CHAPTER 5

Cisco IronPort Email Security Plug-in for Lotus Notes の設定および使用方法

この章では、Cisco IronPort Email Security Plug-in for Lotus Notes で利用可能な機能について説明します。Cisco IronPort Email Security Plug-in には、いくつかの共通の電子メール セキュリティ プラグインが含まれます。ここでは、次の項目を取り上げます。

Cisco IronPort Email Security Plug-in for Lotus Notes の一般的な設定

Cisco IronPort Email Security Plug-in for Lotus Notes は、次のような Cisco IronPort Email Security Plug-in をサポートするフレームワークです。

- Reporting Plug-in：このプラグインは、スパム、ウイルス、フィッシング攻撃の電子メールや、スパムであると誤って分類された電子メールの報告に使用します。
- Encryption Plug-in：このプラグインは、暗号化された安全な電子メールの送信に使用します。

Cisco IronPort Email Security Plug-in は、[Options] ページで設定できます。[Options] ページにアクセスするには、[Actions] > [Cisco Email Security] を選択します。

[Cisco Email Security Options] ページ

レポート、暗号化、およびロギングをイネーブルにするには、このタブで各オプションの [Enable] チェックボックスをオンにします。さらに設定を行うには、[Reporting Options...]、[Encryption Options...]、または [Logging Options...] ボ

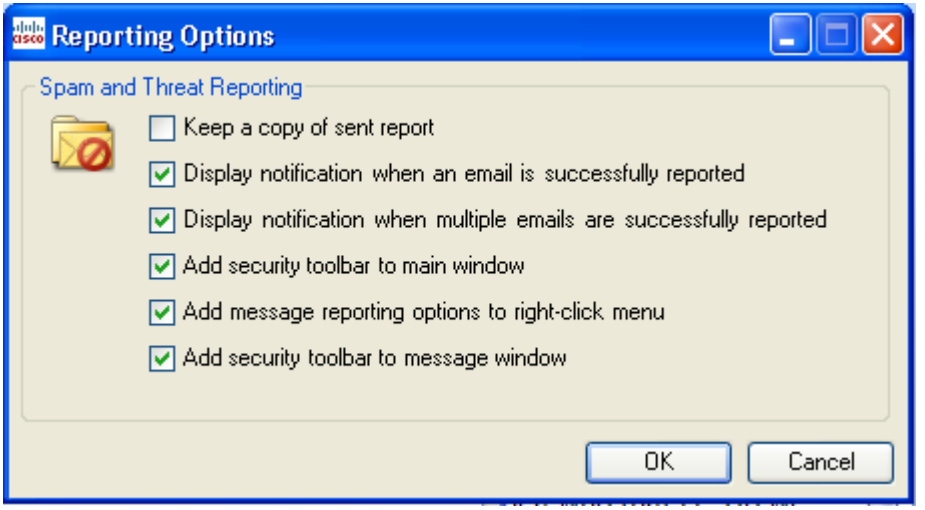
タンをクリックします。問題解決時に診断ツールを使用すると、Cisco IronPort Email Security Plug-in でレポートを実行して、シスコのサポートに送信することもできます。

Reporting Plug-in

[Options] ダイアログ

Reporting Plug-in を使用すると、受信した電子メールがスパム、フィッシング攻撃、ウイルスの場合や、スパムであると誤って分類された場合に、シスコに報告できます。

Cisco Email Security Reporting Plug-in for Lotus Notes は [Options] ダイアログで設定できます。[Reporting Options] ページにアクセスするには、[Actions] > [Cisco Email Security Options] を選択し、ダイアログの [Reporting] タブを選択します。



オプション

ここでは、変更可能なレポート オプションについて説明します。

[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 メッセージや、スパムまたはウイルスであると誤って分類された電子メール メッセージをシスコに報告すると、送信し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]

電子メールの報告時に、このオプションを選択すると電子メールが正常に報告されたことを示す通知アラートを表示できます。

[Display notification when multiple emails are successfully reported]

複数の電子メールの報告時に、このオプションを選択するとすべての電子メールが正常に報告されたことを示す通知アラートを表示できます。

[Add security toolbar to main window]

このオプションを使用すると、セキュリティ ツールバーがメイン ウィンドウに追加されます。

[Add message reporting options to right-click window]

このオプションを使用すると、メッセージ レポート オプションが右クリック ウィンドウに追加されます。

[Add security toolbar to message window]

このオプションを使用すると、セキュリティ ツールバーがメッセージ ウィンドウに追加されます。

Reporting Plug-in for Lotus Notes の使用方法

Cisco Email Security Reporting Plug-in for Lotus Notes を使用すると、受信ボックスに受信したスパム、ウイルス、またはフィッシング メールについてシスコにフィードバックできます。シスコは、このフィードバックを利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。

Lotus Notes でスパム、ウイルス、フィッシング、または誤って分類された電子メールを報告するようにメイン メニュー バーから設定できます。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。報告したメッセージは、シスコの電子メール フィルタの改善に使用され、受信ボックスに一方的に送りつけられるメールを減らすことができます。

Encryption Plug-in

暗号化オプションの設定

Encryption Plug-in の設定は [Cisco Email Security Options] ダイアログで変更できます。暗号化設定を変更するには、[Actions] > [Cisco Email Security Options] を選択し、[Encryption Options] をクリックします。

オプション

暗号化された電子メールを送信するオプション

送信メールを暗号化する場合、電子メールに暗号化のマーク（「フラグ」）を付ける必要があります。これにより、システム管理者によって作成されたフィルタは暗号化する必要があるメッセージを識別できます。

警告　システム管理者に連絡せずに、電子メールに暗号化のフラグを付ける方法を変更しないでください。これらの方法では Cisco IronPort Encryption アプライアンスで変更を行う必要があり、この変更を行えるのはシステム管理者だけです。

次のいずれかの方法で電子メールに暗号化のマークを付けることができます。

- [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] フィールドの先頭に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]* です）。
- [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* を入力した場合、指定された x ヘッダーのメッセージが暗号化されます（デフォルト値は *true* です）。

Encryption Plug-in の使用方法

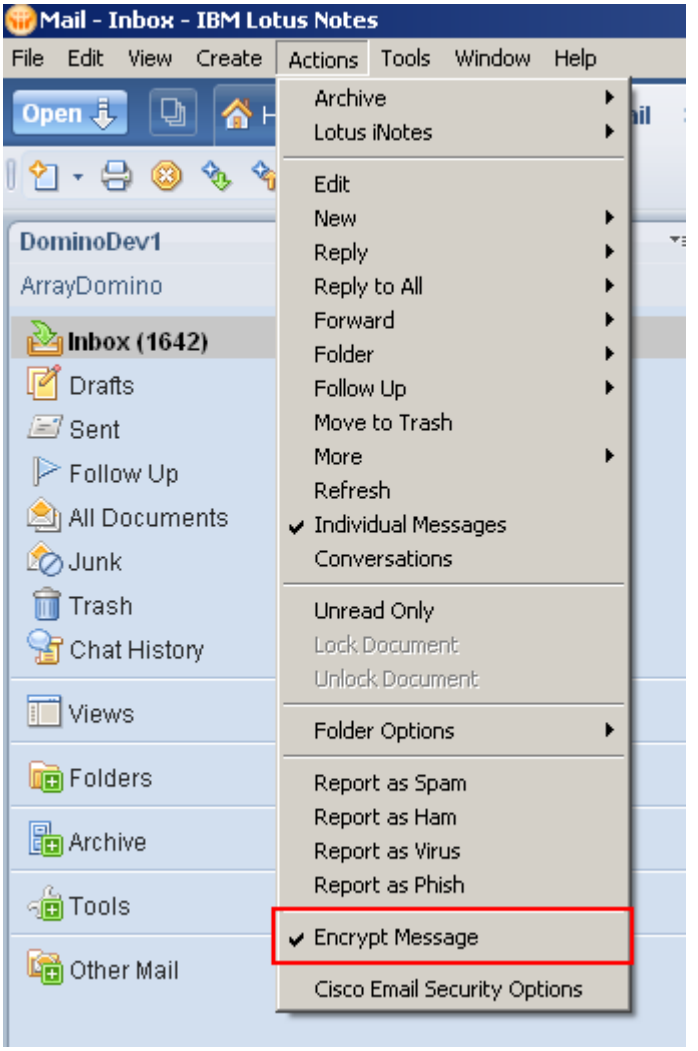
概要

Encryption Plug-in を使用すると、Lotus Notes 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できます。安全な電子メールを送信する場合、Cisco Email Security Encryption Plug-in は暗号化のマークが付けられた電子メールを安全に送信し、目的の受信者だけがそのメールを読めるようにします。

安全な電子メールの送信

メール システムで安全な電子メールを送信するには、[Actions] メニューの [Encrypt Message] をオンにします。

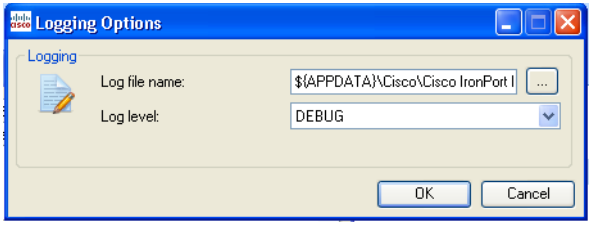
安全なメッセージを送信するには、次のように [Encrypt Message] がオンになっていることを確認します。



[Logging Options] の変更

[Logging Options] ページを開くには、[Logging Options...] をクリックします。

[Logging Options]



オプション

[Logging] メニューから次のオプションを設定できます。

[Log file name]

%appdata%\Cisco に保存されるログ ファイルの名前を指定できます。ログ ファイル名には .log 拡張子が必要です。

[Log level]

ログ レベルは、ログ ファイルに記録される情報を指定します。次のいずれかのログ レベルを選択できます。

- [ERROR] : エラー メッセージおよび例外状況をログに記録します。
- [WARN] : [ERROR] で記録されるメッセージおよび警告メッセージがログに記録されます。
- [INFO] : 基本情報およびその他のステータス メッセージがログに記録されます。自動更新プロセスのステータス メッセージがログに記録されます。[WARN] および [ERROR] で記録されるメッセージもすべてログに記録されます。
- [DEBUG] : 設定に関する詳細情報がログに記録されます。[ERROR]、[WARN]、および [INFO] のすべてのエラー メッセージ、および問題のトラブルシューティングに役立つ可能性がある情報がログに記録されます。

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 IronPort Email Security Plug-in に関する問題が発生した場合、ログ レベルを [DEBUG] に設定すると、開発者が問題を再現して診断を実行できるように最大限の情報を提供できます。

トラブルシューティングと診断

ここでは、Cisco IronPort Email Security Plug-in for Lotus Notes の使用中に発生する可能性がある一般的なエラー、およびそれらのエラーを修正するための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 メッセージが数回表示され、このエラーによって Cisco IronPort Email Security Plug-in for Lotus Notes の機能が影響を受ける場合、修復プロセスを実行してみてください。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、「Cisco Email Security 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。

一般的な起動エラー

コンフィギュレーション ファイルの初期化中に発生するエラー

Outlook の起動時に次のメッセージが表示されることがあります。

- 「Error occurred during Cisco IronPort Email Security Plug-in configuration file initialization.Some settings set to default values.」
- 「Error during reading configuration for Reporting component.Some settings set to default values.」
- 「Error during reading configuration for Encryption component.Some settings set to default values.」

上記のエラー メッセージは、コンフィギュレーション ファイル（*%appdata%\Cisco\Cisco Email Security Plug In\LotusNotes\CommonConfig.xml*）の一部の値が破損した場合に表示されます。

解決策

プラグインは破損したコンフィギュレーション ファイルをデフォルト値に戻します。引き続きエラー メッセージが表示される場合は、修復プロセスを実行してコンフィギュレーション ファイルを修正します。

コンフィギュレーション ファイルが見つからない。設定がデフォルト値に設定される。

Outlook の起動時に次のエラー メッセージのいずれかが表示されることがあります。

- 「Cisco IronPort Email Security Plug-in configuration file not found.Settings set to default values.」
- 「Configuration file for Encryption component was not found.Settings set to default values.」
- 「Configuration file for Reporting component was not found.Settings set to default values.」

解決策

プラグインは破損したコンフィギュレーション ファイルをデフォルト値に戻します。引き続きこのエラー メッセージが表示される場合は、修復プロセスを実行してコンフィギュレーション ファイルを修正します。

メッセージ報告エラー

無効な電子メール アドレス

Lotus Notes で [Report as Spam]、[Report as Virus]、[Report as Phish]、または [Report as 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。

「Invalid address for report type.Please update configuration file.」（レポート タイプに無効なアドレスです。コンフィギュレーション ファイルを更新してください。）

このエラー メッセージは、Reporting Plug-in を使用していて、報告しようとしている電子メールの形式が不適切な場合に表示されます。スパムおよびフィッシング 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」として報告できるように）、Reporting Plug-in ファイルを修正する必要があります。

解決策

%appdata%\Cisco\Cisco Email Security Plug In\LotusNotes フォルダ内のレポート設定を確認します。その設定を削除して、修復プロセスを実行してデフォルト値に戻します。

Cisco IronPort Email Security Plug-in for Lotus Notes ファイルの修復

1. [Control Panel] > [Add or Remove Programs] を選択します。
2. プログラムの一覧で Cisco IronPort Email Security Plug-in を見つけて、[Change] をクリックします。
3. Lotus Notes が終了していることを確認します。
4. Cisco IronPort Email Security Plug-in インストーラを選択して、[Repair] オプション ボタンをクリックします。
5. [Next] 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。
6. 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 Email Security 診断ツール

問題を十分に分析するために必要な詳細情報をシスコに送信できる、Cisco IronPort Email Security Plug-in 用の診断ツールが用意されています。エラーが発生した場合や、修復プロセスでは解決できない Cisco IronPort Email Security Plug-in に関する問題が発生した場合に、診断ツールを使用します。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。

エラーが発生した場合、トラブルシューティングのヒントの「Diagnostic」の項を参照してください。

Cisco 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 Email Security の出力ファイル
- Windows および Lotus Notes に関する情報
- システム ユーザ名および PC 名
- その他の Lotus Notes プラグインに関する情報

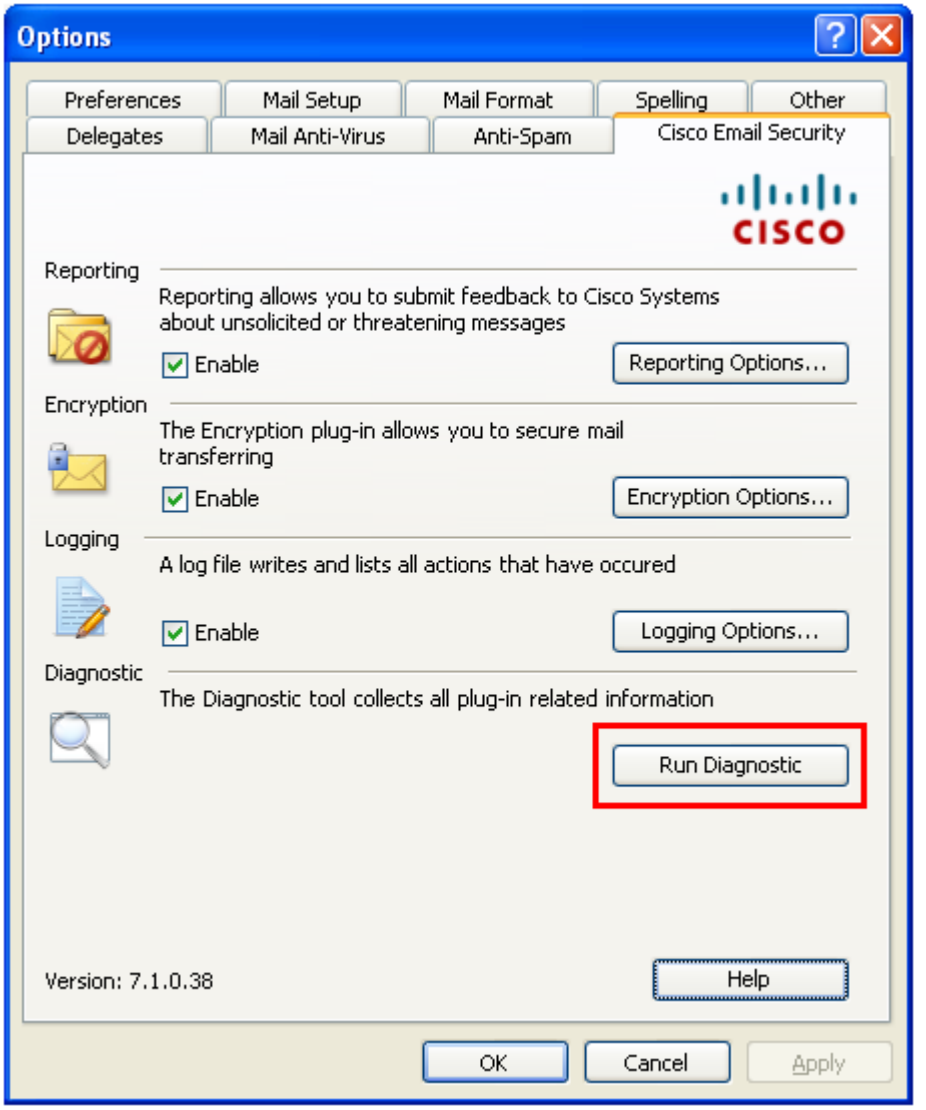
Cisco Email Security 診断ツールの実行

Cisco Email Security 診断ツールは次の場所のいずれかから実行できます。

- **Cisco Email Security の [Options] ダイアログから**：通常、Cisco Email Security の [Options] ダイアログから診断ツールを実行します。診断ツールにアクセスするには、[Actions] > [Cisco Options] を選択します。
- **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。

[Options] ダイアログからの診断ツールの実行

[Actions] > [Cisco Email Security Options] を選択して、[Run Diagnostics] をクリックします。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。診断ツールは、*CiscoDiagnosticReport.zip* という zip ファイルにデータを保存します。

[Go to Report] をクリックして *CiscoDiagnosticReport.zip* ファイルに移動し、システム管理者またはシスコ セキュリティ管理者にファイルを手動で送信できます。

Program Files からの診断ツールの実行

診断ツールを実行するには、[Start] > [Programs] > [Cisco Email Security for Lotus Notes] を選択します。または、Cisco Email Security がインストールされているフォルダ（通常は C:¥Program Files¥Cisco¥Cisco IronPort Email Security Plug-in）に移動して、*Cisco.EmailSecurity.Framework.Diagnostic.exe* ファイルをダブルクリックします。

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] の [Add/Remove Program] を使用するか、setup.exe プログラムを実行します。

アンインストール中、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

（注） プラグインをアンインストールしても Lotus Notes のパフォーマンスには影響しません。

プラグインのアンインストール手順

Cisco IronPort Email Security Plug-in 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。

- [Start] > [Control Panel] > [Add/Remove Programs] をクリックします。Cisco IronPort Email Security Plug-in を選択し、[Remove] をクリックします。

  または

- 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。