。

サーバへの接続中にエラーが発生

Outlook がオンライン状態のときに、インターネット接続が失われた場合またはサーバが一時的に使用できない場合は、次のエラーが発生します。

- *An HTTP error occurred during connection to server.*

ソリューション

ネットワークの設定を確認するか、ローカル管理者に連絡してください。

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 Envelope 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。

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.*

ソリューション

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. Forgot password?*

ソリューション

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.*

ソリューション

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.*

ソリューション

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 IronPort Email Security 診断ツールの実行（4-59 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.*

ソリューション

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 IronPort Email Security 診断ツールの実行（4-59 ページ）を参照してください。

上限を超過

添付前の暗号化電子メールのデフォルトの最大サイズは 7 MB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。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　最後の 2 つのメッセージ（*Failed to report ...*）は、現時点では英語でのみ表示されます。

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

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

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　プログラムの一覧から「Cisco IronPort Email Security Plug In」を選択し、[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は、手順に従って診断ツールを使用し、Cisco IronPort にフィードバックしてください。Cisco IronPort Email Security 診断ツールの実行（4-59 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 IronPort Email Security 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 IronPort Email Security 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 Email Security Plug-in for Outlook ファイルの修復（4-57 ページ）または Cisco IronPort Email Security 診断ツールの実行（4-59 ページ）を参照してください。

注　エラーが発生した場合は、エラーおよびトラブルシューティング（4-52 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 IronPort Email Security 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 IronPort Email Security Plug-in の出力ファイル
- 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 IronPort Email Security 診断ツールの実行

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

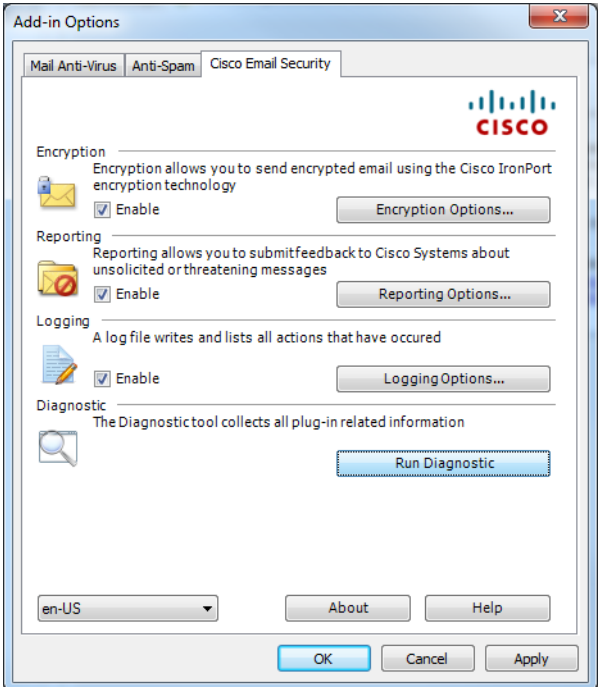
- **Cisco Email Security の [Options] タブから**。通常は、Cisco Email Security の [Options] タブから診断ツールを実行します。
- **「Program Files\ Cisco IronPort Email Security Plug-in」フォルダから**（通常は、C:\Program Files\Cisco\Cisco IronPort Email Security Plug-in）。これは Cisco IronPort Email Security Plug-in がインストールされているフォルダです。
- [Start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

Outlook の [Options] ページからの診断ツールの実行

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 では、[File] > [Options] > [Add-ins] > [Add-in Options] > [Cisco Email Security] > [Run Diagnostic] の順に移動します。
- Outlook 2003/2007 では、[Tools] > [Options] > [Cisco Email Security] > [Run Diagnostic] の順に移動します。

Cisco Email Security の [Add-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、エンドユーザからシステム管理者に送信したり、管理者からシスコのサポート担当者に送信することができます。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 IronPort Email Security Plug-in] > [Cisco IronPort Email Security Plug-in Diagnostic] から診断ツールを実行します。

または

- Cisco IronPort Email Security Plug-in をインストールしたフォルダ（通常、C:\Program Files\Cisco\Cisco IronPort Email Security Plug-in）に移動し、*Cisco.EmailSecurity.Framework.Diagnostic.exe* ファイルをダブルクリックします。

Cisco IronPort Email Security Plug-in のアンインストール

Cisco IronPort Email Security 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、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 IronPort Email Security Plug-in for Outlook のアンインストール手順:

Cisco IronPort Email Security 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。

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 IronPort Email Security Plug In] を選択し、[Uninstall/Change] > [Next] > [Remove] の順にクリックします。

もう 1 つのアンインストール方法:

- プラグイン設定ファイル(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 IronPort Email Security Plug-in をアンインストールします。

APPENDIX A

IronPort エンドユーザ ライセンス契約書

この付録は、次の項で構成されています。

Cisco IronPort Systems, LLC Software License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT") FOR THE LICENSE OF THE SOFTWARE (AS DEFINED BELOW). BY CLICKING THE ACCEPT BUTTON OR ENTERING "Y" WHEN PROMPTED, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY, COLLECTIVELY, THE "COMPANY") CONSENT TO BE BOUND BY AND BECOME A PARTY TO THE FOLLOWING AGREEMENT BETWEEN CISCO IRONPORT SYSTEMS, LLC, A DELAWARE CORPORATION ("IRONPORT") AND COMPANY (COLLECTIVELY, THE "PARTIES"). BY CLICKING THE ACCEPT BUTTON OR ENTERING "Y" WHEN PROMPTED, YOU REPRESENT THAT (A) YOU ARE DULY AUTHORIZED TO REPRESENT YOUR COMPANY AND (B) YOU ACCEPT THE TERMS AND CONDITIONS OF THIS AGREEMENT ON BEHALF OF YOUR COMPANY, AND AS SUCH, AN AGREEMENT IS THEN FORMED. IF YOU OR THE COMPANY YOU REPRESENT (COLLECTIVELY, "COMPANY") DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, CLICK THE CANCEL BUTTON OR ENTER "N" WHEN

PROMPTED AND PROMPTLY (BUT NO LATER THAT THIRTY (30) DAYS OF THE DELIVERY DATE, AS DEFINED BELOW) NOTIFY IRONPORT, OR THE RESELLER FROM WHOM YOU RECEIVED THE SOFTWARE, FOR A FULL REFUND OF THE PRICE PAID FOR THE SOFTWARE.

1. DEFINITIONS

1.1 "Company Service" means the Company's email or internet services provided to End Users for the purposes of conducting Company's internal business and which are enabled via Company's products as described in the purchase agreement, evaluation agreement, beta or pre-release agreement, purchase order, sales quote or other similar agreement between the Company and IronPort or its reseller ("Agreement") and the applicable user interface and IronPort's standard system guide documentation that outlines the system architecture and its interfaces (collectively, the "License Documentation").

1.2 "End User" means the employee, contractor or other agent authorized by Company to access to the Internet or use email services via the Company Service.

1.3 "Service(s)" means (i) the provision of the Software functionality, including Updates and Upgrades, and (ii) the provision of support by IronPort or its reseller, as the case may be.

1.4 "Software" means: (i) IronPort's proprietary software licensed by IronPort to Company along with IronPort's hardware products; (ii) any software provided by IronPort's third-party licensors that is licensed to Company to be implemented for use with IronPort's hardware products; (iii) any other IronPort software module(s) licensed by IronPort to Company along with IronPort's hardware products; and (iv) any and all Updates and Upgrades thereto.

1.5 "Updates" means minor updates, error corrections and bug fixes that do not add significant new functions to the Software, and that are released by IronPort or its third party licensors. Updates are designated by an increase to the Software's release number to the right of the decimal point (e.g., Software 1.0 to Software 1.1). The term Updates specifically excludes Upgrades or new software versions marketed and licensed by IronPort or its third party licensors as a separate product.

1.6 "Upgrade(s)" means revisions to the Software, which add new enhancements to existing functionality, if and when it is released by IronPort or its third party licensors, in their sole discretion. Upgrades are designated by an increase in the Software's release number, located to the left of the decimal point (e.g., Software

1.x to Software 2.0). In no event shall Upgrades include any new versions of the Software marketed and licensed by IronPort or its third party licensors as a separate product.

2. LICENSE GRANTS AND CONSENT TO TERMS OF DATA COLLECTION

2.1 License of Software. By using the Software and the License Documentation, Company agrees to be bound by the terms of this Agreement, and so long as Company is in compliance with this Agreement, IronPort hereby grants to Company a non-exclusive, non-sublicensable, non-transferable, worldwide license during the Term to use the Software only on IronPort's hardware products, solely in connection with the provision of the Company Service to End Users. The duration and scope of this license(s) is further defined in the License Documentation. Except as expressly provided herein, no right, title or interest in any Software is granted to the Company by IronPort, IronPort's resellers or their respective licensors. This license and any Services are co-terminus.

2.2 Consent and License to Use Data. Subject to Section 8 hereof, and subject to the IronPort Privacy Statement at http://www.IronPort.com/privacy.html, as the same may be amended from time to time by IronPort with notice to Company, Company hereby consents and grants to IronPort a license to collect and use the data from the Company as described in the License Documentation, as the same may be updated from time to time by IronPort ("Data"). To the extent that reports or statistics are generated using the Data, they shall be disclosed only in the aggregate and no End User identifying information may be surmised from the Data, including without limitation, user names, phone numbers, unobfuscated file names, email addresses, physical addresses and file content. Notwithstanding the foregoing, Company may terminate IronPort's right to collect and use Data at any time upon prior written or electronic notification, provided that the Software or components of the Software may not be available to Company if such right is terminated.

3. CONFIDENTIALITY. Each Party agrees to hold in confidence all Confidential Information of the other Party to the same extent that it protects its own similar Confidential Information (and in no event using less than a reasonable degree of care) and to use such Confidential Information only as permitted under this Agreement. For purposes of this Agreement "Confidential Information" means information of a party marked "Confidential" or information reasonably considered by the disclosing Party to be of a proprietary or confidential nature; provided that the Data, the Software, information disclosed in design reviews and any pre-production releases of the Software provided by IronPort is expressly designated Confidential Information whether or not marked as such.

4. PROPRIETARY RIGHTS; OWNERSHIP. Title to and ownership of the Software and other materials and all associated Intellectual Property Rights (as defined below) related to the foregoing provided by IronPort or its reseller to Company will remain the exclusive property of IronPort and/or its superior licensors. Company and its employees and agents will not remove or alter any trademarks, or other proprietary notices, legends, symbols, or labels appearing on or in copies of the Software or other materials delivered to Company by IronPort or its reseller. Company will not modify, transfer, resell for profit, distribute, copy, enhance, adapt, translate, decompile, reverse engineer, disassemble, or otherwise determine, or attempt to derive source code for any Software or any internal data files generated by the Software or to create any derivative works based on the Software or the License Documentation, and agrees not to permit or authorize anyone else to do so. Unless otherwise agreed in writing, any programs, inventions, concepts, documentation, specifications or other written or graphical materials and media created or developed by IronPort or its superior licensors during the course of its performance of this Agreement, or any related consulting or professional service agreements, including all copyrights, database rights, patents, trade secrets, trademark, moral rights, or other intellectual property rights ("Intellectual Property Right(s)") associated with the performance of such work shall belong exclusively to IronPort or its superior licensors and shall, in no way be considered a work made for hire for Company within the meaning of Title 17 of the United States Code (Copyright Act of 1976).

5. LIMITED WARRANTY AND WARRANTY DISCLAIMERS

5.1 Limited Warranty. IronPort warrants to Company that the Software, when properly installed and properly used, will substantially conform to the specifications in the License Documentation for a period of ninety (90) days from the delivery date or the period set forth in the License Documentation, whichever is longer ("Warranty Period"). FOR ANY BREACH OF THE WARRANTY CONTAINED IN THIS SECTION, COMPANY'S EXCLUSIVE REMEDY AND IRONPORT'S ENTIRE LIABILITY, WILL BE PROMPT CORRECTION OF ANY ERROR OR NONCONFORMITY, PROVIDED THAT THE NONCONFORMITY HAS BEEN REPORTED TO IRONPORT AND/OR ITS RESELLER BY COMPANY WITHIN THE WARRANTY PERIOD. THIS WARRANTY IS MADE SOLELY TO COMPANY AND IS NOT TRANSFERABLE TO ANY END USER OR OTHER THIRD PARTY. IronPort shall have no liability for breach of warranty under this Section or otherwise for breach of this Agreement if such breach arises directly or indirectly out of or in connection with the following: (i) any unauthorized, improper, incomplete or inadequate maintenance or calibration of the Software by Company or any third

party; (ii) any third party hardware software, services or system(s); (iii) any unauthorized modification or alteration of the Software or Services; (iv) any unauthorized or improper use or operation of the Software or Company's failure to comply with any applicable environmental specification; or (v) a failure to install and/or use Updates, Upgrades, fixes or revisions provided by IronPort or its resellers from time to time.

5.2 WARRANTY DISCLAIMER. THE EXPRESS WARRANTIES SET FORTH IN SECTION 5.1 OF THIS AGREEMENT CONSTITUTE THE ONLY PERFORMANCE WARRANTIES WITH RESPECT TO THE SOFTWARE OR SERVICES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IRONPORT LICENSES THE SOFTWARE AND SERVICES HEREUNDER ON AN "AS IS" BASIS. EXCEPT AS SPECIFICALLY SET FORTH HEREIN, IRONPORT AND ITS SUPERIOR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, OR STATUTORY (EITHER IN FACT OR BY OPERATION OF LAW), AND EXPRESSLY DISCLAIM ALL OTHER WARRANTIES, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NEITHER IRONPORT NOR ITS THIRD PARTY LICENSORS WARRANT THAT THE SOFTWARE OR SERVICES (1) IS FREE FROM DEFECTS, ERRORS OR BUGS, (2) THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED, OR (3) THAT ANY RESULTS OR INFORMATION THAT IS OR MAY BE DERIVED FROM THE USE OF THE SOFTWARE WILL BE ACCURATE, COMPLETE, RELIABLE AND/OR SECURE.

6. LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR ANY LOSS OF PROFITS, COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, EVEN IF SUCH PARTY RECEIVED ADVANCE NOTICE OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF EITHER PARTY ARISING UNDER ANY PROVISION OF THIS AGREEMENT, REGARDLESS OF WHETHER THE CLAIM FOR SUCH DAMAGES IS BASED IN CONTRACT, TORT, OR OTHER LEGAL THEORY, EXCEED THE TOTAL AMOUNT PAID FOR THE SOFTWARE OR SERVICES DURING THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY.

7. TERM AND TERMINATION. The term of this Agreement shall be as set forth in the License Documentation (the "Term"). If IronPort defaults in the performance of any material provision of this Agreement or the License Documentation, then Company may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day period. If Company defaults in the performance of any material provision of this Agreement or the License Documentation, IronPort may terminate this Agreement upon thirty (30) days written notice if the default is not cured during such thirty (30) day notice and without a refund. This Agreement may be terminated by one Party immediately at any time, without notice, upon (i) the institution by or against the other Party of insolvency, receivership or bankruptcy proceedings or any other proceedings for the settlement of such Party's debts, (ii) such other Party making a general assignment for the benefit of creditors, or (iii) such other Party's dissolution. The license granted in Section 2 will immediately terminate upon this Agreement's termination or expiration. Within thirty (30) calendar days after termination or expiration of this Agreement, Company will deliver to IronPort or its reseller or destroy all copies of the Software and any other materials or documentation provided to Company by IronPort or its reseller under this Agreement.

8. U.S. GOVERNMENT RESTRICTED RIGHTS; EXPORT CONTROL. The Software and accompanying License Documentation are deemed to be "commercial computer software" and "commercial computer software documentation", respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying License Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Company acknowledges that the Software and License Documentation must be exported in accordance with U.S. Export Administration Regulations and diversion contrary to U.S. laws is prohibited. Company represents that neither the United States Bureau of Export Administration nor any other federal agency has suspended, revoked or denied Company export privileges. Company represents that Company will not use or transfer the Software for end use relating to any nuclear, chemical or biological weapons, or missile technology unless authorized by the U.S. Government by regulation or specific license. Company acknowledges it is Company's ultimate responsibility to comply with any and all import and export restrictions, and other applicable laws, in the U.S. or elsewhere, and that IronPort or its reseller has no further responsibility after the initial sale to Company within the original country of sale.

9. MISCELLANEOUS. This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Nothing contained herein shall be construed as creating any agency, partnership, or other form of joint enterprise between the parties. Neither party shall be liable hereunder by reason of any failure or delay in the performance of its obligations hereunder (except for the payment of money) on account of (i) any provision of any present or future law or regulation of the United States or any applicable law that applies to the subject hereof, and (ii) interruptions in the electrical supply, failure of the Internet, strikes, shortages, riots, insurrection, fires, flood, storm, explosions, acts of God, war, terrorism, governmental action, labor conditions, earthquakes, or any other cause which is beyond the reasonable control of such party. This Agreement and the License Documentation set forth all rights for the user of the Software and is the entire agreement between the parties and supersedes any other communications with respect to the Software and License Documentation. The terms and conditions of this Agreement will prevail, notwithstanding any variance with the License Documentation or any purchase order or other written instrument submitted by a party, whether formally rejected by the other party or not. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of IronPort, except that IronPort may modify the IronPort Privacy Statement at any time, in its discretion, via notification to Company of such modification that will be posted at http://www.IronPort.com/privacy.html. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by IronPort or a duly authorized representative of IronPort. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

10. IRONPORT CONTACT INFORMATION. If Company wants to contact IronPort for any reason, please write to IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066, or call or fax us at tel: 650.989.6500 and fax: 650.989.6543.