AsyncOS 13.5.1 for Cisco Email Security Appliances リリースノート

発行日:2020 年 6 月 2 日
改訂日:2021 年 9 月 17 日

目次

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

AsyncOS 13.5.1 の新機能

機能	説明
メールボックス内のメッセージの検索と修復	アプライアンスを設定し、検索および修復機能を使用して、手動でメッセージを修復できるようになりました。この機能により、メッセージ トラッキング フィルタを使用してメッセージを検索し、メッセージに修復アクションを適用できるようになります。 詳細は、ユーザーガイドの「メールボックスでのメッセージの修復」の章を参照してください。
Cisco Success Network を使用した Cisco E メール セキュリティ ゲートウェイのユーザエクスペリエンスの向上	Cisco Success Network（CSN）機能を使用して、アプライアンスや機能の使用状況の詳細をシスコに送信できます。これらの詳細情報は、アプライアンスのバージョン、およびアプライアンスでアクティブになっているが有効になっていない機能を識別するために使用されます。 アプライアンスや機能の使用状況の詳細をシスコに送信する機能により、組織は次のことを行うことができます。 • 収集されたテレメトリデータの分析を実行し、デジタルキャンペーンを使用してユーザに推奨事項を提示することによって、ユーザネットワークでの製品の有効性を向上させます。 • Cisco E メール セキュリティ ゲートウェイの使用により、ユーザエクスペリエンスが向上します。 詳細については、ユーザーガイドまたはオンラインヘルプの「Cisco Threat Response との統合（Integrating with Cisco Threat Response）」の章を参照してください。

新しい Cisco Talos 電子メールステータスポータル	新しい Cisco Talos 電子メールステータスポータルは、従来のシスコ電子メール送信およびトラッキングポータルに変わるものです。 Cisco Talos 電子メールステータスポータルは、シスコユーザーからの電子メール送信のステータスをモニターリングするための Web ベースツールです。 **(注)** 従来のポータルのユーザーは、新しいポータルで以前の送信に引き続きアクセスできます。 **(注)** 新しいポータルでは電子メールゲートウェイによって誤って識別された可能性のあるスパムやフィッシング、ハム、マーケティングまたは非マーケティング電子メールのサンプル送信することはできません。電子メールサンプルの送信方法の詳細については、次の URL にある Cisco Talos 電子メールステータスポータルのヘルプページを参照してください。 https://talosintelligence.com/tickets/email_submissions/help 詳細については、ユーザーガイドまたはオンラインヘルプの「スパムおよびグレイメールの管理(Managing Spam and Graymail)」の章を参照してください。
プロキシサーバーを使用して Cisco Threat Response にアプライアンスを接続する機能	プロキシサーバを使用してアプライアンスを Cisco Threat Response に接続できるようになりました。 次のいずれかの方法でプロキシ サーバを設定できます。 • Web インターフェイスの [セキュリティサービス(Security Services)] > [サービスアップデート(Service Updates)] ページ。 • CLI の *updateconfig* > *setup* サブコマンド。 詳細については、ユーザーガイドの「System Administration」の章を参照してください。
新しい Web インターフェイスの暗色モードでの利用	暗色モードは反転カラースキームであり、暗い色の背景上で明るい色のタイポグラフィ、UI 要素、アイコンが使用されます。 アプライアンスの新しい Web インターフェイスを暗色モードで利用できるようになりました。 暗色モードに切り替えるには、新しい Web インターフェイスの右上隅にあるユーザーアイコンをクリックし、[暗色表示テーマ(Dusk Theme)] を選択します。 詳細については、ユーザーガイドの「Setup and Installation」の章を参照してください。

Cisco Threat Response サーバーでの APJC データセンターのサポート	アプライアンスを Cisco Threat Response に接続するための Cisco Threat Response サーバーとして、APJC データセンターの「APJC (*api.apj.sse.itd.cisco.com*)」を選択できるようになりました。 詳細は、ユーザーガイドまたはオンラインヘルプの「Integrating with Cisco Threat Response」の章、および『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。
How-To ウィジェットで使用可能な新しいウォークスルー	How-To は、アプライアンスで複雑なタスクを実行するためにウォークスルー形式でユーザにアプリ内アシスタンスを提供する、コンテキスト型ウィジェットです。 このリリースでは、次のウォークスルーが追加されています。 • 財務データの偶発的な漏洩の防止方法 • フィッシングについての啓蒙活動メッセージでのエンジンスキャンの省略方法 **（注）** ウォークスルーのリストは更新可能なクラウドです。ハウツー ウィジェットの更新バージョンとポップアップウィンドウを表示するには、必ずブラウザのキャッシュをクリアしてください。 詳細は、ユーザーガイドまたはオンラインヘルプの「Accessing the Appliance」の章と『CLI Reference Guide for AsyncOS for Cisco Email Security Appliances』を参照してください。 各リリースでサポートされているウォークスルーの完全なリストを表示するには、『Walkthroughs Supported in AsyncOS for Cisco Email Security Appliances』を参照してください。

AsyncOS 13.5.0 の新機能

機能	説明
Cisco E メール セキュリティ ゲートウェイと Cisco Advanced Phishing Protection クラウドサービスの統合	Cisco E メール セキュリティ ゲートウェイ上の Cisco Advanced Phishing Protection エンジンは、組織に送信された過去の電子メールトラフィックに基づいて、正当なすべての送信者の固有の動作を確認します。Cisco Advanced Phishing Protection のクラウドサービス インターフェイスは、悪意のある可能性があるメッセージを正常なメッセージと区別するためにリスク分析を実行します。 Cisco Advanced Phishing Protection クラウドサービスは、電子メールゲートウェイを組織への着信メッセージのメタデータのコピーを受信するためのセンサーエンジンとして使用します。このセンサーエンジンが、電子メールゲートウェイからのメッセージヘッダーなどのメタデータを収集し、それらを分析するために Cisco Advanced Phishing Protection クラウドサービスへ中継します。分析後に、悪意のある可能性があるメッセージは、Cisco Advanced Phishing Protection クラウドサービス上の事前に設定されたポリシーに基づいて、受信者のメールボックスから自動的に修復されます。 Cisco E メール セキュリティ ゲートウェイをセンサーエンジンとして使用できると、組織が次のことを行うときに役立ちます。 • 受信者のメールボックスからのメッセージヘッダーで確認された脅威を特定し、調査し、修復する。 • 組織内の複数の電子メールゲートウェイからメッセージのメタデータのレポートデータを表示する。 • 悪意のあるメッセージに関して、エンドユーザにリアルタイムのアラートを送信する。 詳細については、ユーザーガイドの「Cisco E メール セキュリティ ゲートウェイと Cisco 高度なフィッシング防御の統合（Integrating the Cisco Email Security Gateway with Cisco Advanced Phishing Protection）」の章を参照してください。
サービスログを使用したフィッシング検知有効性の向上	サービスログ機能は、Cisco E メール セキュリティ アプライアンス データ シートに基づいて個人データを収集するために使用されます。 サービスログは、フィッシング検出を改善するために Cisco Talos クラウドサービスに送信されます。 詳細については、「アプライアンスでのサービスログの有効化（14 ページ）」を参照してください。

フィッシングに対する有効性の向上	Cisco E メール セキュリティ アプライアンスは、フィッシングをより迅速かつ効果的に行うため、IP レピュテーションと URL レピュテーションが改善されています。 詳細については、『User Guide for AsyncOS 13.5 for Cisco Email Security Appliance』を参照してください。

（注） HTTP プロキシサーバを設定している場合、IP レピュテーション/URL レピュテーションサービス、およびサービスログは、インターネットに直接接続して IP と URL のレピュテーションを取得します。これらのサービスにプロキシを使用する場合は、電子メールゲートウェイで HTTPS プロキシサーバを設定します。

（注） HTTPS プロキシサーバを設定している場合は、E メールゲートウェイから発信される HTTPS トラフィックを復号するようにプロキシサーバを設定しないでください。

（注） 電子メールゲートウェイおよび TLS 1.3 セキュアプロトコルを使用する Cisco IP レピュテーションサービスと URL レピュテーションサービスとサービスログ間の電子メールトラフィックを許可するために、ネットワークでアプリケーションレイヤ ファイアウォール ルール（たとえば、サーバー名指定（SNI）のマッチング）を使用しないようにしてください。

動作における変更

AsyncOS 13.5.1 の動作の変更

コンテンツスキャナの変更点	アプライアンスのコンテンツスキャナーは、メッセージのパスワードで保護された添付ファイル（.zip 形式）の最初のネストされたレベルでファイル名を抽出できるようになりました。
SSL 暗号設定の変更	@STRENGTH パラメータが、受信 SMTP、送信 SMTP、および GUI 接続のデフォルト SSL 暗号文字列に追加されました。 現在、アプライアンス（クライアントとして動作）からリモートで設定された MTA（サーバーとして動作）に送信されたすべての接続要求は、MTA が弱い暗号と古い TLS 方式のみをサポートしている場合は拒否されます。@STRENGTH パラメータは、暗号リストをソートし、リストの一番上に最も強力な暗号を表示します。暗号リストには、選択した TLS 方式に基づいて弱い暗号が含まれないようにされます。

アプライアンスの Sophos Anti-Virus 設定の変更	このリリース以前は、アプライアンスの Sophos Anti-Virus エンジンで、StrongPDF オプションがデフォルトで自動的に有効になりました。Sophos Anti-Virus エンジンは、StrongPDF オプションを使用して、EOF（End-of-File）がないなどの理由で「スキャン不能」として破損したクリーンな PDF ファイルを分類しました。 このリリースにアップグレードすると、StrongPDF オプションはデフォルトで無効になります。Sophos Anti-Virus エンジンは、EOF（End-of-File）の欠落などにより「クリーン」として破損したクリーン PDF ファイルを自動的に分類するようになりました。 CLIで *antivirusconfig* > *PDF* サブコマンドを使用して、アプライアンスの Sophos Anti-Virus エンジンで StrongPDF オプションを有効にすることができます。
ファイル レピュテーション クエリーのタイムアウトの変更	アプライアンスは、ファイル レピュテーション クエリ プロセス中の合計タイムアウト期間に 2 秒の追加バッファー時間を追加するようになりました。
アンダースコア（_）を含むドメイン名のサポート終了	Cisco E メール セキュリティ アプライアンスでは、電子メールアドレスのドメイン名部分にアンダースコア（_）を含むメッセージが処理されなくなります。
着信メッセージのメッセージ ID ヘッダーの変更	メッセージ ID ヘッダーを含まないすべての着信メッセージに対して、システム生成のメッセージ ID ヘッダーが追加されるようになりました。アプライアンスでメッセージが処理された後のメール配信時に、システムによって生成されたメッセージ ID ヘッダーがメッセージに追加されます。
ログインユーザー名の変更	今回のリリースまでは、数字のみで構成されるユーザー名ではアプライアンスにログインできませんでした。 このリリースにアップグレードすると、数字だけで構成されるユーザー名でアプライアンスにログインできるようになります。
DANE の検証変更内容	DANE が有効になっており、発信メッセージの SMTP ルートに追加されているドメインに対しては、DANE 検証がバイパスされるようになりました。
通知メールの変更	今回のリリースまでは、特定の受信者に通知メールを送信するコンテンツ フィルタ アクションを設定していた場合、元のメッセージのすべての受信者に対して、1 種類の通知メールが送信されていました。 このリリースにアップグレードすると、コンテンツ フィルタ アクションで定義された受信者にのみ通知メールが送信されるようになります。
RC4 暗号化アルゴリズムのサポート終了	RC4 暗号化アルゴリズムタイプがサポートされなくなります。暗号化プロファイルのエンベロープを設定する際、RC4 暗号化アルゴリズムのオプションを選択できなくなります。

SSL 設定の変更	SSL の設定に関する変更は、次のとおりです。 • SSLv2 および SSL v3 方式のサポートが終了しました。 • アプライアンスが FIPS モードの場合、TLS v1.0 方式はサポートされません。 • アプライアンスが非 FIPS モードの場合、TLS v1.0 方式はデフォルトで無効になります。 • TLS クライアントサービス（LDAP および Updater）に対しては、次の方法で TLS v1.0 方式を有効にできます。 – アプライアンスの Web インターフェイスの [システム管理（System Administration）] > [SSL の設定（SSL Configuration）] ページ。ユーザーガイドの「System Administration」の項を参照してください。 – CLI の *sslconfig* コマンド。『CLI Reference Guide for AsyncOS 13.5.1 for Cisco Email Security Appliances』を参照してください。 **（注）** TLS v1.0 が有効になっている非 FIPS モードの下位の AsyncOS バージョン（たとえば、12.x）から AsyncOS 13.5.1 以降にアップグレードすると、TLS v1.0 がデフォルトで無効になります。アップグレード後にアプライアンスで TLS v1.0 方式を有効にする必要があります。
アプライアンスおよびカスタム CA 証明書の有効期限を通知する新しいアラート	アプライアンス証明書やカスタム CA 証明書が有効期限に近づくか、期限切れになると、クリティカルまたは警告の重大度を付けたシステムアラートが送られるようになりました。

AsyncOS 13.5.0 の動作の変更

パスフレーズ設定への変更	ログインパスフレーズを自動的に生成するオプションが削除されます。選択したパスフレーズをここで手動で入力する必要があります。
データベースサイズの制限に達したときのアラートの変更	このリリースにアップグレードした後、メッセージの詳細と過去のファイルの詳細を保存するデータベース内のメッセージが 2GB のサイズに達するとアラートが送信されます。 データベースを分析し、修正措置を実施するには、シスコのカスタマーサポートにご連絡ください。

スパム陽性メッセージのアウトブレイクフィルタの変更	このリリースより前では、スパム陽性のメッセージがアウトブレイクフィルタによってアウトブレイク陽性として識別されると、そのメッセージはアウトブレイク隔離エリアに送信されていました。 このリリースにアップグレードした後は、スパム陽性のメッセージがアウトブレイクフィルタによってアウトブレイク陽性として識別されても、そのメッセージはアウトブレイク隔離エリアに送信されません。
短縮 URL 展開の変更	このリリースより前は、アプライアンスで *websecurityadvancedconfig* CLI コマンドを使用して、短縮 URL の展開を無効にできました。 このリリースにアップグレード後は、すべての短縮 URL が展開されます。短縮 URL の展開を無効にするオプションはありません。

アップグレードの方法

リリース 13.5.1-277 へのアップグレード - GD（一般導入）

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

リリース 13.5.1-277 へは、次のバージョンからアップグレードできます。

- 12.0.0-419
- 12.1.0-089
- 12.5.0-066
- 12.5.1-037
- 12.5.2-011
- 13.0.0-392
- 13.0.0-403
- 13.0.1-030
- 13.5.0-263
- 13.5.1-177
- 13.5.1-269
- 13.5.1-273

リリース 13.5.1-273 へのアップグレード - LD（限定的な導入）

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

リリース 13.5.1-273 へは、次のバージョンからアップグレードできます。

- 12.0.0-419
- 12.1.0-089
- 12.5.0-066
- 12.5.1-037
- 12.5.2-011
- 13.0.0-392
- 13.0.0-403
- 13.0.1-030
- 13.5.0-263
- 13.5.1-177
- 13.5.1-269

リリース 13.5.0-263 へのアップグレード - LD（限定的な導入）

リリース 13.5.0-263 へは、次のバージョンからアップグレードできます。

- 12.0.0-419
- 12.1.0-089
- 12.1.0-091
- 12.5.0-059
- 12.5.0-066
- 12.5.1-037
- 13.0.0-314
- 13.0.0-375
- 13.0.0-392
- 13.5.0-236

インストールおよびアップグレードに関する注意事項

このセクションに記載されているインストールとアップグレードの影響を把握および検討してください。

Web インターフェイスまたは CLI（コマンド ライン インターフェイス）から AsyncOS をアップグレードすると、設定は /configuration/upgrade ディレクトリ内のファイルに保存されます。FTP クライアントを使用して、アップグレード ディレクトリにアクセスできます。各設定ファイル名にはバージョン番号が付加され、設定ファイル内のパスワードは人間が判読できないようにマスクされます。

管理者権限を持つユーザーとしてログインして、アップグレードする必要があります。また、アップグレード後にアプライアンスを再起動する必要があります。

このリリースでサポートされているハードウェア

- すべての仮想アプライアンスモデル
- 次のハードウェア モデル
  - C190
  - C195
  - C390
  - C395
  - C690
  - C695
  - C695F

（注） （C695 および C695F モデルの場合のみ）：アプライアンスをアップグレードまたは再起動する前に、接続されているファイバ スイッチ ポート インターフェイスで LLDP を無効にします。これにより、FCoE トラフィックが自動的に無効になります。

アプライアンスがサポートされているかどうかを確認し、現在互換性がない場合にその状況を解決するには、http://www.cisco.com/c/en/us/support/docs/field-notices/638/fn63931.html を参照してください。

このリリースでは、次のハードウェアはサポートされていません。

- C160、C360、C660、および X1060
- C170、C370、C370D、C670、および X1070
- C380 および C680 アプライアンス

仮想アプライアンスの展開またはアップグレード

仮想アプライアンスを展開またはアップグレードする場合は、『Cisco コンテンツセキュリティ仮想アプライアンス インストール ガイド』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/email-security-appliance/products-installation-guides-list.html から入手できます。

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の展開またはアップグレード (12 ページ)」で説明されているマニュアルを使用して、この AsyncOS リリースで仮想アプライアンスをセットアップします。

ステップ 2 ハードウェア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ハードウェアアプライアンスから設定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設定ファイルをロードします。

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。

仮想アプライアンスのテクニカル サポートの取得

仮想アプライアンスのテクニカル サポートを受けるための要件は、http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/products-installation-guides-list.html にある『Cisco コンテンツセキュリティ仮想アプライアンス インストール ガイド』に記載されています。

以下のサービスとサポート (20 ページ)も参照してください。

仮想アプライアンスからの Cisco Registered Envelope Service 管理者のプロビジョニングとアクティブ化

仮想アプライアンスのプロビジョニングに必要な情報については、Cisco TAC にお問い合わせください。

アップグレード前の注意事項

アップグレードする前に、次の事項を確認してください。

Cisco Talos サービスにアクセスするためのファイアウォール設定

電子メールゲートウェイを Cisco Talos サービスに接続するには、次のホスト名または IP アドレス用にファイアウォール上で HTTPS（Out）443 ポートを開く必要があります（以下の表を参照）。

（注） HTTPS アップデータプロキシ設定は、Cisco Talos サービスへの接続に使用されます。

ホスト名	IPv4	IPv6
grpc.talos.cisco.com	146.112.62.0/24	2a04:e4c7:ffff::/48
email-sender-ip-rep-grpc.talos.cisco.com	146.112.63.0/24	2a04:e4c7:fffe::/48
serviceconfig.talos.cisco.com	146.112.255.0/24	-
	146.112.59.0/24	-

詳細については、ユーザガイドの「Firewall」の章を参照してください。

Cisco Advanced Phishing Protection クラウドサービスにアクセスするためのファイアウォールの設定

電子メールゲートウェイを Cisco Advanced Phishing Protection クラウドサービスに接続するには、次のホスト名用にファイアウォール上で HTTPS（Out）443 ポートを開く必要があります。

- kinesis.us-west-2.amazonaws.com
- sensor-provisioner.ep.prod.agari.com
- houston.sensor.prod.agari.com

詳細については、ユーザガイドの「Firewall」の章を参照してください。

アプライアンスでのサービスログの有効化

サービスログは、Cisco E メール セキュリティ アプライアンス データ シートに基づいて個人データを収集するために使用されます。

サービスログは、フィッシング検出を改善するために Cisco Talos クラウドサービスに送信されます。

Cisco E メール セキュリティ ゲートウェイは、顧客の電子メールから限定された個人データを収集し、幅広く有用な脅威検出機能を提供します。この機能は、検出された脅威アクティビティを収集し、傾向を提示し、関連付けるための専用分析システムと組み合わせることができます。シスコでは、個人データを使用して、脅威の状況を分析し、悪意のある電子メールに脅威の分類ソリューションを提供し、スパム、ウイルス、ディレクトリ獲得攻撃などの新しい脅威から電子メールゲートウェイを保護するために、電子メールゲートウェイの機能を向上させています。

アップグレードプロセス中に、次のいずれかからアプライアンスのサービスログを有効にする方法を選択できます。

- Web インターフェイスの [システム管理（System Administration）] > [システムアップグレード（System Upgrade）] ページで、[サービスログ（Service Logs）] に [同意する（I Agree）] オプションを選択します。
- 「upgrade」CLI コマンドの「サービスログをデフォルトで有効にして続行しますか? [Y]（Do you agree to proceed with Service Logs being enabled by default? [y]）」に「Yes」と入力します。

詳細については、ユーザーガイドの「Improving Phishing Detection Efficacy using Service Logs」の章を参照してください。

クラスタレベルでのインテリジェント マルチスキャンとグレイメール設定のアップグレード

AsyncOS 13.5.1 にアップグレードする前に、インテリジェント マルチスキャンとグレイメールの設定が同じクラスタレベルに存在していることを確認します。クラスタレベルが異なっている場合は、アップグレード後にインテリジェント マルチスキャンとグレイメールの設定を確認する必要があります。

FIPS の準拠性

AsyncOS 13.5.1 リリースは、FIPS 準拠のリリースではありません。アプライアンスで FIPS モードを有効にしている場合は AsyncOS 13.5.1 にアップグレードする前に FIPS モードを無効にする必要があります。

AsyncOS の以前のバージョンへの復元

次の AsyncOS バージョンは、内部テストインターフェイスの脆弱性（http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa）の影響を受けます。

- 9.1.2-023
- 9.1.2-028
- 9.1.2-036
- 9.7.2-046
- 9.7.2-047

- 9.7-2-054
- 10.0.0-124
- 10.0.0-125

集中管理（クラスタ化されたアプライアンス）を使用した展開のアップグレード

クラスタに C160、C360、C660、X1060、C170、C370、C670、C380、C680、または X1070 ハードウェア アプライアンスが含まれている場合は、アップグレードの前に、これらのアプライアンスをクラスタから削除してください。

クラスタ内のすべてのマシンが同じバージョンの AsyncOS を実行している必要があり、x60、x70、および x80 ハードウェアをこのリリースにアップグレードすることはできません。必要に応じて、x60、x70、および x80 アプライアンス用に別のクラスタを作成してください。

直前のリリース以外のリリースからのアップグレード

このリリースの直前のリリース以外のメジャー（AsyncOS X.0）またはマイナー（AsyncOS X.x）リリースからアップグレードする場合は、現在のリリースとこのリリースの間にあるメジャー リリースとマイナー リリースのリリース ノートを確認する必要があります。

メンテナンス リリース（AsyncOS X.x.x）には、バグ修正のみが含まれています。

設定ファイル

通常、シスコは、以前のメジャーリリースに関して、設定ファイルの下位互換性をサポートしていません。マイナーリリースのサポートが提供されています。以前のバージョンの設定ファイルは以降のリリースで動作する可能性がありますが、ロードするために変更が必要になる場合があります。設定ファイルのサポートについて不明な点がある場合は、シスコカスタマーサポートでご確認ください。

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。これは既知の問題です。

障害 ID：CSCuz28415

このリリースへのアップグレード

はじめる前に

- ワークキュー内のすべてのメッセージをクリアします。ワークキューをクリアせずにアップグレードを実行することはできません。
- Known Issues（8 ページ）と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）を確認してください。
- 仮想アプライアンスをアップグレードする場合は、仮想アプライアンスのアップグレード（12 ページ）を参照してください。

手順

E メール セキュリティ アプライアンスをアップグレードするには、次の手順を実行します。

ステップ 1	アプライアンスから、XML 設定ファイルを保存します。
ステップ 2	セーフリスト/ブロックリスト機能を使用している場合は、アプライアンスからセーフリスト/ブロックリストデータベースをエクスポートします。
ステップ 3	すべてのリスナーを一時停止します。
ステップ 4	ワークキューが空になるまで待ちます。
ステップ 5	[システム管理(System Administration)] タブで、[システムアップグレード(System Upgrade)] ページを選択します。
ステップ 6	[利用可能なアップグレード(Available Upgrades)] ボタンをクリックします。ページが更新され、使用可能な AsyncOS アップグレード バージョンのリストが表示されます。
ステップ 7	[アップグレードの開始(Begin Upgrade)] ボタンをクリックすると、アップグレードが開始されます。表示される質問に答えます。
ステップ 8	アップグレードが完了したら、[今すぐリブート(Reboot Now)] ボタンをクリックしてアプライアンスを再起動します。
ステップ 9	すべてのリスナーを再開します。

次の作業

- アップグレード後、SSL の設定を確認し、使用する正しい GUI HTTPS、インバウンド SMTP、およびアウトバウンド SMTP 方式が選択されていることを確認します。[システム管理(System Administration)] > [SSL 構成(SSL Configuration)] ページを使用するか、CLI で `sslconfig` コマンドを使用します。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の「System Administration」の章を参照してください。
- 「パフォーマンスアドバイザリ(17 ページ)」を確認してください。
- SSH キーを変更した場合は、アップグレード後に Cisco E メールセキュリティアプライアンスと Cisco セキュリティ管理アプライアンス間の接続を再認証します。

アップグレード後の注意事項

AsyncOS 13.x へのアップグレード後のクラスタレベルでの DLP 設定の不整合

AsyncOS 13.x にアップグレードした後、アプライアンスがクラスタモードになっていて、DLP が設定されている場合、CLI を使用して `clustercheck` コマンドを実行すると、DLP 設定の不整合が表示されます。

この不整合を解決するには、クラスタ全体でクラスタ内の他のいずれかのマシンの DLP 設定を使用するように強制します。次の例に示すように、*clustercheck* コマンドで「`How do you want to resolve this inconsistency?`」というプロンプトを使用します。

```
(Cluster)> clustercheck
Checking DLP settings...
```

```
Inconsistency found!
DLP settings at Cluster test:
mail1.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
mail2.example.com was updated Wed Jan 04 05:52:57 2017 GMT by 'admin' on mail2.example.com
How do you want to resolve this inconsistency?
1. Force the entire cluster to use the mail1.example.com version.
2. Force the entire cluster to use the mail2.example.com version.
3. Ignore.
[3]>
```

インテリジェント マルチスキャンおよびグレイメールのグローバル設定の変更

AsyncOS 13.5.1 にアップグレードした後のインテリジェント マルチスキャン（IMS）およびグレイメールのグローバル設定の変更点は次のとおりです。

- IMS およびグレイメールのグローバル設定が異なるクラスタ レベルで設定されている場合、アプライアンスはグローバル設定を最も低い設定レベルにコピーします。たとえば、クラスタ レベルで IMS を設定し、マシン レベルでグレイメールを設定すると、アプライアンスは IMS グローバル設定をマシン レベルにコピーします。
- スキャンメッセージの最大メッセージサイズとタイムアウト値が異なる場合、アプライアンスは [最大タイムアウト（maximum timeout）] および [最大メッセージ（maximum message size）] の値を使用して、IMS およびグレイメールのグローバル設定を行います。たとえば、IMS およびグレイメールの最大メッセージサイズの値がそれぞれ 1M と 2M である場合、アプライアンスは IMS とグレイメールの両方の最大メッセージサイズ値として 2M を使用します。

パフォーマンスアドバイザリ

アウトブレイクフィルタ

アウトブレイクフィルタは、コンテキスト適応スキャンエンジンを使用してメッセージの脅威レベルを判定し、アダプティブルールとアウトブレイクルールの組み合わせに基づいてメッセージにスコアを付けます。一部の設定では、中程度のパフォーマンス低下が発生する可能性があります。

IronPort スパム隔離

C シリーズのアプライアンスに対して IronPort スパム隔離オンボックスを有効にすると、公称水準の負荷がかかっているアプライアンスでは、システムスループットにわずかな低下が生じます。ピークスループット付近またはピークスループットで実行されているアプライアンスの場合、アクティブな隔離からの追加の負荷によって、スループットが 10 ～ 20% 低下する可能性があります。システムのキャパシティがいっぱいか、いっぱいに近いときに IronPort スパム隔離を使用する場合は、規模が大きい C シリーズ アプライアンスまたは M シリーズ アプライアンスへの移行を検討してください。

スパム対策ポリシーをスパムのドロップから隔離に変更する場合（オンボックスまたはオフボックス）、ウイルスおよびコンテンツ セキュリティのために追加のスパムメッセージをスキャンする必要があるため、システムの負荷が増大します。インストールのサイジングを適切に行う際にサポートが必要な場合は、認定サポートプロバイダにお問い合わせください。

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

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

13.5.1 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=13.5.1&sb=afr&sts=open&svr=3nH&bt=custV
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=13.5.1&sb=fr&sts=fd&svr=3nH&bt=custV

13.5.0 の既知および修正済みの問題

既知の問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=13.5.0&sb=afr&sts=open&svr=3nH&bt=custV
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=282509130&rls=13.5.0&sb=fr&sts=fd&svr=3nH&bt=custV

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://tools.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(Release)] フィールドに、リリースのバージョン(たとえば、13.5.1)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。

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)] フィールドの上にある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

マニュアルの内容 (Cisco Content Security 製品)	参照先
ハードウェアおよび仮想アプライアンス	この表で該当する製品を参照してください。
Cisco コンテンツ セキュリティ管理	http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Cisco Web セキュリティ	http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco E メール セキュリティ	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco コンテンツ セキュリティ アプライアンス用 CLI 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 IronPort 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：http://www.cisco.com/en/US/support/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 ガイドまたはオンライン ヘルプを参照してください。