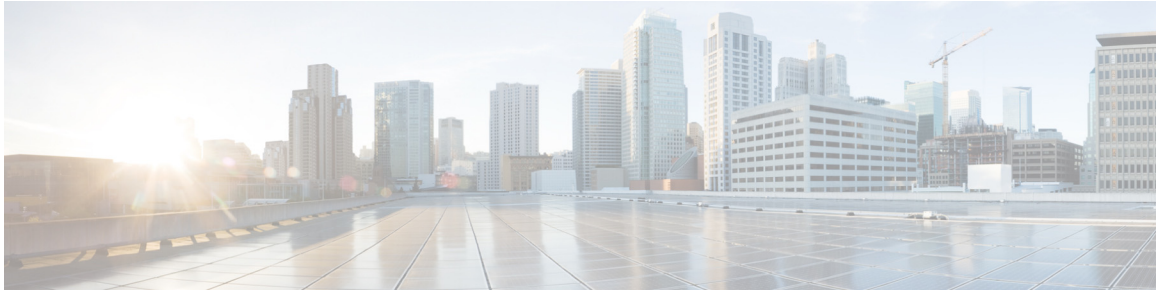

Cisco Secure Email and Web Manager 用 AsyncOS 14.2 リリースノート：MD（メンテナンス導入）

発行日：2022 年 5 月 26 日

改訂日：2023 年 11 月 27 日

目次

（注） スパムの隔離ポータルにログインする際は、正確な電子メール ID とドメイン名を必ず入力してください。

（注） 別の管理者ログインで管理されている Cisco SecureX アカウントをすでに持っている場合は、SSE にデバイスを登録してからスマートライセンス登録を実行することを推奨します。最初にデバイスを SSE に登録せずにスマートライセンス登録を実行しないでください。これは既知の問題（不具合 ID：CSCvy10226）です。

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

機能	説明
PVO 検疫しきい値アラート	Cisco Secure Email and Web Manager では、PVO 検疫メッセージの数が、特定の期間と PVO 検疫に対して設定されたユーザー定義のしきい値を超えると、受信者にアラートが送信されます。 Cisco Secure Email and Web Manager を使用すると、電子メールとして設定したアラートを受信できます。 次の方法を使用して、PVO 検疫しきい値アラートを設定できます。 • レガシー Web インターフェイスの [電子メール（Email）] > [メッセージ検疫（Message Quarantine）] > [ポリシー、ウイルス、およびアウトブレイク検疫（Policy, Virus, and Outbreak Quarantines）] ページ • CLI の `quarantineconfig` コマンド 詳細については、ユーザーガイドの「Centralized Policy, Virus, and Outbreak Quarantines」の章の「PVO Quarantine Threshold Alert」セクションを参照してください。
共有メールボックス用のエンドユーザー検疫の設定	管理者がシングルサインオンによる EUQ へのアクセスを有効にしていて、共有メールボックスへの委任アクセス権を持っている場合、その共有メールボックスのエンドユーザー検疫（EUQ）にアクセスして、スパム検疫済みメッセージに対して任意のアクションを実行できるようになりました。そのため、管理者のワークロードが軽減され、検疫済みメッセージのタイムリーな配信が可能になります。 SAML 2.0 認証を使用して EUQ にログインできる場合、EUQ にアクセスして共有メールボックスのスパム検疫メッセージを検索できます。プライマリメールボックスのスパム検疫済みメッセージを表示したり、アクセスできる共有メールボックスを追加して、その共有メールボックスのスパム検疫済みメッセージを表示したりできます。 EUQ を使用すると、複数の共有メールボックスを追加でき、スパム検疫済みメッセージを表示、検索、リリース、リリースしてセーフリストに追加、および削除するオプションが使用可能になります。 共有メールボックスには、次の方法でアクセスできます。 • スパム検疫通知メールに含まれている [電子メールの隔離（email quarantine）] または [すべての隔離済みメッセージを表示（View All Quarantined Messages）] リンクをクリックします。 • スパム検疫ポータルを使用して、Cisco Secure Email and Web Manager EUQ にログインします。 詳細については、ユーザーガイドの「Spam Quarantine」の章の「Configuring End-User Quarantine for Shared Mailbox」セクションを参照してください。 （注） Office 365 ユーザーは、この機能を使用できます。この機能では、Microsoft Azure Active Directory API を使用して、共有メールボックスに関連付けられたエンドユーザー検疫へのアクセスが提供されます。

中央集中型電子メールトラッキングサービスのデータストレージ時間の管理	日数に基づいて中央集中型電子メール トラッキング データベースにメッセージ(データ)を保存するように Cisco Secure Email and Web Manager を設定できるようになりました。 この機能は、次のいずれかの方法で設定できます。 • レガシー Web インターフェイスの [システム管理(System Administration)] > [ディスク管理(Disk Management)] > [データディスク管理の編集(Edit Data Disk Management)] ページで、[データストレージ時間の適用] オプションを使用する。 • CLI の `diskquotaconfig > edit > Centralized Email Tracking` サブコマンドで `Manage data based on the storage time` ステートメントを使用する。 **重要**:Cisco Secure Email and Web Manager 13.6.2 バージョン以降、Splunk データベースは電子メールトラッキングデータに使用されなくなりました。新しい電子メールトラッキングデータはすべて Lucene データベースに保存されます。この機能を使用すると、電子メールトラッキングデータを含む Splunk データベースが自動的に削除されます。 **アクション**:電子メールトラッキングデータのバックアップを作成します(必要な場合)。CLI の `backupconfig` コマンドを使用して、バックアップアクションを実行できます。詳細については、ユーザーガイドの「Common Administrative Tasks」の章の「Scheduling Single or Recurring Backups」セクションを参照してください。 **(注)** 組織のネットワークにある Cisco Secure Email and Web Manager が 1 つだけの場合は、ネットワークに新しい仮想マシン(VM)を展開する必要があります。仮想 Cisco Secure Email and Web Manager の展開方法の詳細については、『Cisco Secure Email and Web 仮想アプライアンス設置ガイド』を参照してください。 詳細については、ユーザーガイドの「Common Administrative Tasks」の章の「Managing Data Storage Time」セクションを参照してください。

ファイル分析レポート用のアプライアンスのグループ化に対する強化	Cisco Secure Email and Web Manager は、スマートアカウント ID を使用して、組織内のアプライアンスをグループ化し、すべてのアプライアンスのファイル分析結果を表示するようになりました。 Cisco Secure Email and Web Manager でスマートライセンスが有効になっている場合、ファイル分析レポート用にアプライアンスグループを設定すると、システムによりスマートアカウント ID がアプライアンスグループ ID として自動的に登録されます。アプライアンスグループ ID はいつでも変更でき、変更はコミットアクションなしですぐに有効になります。 **（注）** この機能を使用するには、電子メール ゲートウェイと Cisco Secure Email and Web Manager を 14.2 バージョンにアップグレードする必要があります。 詳細については、ユーザーガイドの「Using Centralized Email Security Reporting」の章の「(Cloud File Analysis) Configure the Management Appliance to Display Detailed File Analysis Result」セクションを参照してください。 **（注）** この機能はオンプレミスの管理者ユーザーのみが使用できます。
新しい送信者ドメインのレピュテーション判定	このリリースでは、送信者ドメインのレピュテーションの判定は、意図する意味と推奨される使用法を正確に反映するように更新されています。 AsyncOS 14.2.x リリースにアップグレードすると、レポートおよびメッセージトラッキングの従来の SDR 判定は、次のように新しい SDR 判定に置き換えられます。 • 信頼できない • 要検討 • ニュートラル • 好ましい • 信頼できる • 不明 SDR レポートとメッセージトラッキングの結果は、アップグレード時に新しい判定で更新されます。電子メールゲートウェイも、新しい SDR 判定を含む最新の 14.2 バージョンにアップグレードしてください。 **（注）** SDR レポーティングおよびトラッキング AsyncOS API は、新しい SDR 脅威レベルとカテゴリ構造を反映するように更新されています。 **（注）** SDR トラッキングログが更新され、新しい SDR 脅威レベルと送信者の成熟度の詳細が反映されます。

Cisco Secure Email Cloud Gateway 用 AsyncOS 14.2 の新機能のサポート	[URL レトロスペクションレポート（URL Retrospection Report）] ページ：このレポートページには、URL レトロスペクティブサービスによって処理された URL が表示されます。また、悪意のある URL、URL レトロスペクティブサービスから判定を受け取った日時、影響を受けたメッセージの修復ステータスが一覧表示されます。 （注） URL レトロスペクション レポート データは、クラウド管理者ユーザーのみが利用できます。 詳細については、ユーザーガイドの「Using Centralized Email Security Reporting」の章の「URL Retrospection Report Page」セクションを参照してください。
スマート ソフトウェア ライセンシングの機能強化	スマート ソフトウェア ライセンシング機能に加えられた拡張機能は次のとおりです。 **ライセンス予約**：Cisco Smart Software Manager（CSSM）ポータルに接続せずに、Cisco Secure Email and Web Manager で有効になっている機能のライセンスを予約できます。これは主に、インターネットや外部デバイスとの通信がない高度にセキュリティ保護されたネットワーク環境に Cisco Secure Email and Web Manager を展開するユーザーにとって有益です。 詳細については、ユーザーガイドの「Common Administrative Tasks」の章の「Overview」および「Reserving Feature Licenses」セクションを参照してください。 **Device Led Conversion（DLC）**：Cisco Secure Email and Web Manager をスマートライセンスに登録すると、既存の有効なクラシックライセンスはすべて、Device Led Conversion（DLC）プロセスを使用して自動的にスマートライセンスに変換されます。これらの変換されたライセンスは、CSSM ポータルのバーチャルアカウントで更新されます。 詳細については、ユーザーガイドの「Common Administrative Tasks」の章の「Overview」セクションを参照してください。
クラシックライセンスの変更：Web インターフェイスおよび CLI の期限日	このリリース以降、クラシックライセンスの Web インターフェイスおよび CLI の既存の [期限日（Expiration Date）] 列ヘッダーが [期限日（猶予期間を含む）（Expiration Date (including grace period)）] に変更されます。これは、期限日に猶予期間が含まれることを示しています。 （注） すべてのアラートメッセージとメールログは、機能キーの猶予期間を含む期限日を表示するように変更されます。

Syslog プッシュ用の新しいパラメータ：Syslog ディスクバッファ	（TCP プロトコルのみに適用可能）：Syslog ディスクバッファのパラメータを使用すると、Syslog プッシュ ログ サブスクリプションのローカルディスクバッファを設定でき、リモート Syslog サーバーを使用できない場合、Cisco Secure Email and Web Manager がログイベントをキャッシュできます。Syslog サーバーが使用可能になると、Cisco Secure Email and Web Manager は、そのログサブスクリプションのバッファにあるすべてのデータを Syslog サーバーに送信し始めます。 詳細については、ユーザーガイドの「Logging」の章の「Log Retrieval」セクションを参照してください。
電子メールトラッキングデータ用の Splunk データベースは未サポート	Web インターフェイスまたは CLI を使用して Cisco Secure Email and Web Manager にログインすると、電子メールトラッキングデータに Splunk データベースを使用している場合、次のメッセージが表示されることがあります。 *「Splunk データベースに x GB の電子メールトラッキングデータがあります。Cisco Secure Email and Web Manager 13.6.2 バージョン以降、Splunk データベースは電子メールトラッキングデータに使用されなくなりました。新しい電子メールトラッキングデータはすべて、Lucene データベースに保存されます。Cisco Secure Email and Web Manager の今後の一般提供（GA）リリースでは、電子メールトラッキングデータ用の Splunk データベースのサポートはありません。* **アクション**：電子メールトラッキングデータのバックアップを作成します（必要な場合）。CLI の `backupconfig` コマンドを使用して、バックアップアクションを実行できます。詳細については、ユーザーガイドの「Common Administrative Tasks」の章の「Scheduling Single or Recurring Backups」セクションを参照してください。 **（注）** 組織のネットワークにある Cisco Secure Email and Web Manager が 1 つだけの場合は、ネットワークに新しい仮想マシン（VM）を展開する必要があります。仮想 Cisco Secure Email and Web Manager の展開方法の詳細については、『Cisco Secure Email and Web 仮想アプライアンス設置ガイド』を参照してください。 **（注）** この動作は、オンプレミスの Cisco Secure Email and Web Manager にのみ適用されます。

動作における変更

JWT トークン:エラーメッセージの変更	このリリース以前は、JSON Web トークン(JWT)トークンを使用して API 要求を行う際に JWT トークンが期限切れになっていると、期限切れトークンのエラーメッセージが表示されました。 このリリース以降は、JWT トークンを使用して API 要求を行う際に、使用された JWT トークンが 12 時間より古い場合、無効なトークンまたは期限切れのトークンのエラーメッセージが表示されます。期限切れトークンのエラーメッセージは、トークン生成から最大 12 時間しか表示されません。
SPoG 機能の変更内容	SPoG を有効または無効にすると、新しい Web インターフェイスに同時にログインしているすべてのユーザーのセッションが無効になり、サーバーへの新しい要求によってログアウトされます。ユーザーは再度ログインする必要があります。 また、Cisco Secure Email and Web Manager が SPoG に追加されており、現在同じ Cisco Secure Email and Web Manager の新しい Web インターフェイスにログインしている場合は、JWT 検証のフローが変更されたため、ログアウトされます。 (注) SPoG 機能は、SPoG クラスタの下の Cisco Secure Email and Web Manager がすべて同じバージョンである場合にのみ動作します。
新しいコマンドの導入 - `wsaupdatesconfig`	このリリース以降、Secure Email and Web Manager は新しい `wsaupdatesconfig` コマンドをサポートします。`wsaupdatesconfig` コマンドは、Secure Email and Web Manager 上の WBRS、AVC、または WBRS と AVC の両方のデータを強制的に更新します。
絶対タイムアウトの変更	このリリース以前は、デフォルトの Web UI の [非アクティブタイムアウト(Inactivity Timeout)] フィールドを 12 時間以上に設定した場合、12 時間経過しても Cisco Secure Email and Web Manager の新しい Web インターフェイスからログアウトされず、インターフェイスで使用可能なオプションにアクセスできました。 このリリースにアップグレード後は、デフォルトの Web UI の [非アクティブタイムアウト(Inactivity Timeout)] フィールドを 12 時間以上に設定しても、12 時間経過すると Cisco Secure Email and Web Manager の新しい Web インターフェイスからログアウトされます。
レポートカレンダーの変更	このリリース以前の新しい Web インターフェイスでは、月ごとに集計されているレポートデータの日付を選択できましたが、データが月ごとに集計されている場合にのみ月次データを表示できるため、日付に対して間違った結果が表示されました。 このリリースにアップグレード後は、毎月初日のみを選択できるため、その月の完全なレポートデータが表示されます。

メールログの変更	このリリース以前は、メールログの件名の情報は引用符で囲まれていませんでした。 このリリースにアップグレード後は、メールログの件名の情報は二重引用符で囲まれるようになりました。
FQDN 検証の変更	このリリース以降、ピア証明書を検証するか、証明書をインポートするときに、インポートする証明書またはサーバー証明書で件名（共通名）フィールドが使用できない場合、FQDN 検証は SAN 拡張が重要かどうかを確認します。 （注） この動作の変更は、証明書のインポートまたはピア証明書の検証中に FQDN 検証を有効にしている場合にのみ適用されます。
アップデータサーバーの CA 証明書の変更	このリリースで加えられたアップデータサーバーの CA 証明書の動作の変更は次のとおりです。 • FQDN 検証は、Cisco Secure Email and Web Manager にアップデータサーバーの CA 証明書を追加するときに実行されます。新しいステートメント「共通名または SAN:dNSName あるいは両方が完全修飾ドメイン名（FQDN）形式であるか確認しますか？（Do you want to check if Common Name or SAN:dNSName or both are in Fully Qualified Domain Name(FQDN) format?）」が、FQDN 検証を実行するための CLI の `updateconfig > trusted_certificates > add` サブコマンドに追加されます。 • CA 証明書の検証は、Cisco Secure Email and Web Manager にアップデータ CA 証明書を追加するときに実行されます。 （注） Cisco Secure Email and Web Manager では、ルート CA 証明書とチェーン内の他の証明書が信頼されている場合、アップデータ CA 証明書を追加できます。
システムアップグレード中の CA 証明書の検証	このリリース以降、Cisco Secure Email and Web Manager をアップグレードすると、CA 証明書がアクティブ（期限切れではない）で、証明書の CA フラグが true に設定されている場合にのみ、既存の CA 証明書がアップグレードされます。Cisco Secure Email and Web Manager では、システムのアップグレード中に期限切れの証明書と CA フラグが false に設定された CA 証明書が拒否されます。また、Cisco Secure Email and Web Manager に構成ファイルをロードすると、CA フラグが false に設定された CA 証明書と期限切れの証明書が削除されます。

新しい Web インターフェイスへのアクセス

（注） 次世代のユーザーインターフェイスは、Trailblazer が有効になっている場合に最適なため、Trailblazer を有効にして新しいインターフェイスにアクセスすることをお勧めします。

新しい Web インターフェイスでは、レポートのモニタリング、検疫、およびメッセージ検索機能が新しくなりました。

（注） アプライアンスの新しい Web インターフェイスは、AsyncOS API HTTP/HTTPS ポート（6080/6443）および trailblazer HTTPS ポート（4431）を使用します。CLI で `trailblazerconfig` コマンドを使用して、trailblazer HTTPS ポートを設定できます。trailblazer HTTPS ポートがファイアウォールで開かれていることを確認します。

新しい Web インターフェイスには次のいずれかの方法でアクセスできます。

- `trailblazerconfig` CLI コマンドが有効になっている場合は、`https://example.com:<trailblazer-https-port>/ng-login` の `URL` を使用します。

  ここで、`example.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスで設定されている trailblazer の HTTPS ポートです。

  デフォルトで、`trailblazerconfig` はアプライアンスで有効になっています。

  - 設定した HTTPS ポートがファイアウォールで開かれていることを確認します。デフォルトの HTTPS ポートは 4431 です。
  - また、アプライアンスにアクセスするために指定したホスト名を DNS サーバーが解決できることを確認します。

- `trailblazerconfig` CLI コマンドが無効になっている場合は、`https://example.com:<https-port>/ng-login` の `URL` を使用します。

  ここで、`example.com` はアプライアンスのホスト名で、`<https-port>` はアプライアンスで設定されている HTTPS ポートです。

（注） trailblazerconfig CLI コマンドが無効になっている場合は、特定のブラウザの API ポートに複数の証明書を追加する必要がある場合があります。

- アプライアンスにログインし、[セキュリティ管理アプライアンスの外観が新しくなりましたので、**お試しください（Security Management Appliance is getting a new look. Try it!）] をクリックして、**新しい Web インターフェイスに移動します。

新しい Web インターフェイスは新しいブラウザウィンドウで開きます。それにアクセスするには、再度ログインする必要があります。アプライアンスから完全にログアウトする場合は、アプライアンスの新しい Web インターフェイスとレガシー Web インターフェイスの両方からログアウトする必要があります。

HTML ページのシームレスなナビゲーションとレンダリングのために、次のブラウザを使用してアプライアンスの新しい Web インターフェイス（AsyncOS 12.0 以降）にアクセスすることをお勧めします。

- Google Chrome（最新の安定バージョン）
- Mozilla Firefox（最新の安定バージョン）
- Safari（最新の安定バージョン）

サポートされているブラウザのいずれかで、アプライアンスのレガシー Web インターフェイスにアクセスできます。

アプライアンスの新しい Web インターフェイス（AsyncOS 12.0 以降）でサポートされている解像度は、1280 X 800 ～ 1680 X 1050 です。すべてのブラウザに対して最適に表示される解像度は 1440 X 900 です。

（注） シスコでは、より高い解像度でアプライアンスの新しい Web インターフェイスを表示することは推奨していません。

エンドユーザーは、以下のいずれかの方法で、新しい Web インターフェイスのスパム検疫にアクセスできるようになりました。

- `trailblazerconfig` CLI コマンドが有効になっている場合は、`https://example.com:<trailblazer-https-port>/euq-login` の URL を使用します。

  ここで、`example.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスで設定されている trailblazer の HTTPS ポートです。

- `trailblazerconfig` CLI コマンドが無効になっている場合は、`https://example.com:<https-port>/euq-login` の URL を使用します。

  ここで、`example.com` はアプライアンスのホスト名で、`<https-port>` はアプライアンスで設定されている HTTPS ポートです。

（注） HTTP/HTTPS ポートおよび AsyncOS API ポートがファイアウォールで開かれていることを確認します。

アップグレード パス

リリース 14.2.0-241 MD（メンテナンス導入）へのアップグレード

次のバージョンから、リリース 14.2.0-241 にアップグレードすることができます。

- 12.8.1-021
- 13.8.1-108
- 13.8.1-110
- 14.2.0-224

リリース 14.2.0-224 MD（メンテナンス導入）へのアップグレード

次のバージョンから、リリース 14.2.0-224 にアップグレードできます。

- 13.8.1-052
- 13.8.1-068
- 13.8.1-074
- 13.8.1 - 090
- 13.8.1-101
- 13.8.1-102
- 13.8.1-108
- 14.0.0 - 404
- 14.0.0 - 418
- 14.1.0-199
- 14.1.0-227
- 14.1.0-239
- 14.1.0-250
- 14.2.0-203
- 14.2.0-206
- 14.2.0-212
- 14.2.0-217

インストールおよびアップグレードに関する注意事項

重要な追加資料

関連する E メールセキュリティおよび Web セキュリティのリリースのリリースノートも確認する必要があります。

この情報へのリンクについては、関連資料（17 ページ）を参照してください。

仮想アプライアンス

仮想アプライアンスのセットアップについては、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。このドキュメントは、https://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/products-installation-guides-list.html から入手できます。

（注） 仮想アプライアンスのファイバ ネットワーク インターフェイス カードには、AsyncOS バージョン 12.5 以降との互換性がありません。これは既知の問題です。障害 ID：CSCvr26218

仮想アプライアンスのアップグレード

現在の仮想アプライアンスのリリースが 2 TB 以上のディスク領域をサポートしておらず、このリリースで 2 TB 以上のディスク領域を使用する場合は、仮想アプライアンスを単にアップグレードすることはできません。

代わりに、このリリース用に新しい仮想マシンインスタンスを導入する必要があります。

仮想アプライアンスをアップグレードしても、既存のライセンスは変更されません。

ハードウェア アプライアンスから仮想アプライアンスへの移行

ステップ 1 仮想アプライアンス（12 ページ）で説明されているマニュアルを使用して、仮想アプライアンスをセットアップします。

ステップ 2 物理アプライアンスをこの AsyncOS リリースにアップグレードします。

ステップ 3 アップグレードされた物理アプライアンスからコンフィギュレーション ファイルを保存します。

ステップ 4 ハードウェア アプライアンスから仮想アプライアンスにコンフィギュレーション ファイルをロードします。

ディスク領域とネットワーク設定に関連する適切なオプションを選択してください。

次の作業

ハードウェア アプライアンスをバックアップ アプライアンスとして使用する場合は、ユーザーガイドまたはオンラインヘルプでバックアップに関する情報を参照してください。たとえば、バックアップ アプライアンスが管理対象の E メールセキュリティおよび Web セキュリティアプライアンスから直接データを取得しないようにするか、または Web セキュリティアプライアンスに設定を公開する必要があります。

アップグレード前の要件

次の重要なアップグレード前タスクを実行します。

- 関連する E メールセキュリティおよび Web セキュリティアプライアンスのバージョンの確認（13 ページ）
- 既存の設定のバックアップ（13 ページ）
- ポリシー、ウイルス、およびアウトブレイク検疫の FIPS モードでの一元管理設定（13 ページ）

関連する E メールセキュリティおよび Web セキュリティアプライアンスのバージョンの確認

アップグレードする前に、管理する E メール セキュリティ アプライアンス と Web セキュリティ アプライアンス が互換性のあるリリースを実行していることを確認します。インストールおよびアップグレードに関する注意事項（11 ページ）を参照してください。

既存の設定のバックアップ

Cisco Secure Email and Web Manager をアップグレードする前に、既存のセキュリティ管理アプライアンスから XML 設定ファイルを保存します。アプライアンスから任意の場所にこのファイルを保存します。重要な注意事項と手順については、ユーザーガイドまたはオンラインヘルプの「Saving and Exporting the Current Configuration File」のセクションを参照してください。

ポリシー、ウイルス、およびアウトブレイク検疫の FIPS モードでの一元管理設定

管理対象の E メール セキュリティ アプライアンスを FIPS モードで AsyncOS 14.2 以降にアップグレードすると、ポリシー、ウイルス、およびアウトブレイク検疫の一元管理設定が無効になります。AsyncOS 13.0 以降、E メール セキュリティ アプライアンスの FIPS モードでは、2048 ビットの証明書を使用して、ポリシー、ウイルス、およびアウトブレイク検疫の一元管理設定が有効になります。以前の AsyncOS バージョンには、サイズが 1024 ビットの証明書があります。

ポリシー、ウイルス、アウトブレイク検疫の一元管理を有効にする手順は次のとおりです。

ステップ 1 Cisco Secure Email and Web Manager アプライアンスを AsyncOS 14.2 にアップグレードします。

ステップ 2 Cisco E メール セキュリティ アプライアンスをサポートされている最新バージョンにアップグレードします。

アップグレード後、ポリシー、ウイルス、およびアウトブレイク検疫の集中型設定が無効になります。

ステップ 3 アップグレードした Cisco セキュリティコンテンツ管理アプライアンスで、CLI コマンド `updatepvocert` を実行します。

集中型のポリシー、ウィルス、およびアウトブレイク検疫の CA 証明書は 2048 ビットに更新されます。

ステップ 4 アップグレードした Cisco E メール セキュリティ アプライアンスで、ポリシー、ウイルス、アウトブレイク検疫の一元管理が有効になっているかどうかを確認します。詳細については、『Cisco Security Content Management Appliance User Guide』を参照してください。

アップグレード中の IPMI メッセージ

CLI を使用してアプライアンスをアップグレードする場合、IPMI に関連するメッセージが表示されることがあります。これらのメッセージは無視しても差し支えありません。この動作は既知の問題です。

障害 ID：CSCuz33125

このリリースへのアップグレード

ステップ 1 アップグレード前の要件（12 ページ）で説明されているすべてのトピックに対処します。

ステップ 2 このリリースのユーザーガイド PDF の「Before You Upgrade: Important Steps」セクションに記載されているすべての手順に従ってください。

ステップ 3 アップグレードを実行します。

既存のリリースのユーザーガイド PDF の「Common Administrative Tasks」の章の「Upgrading AsyncOS」のセクションの手順に従ってください。

（注） リブートしてから少なくとも 20 分経過するまで、いかなる理由があっても（アップグレードの問題をトラブルシューティングするためであっても）アプライアンスの電源をオフにしないでください。仮想アプライアンスがある場合は、ハイパーバイザまたはホスト OS ツールを仮想マシンのリセット、サイクル、または電源オフに使用しないでください。

ステップ 4 約 10 分後、アプライアンスにアクセスしてログインします。

ステップ 5 このリリースのユーザーガイド PDF の「After Upgrading」のセクションに記載されている手順に従ってください。

ステップ 6 該当する場合は、ハードウェア アプライアンスから仮想アプライアンスへの移行（12 ページ）を参照してください。

重要：このリリースにアップグレード後、ブラウザの操作をシームレスにするために、以下のいずれかのステップを試行できます。

- Web インターフェイスで使用される証明書を承認し、新しいブラウザウィンドウで `https://hostname.com:<https_api_port>`（例：`https://some.example.com:6443`）の URL 構文を使用して証明書を承認します。ここで、`<https_api_port>` は [ネットワーク（Network）] > [IP インターフェイス（IP Interfaces）] で設定されている AsyncOS API HTTPS ポートです。また、API ポート（HTTP/HTTPS）がファイアウォールで開かれていることを確認します。
- デフォルトで、`trailblazerconfig` の CLI コマンドはアプライアンスで有効になっています。HTTPS ポートがファイアウォールで開かれていることを確認します。また、アプライアンスにアクセスするために指定したホスト名を DNS サーバーが解決できることを確認してください。

  `trailblazerconfig` の CLI コマンドが無効になっている場合、CLI を使用して `trailblazerconfig > enable` コマンドを実行することにより、以下の問題を回避できます。

  - 特定のブラウザで API ポートの複数の証明書を追加する必要がある。
  - スパムの隔離、セーフリスト、またはブロックリストのページを更新するときに、レガシー Web インターフェイスにリダイレクトされる。
  - 高度なマルウェア防御レポート ページのメトリック バーにデータが含まれない。

  詳細については、ユーザーガイドの「The trailblazerconfig Command」のセクションを参照してください。

（注） Web インターフェイスにアクセスできない場合は、アプライアンスを再起動するか、ブラウザのキャッシュをクリアします。問題が解決しない場合は、シスコカスタマーサポートにご連絡ください。

アップグレード後の要件

スパム通知 URL の変更

Cisco Secure Email and Web Manager 14.2 へのアップグレード後、保存されているスパム通知 URL を使用してもログインできない場合は、スパム通知メールに記載されている新しい URL を使用してください。

このリリースでサポートされているハードウェア

サポート対象ハードウェア:

- M190
- M195
- M390
- M395
- M690
- M695

サポート対象 VM:

- M100V
- M300V
- M600V

既知および修正済みの問題

シスコのバグ検索ツールを使用して、このリリースの既知および修正済みの不具合に関する情報を検索します。

- バグ検索ツールの要件（15 ページ）
- 既知および修正済みの問題のリスト（16 ページ）
- 既知および解決済みの問題に関する情報の検索（16 ページ）

バグ検索ツールの要件

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

既知および修正済みの問題のリスト

既知の問題	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=14.2.0&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=14.2.0&sb=fr&sts=fd&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager

既知および解決済みの問題に関する情報の検索

シスコのバグ検索ツールを使用して、既知および解決済みの不具合に関する最新情報を検索します。

はじめる前に

シスコ アカウントを持っていない場合は、登録します。
https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui に移動します。

手順

ステップ 1 https://bst.cloudapps.cisco.com/bugsearch/ に移動します。

ステップ 2 シスコ アカウントのクレデンシャルでログインします。

ステップ 3 [リストから選択(Select from list)] > [セキュリティ(Security)] > [E メールセキュリティ(Email Security)] > [Cisco E メールセキュリティアプライアンス(Cisco Email Security Appliance)] の順にクリックし、[OK] をクリックします。

ステップ 4 [リリース(Releases)] フィールドに、リリースのバージョン(14.2.0 など)を入力します。

ステップ 5 要件に応じて、次のいずれかを実行します。

- 解決済みの問題のリストを表示するには、[バグの表示(Show Bugs)] ドロップダウンから、[これらのリリースで修正済み(Fixed in these Releases)] を選択します。
- 既知の問題のリストを表示するには、[バグの表示(Show Bugs)] ドロップダウンから [これらのリリースに影響(Affecting these Releases)] を選択し、[ステータス(Status)] ドロップダウンから [開く(Open)] を選択します。

(注) ご不明な点がある場合は、ツールの右上にある [ヘルプ(Help)] または [フィードバック(Feedback)] リンクをクリックしてください。また、インタラクティブなツアーもあります。これを表示するには、[検索(search)] フィールドの上のオレンジ色のバーにあるリンクをクリックします。

関連資料

次の表の主要なドキュメントに加えて、ナレッジベースおよびシスコサポートコミュニティを含む他のリソースに関する情報は、オンラインヘルプおよびユーザーガイド PDF の「More Information」の章に記載されています。

Cisco Secure 製品	参照先
Cisco Secure Email and Web Manager アプライアンス	http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Secure Web Appliance	http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Secure E メール セキュリティ アプライアンス	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html
コンテンツ セキュリティ製品用コマンドライン リファレンス ガイド	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-command-reference-list.html
Cisco Email Encryption	http://www.cisco.com/c/ja_jp/support/security/email-encryption/tsd-products-support-series-home.html

サービスとサポート

（注） 仮想アプライアンスのサポートを受けるには、仮想ライセンス番号（VLN）をご用意の上 Cisco TAC に連絡してください。

Cisco TAC：https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html

従来の IronPort のサポートサイト：http://www.cisco.com/web/services/acquisitions/ironport.html

重大ではない問題の場合は、アプライアンスからカスタマー サポートにアクセスすることもできます。手順については、ユーザーガイドまたはオンライン ヘルプを参照してください。

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

このマニュアルは、「関連資料」の項に記載されているマニュアルと併せてご利用ください。