AsyncOS 14.3 for Cisco Secure Email Cloud Gateway リリースノート

発行日:2022 年 10 月 11 日
改訂日:2023 年 3 月 16 日

目次

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

機能	説明
Secure Email Cloud Gateway と脅威防御の統合	Threat Defense Connector クライアントは、Secure Email Cloud Gateway を Secure Email Threat Defense に接続して、高度なフィッシングとスプーフィングのメッセージをスキャンします。 Threat Defense コネクタを設定すると、Secure Email Cloud Gateway は実際のメッセージのコピーを添付ファイルとして Threat Defense ポータルのメッセージ受信アドレスに送信します。メッセージはユーザーの受信トレイに配信され、Threat Defense ポータルで高度なスキャンが完了します。 次のいずれかの方法で、脅威防御コネクタを有効にできます。 • Web インターフェイスの [セキュリティサービス（Security Services）] > [Threat Defense Connector] ページから。 • CLI での `Threatdefenseconfig` コマンドの使用。 詳細については、このリリースに関連するユーザーガイド、または CLI リファレンスガイドの「Secure Email Cloud Gateway と脅威防御の統合」の章を参照してください。
Cisco Secure Email Phishing Defense のサポート終了	このリリース以降、2022 年 12 月 14 日の時点で、Cisco Secure Email Phishing Defense（旧称 Cisco Advanced Phishing Protection）機能が Secure Email Cloud Gateway 14.3 以降でサポートされなくなります。詳細については、こちらをクリックしてください。支援が必要な場合は、Cisco Technical Assistance にお問い合わせください。 **（注）** 上記のステートメントは、有効なライセンスを所有し、Cisco Secure Email Phishing Defense 機能をアクティブに使用している既存のユーザーには適用されません。
AMP の設定のカスタムユーザーロール	管理者は、AMP の設定、AMP レポート、ファイル分析隔離、およびメッセージトラッキングへのアクセスを提供するカスタムユーザーロールを定義できます。管理者は、このカスタムユーザーロールを委任された管理者に割り当てることができます。 管理者は、次の方法で AMP 設定のカスタムユーザーロールを定義できます。 • [システム管理者（System Administrator）] > [ユーザーロール（System Administrator）] > [ユーザーロールの追加（Add User Role）] に移動し、Web インターフェイスの [AMP の設定（AMP Configurations）] フィールドで [アクセスなし（No access）] または [フルアクセス（Full access）] を選択します。 • CLI で `userconfig` > `ROLE` サブコマンドを使用し、AMP の設定ステートメントに適切な入力を提供します。 詳細については、このリリースに関連するユーザーガイド、または CLI リファレンスガイドの「管理タスクの分散」の章を参照してください。

統合イベントログの機能拡張	統合イベントログに 2 つの新しいフィールドが追加され、電子メールゲートウェイをセキュリティ情報およびイベント管理（SIEM）アプリケーションと統合するときに、追加のデータを含めるために使用できます。 • カスタムログエントリ • カスタムログヘッダー 2 つのフィールドを使用して、統合イベントログにカスタムヘッダー、カスタムログエントリ、またはその両方を追加できます。 **（注）** 統合イベントログに追加できるカスタムログヘッダーは 25 個だけです。 電子メールゲートウェイに次のように 2 つのフィールドを設定できます。 • [カスタムログエントリ（Custom Log Entry）] フィールド：Web インターフェイスで [CEF ログエントリの追加コンテンツ フィルタ アクション（Add CEF Log Entry Content Filter Action）]（受信または送信コンテンツフィルタのいずれか該当する方）を使用するか、CLI の [policyconfig] > [受信メール ポリシー（incoming mail policies）] または [送信メールポリシー（outgoing mail policies）] > [フィルター（filters）] > [新規（new）] > [追加（add）] > [アクション（Action）] サブコマンドで [CEF ログエントリの追加（Add CEF Log Entry）] コンテンツ フィルタ アクションを入力します。 **（注）** 対応するメッセージ フィルタ アクション `cef-log-entry` が使用されます。 • カスタム ログ ヘッダー フィールド：Web インターフェイスの [ログサブスクリプション（Log Subscriptions）] > [グローバル設定（Global Settings）] ページの CEF ヘッダーオプション、または CLI の `logconfig` > `ceflogheaders` サブコマンドを使用します。 [選択したログフィールド（Selected Log Fields）] にある [カスタムログエントリ（Custom Log Entries）] または [カスタムログヘッダー]（いずれか該当する方）を使用して [統合イベントログ（Consolidated Event Logs）] ログサブスクリプションを設定すると、CEF ログエントリが [統合イベントログ（Consolidated Event Logs）] に表示されます。 詳細については、このリリースに関連するユーザーガイド、または CLI リファレンスガイドの「コンテンツフィルタ」および「ロギング」の章を参照してください。

パスワードで保護された添付ファイルを開くためのユーザー定義のパスフレーズのみを使用	このリリース以降、メールゲートウェイで作成されたユーザー定義のパスフレーズのみを使用して、受信および送信メッセージでパスワードで保護された添付ファイルを開くことを選択できます。 この機能は、次のいずれかの方法で設定できます。 • Web インターフェイスの [セキュリティサービス(Security Services)] > [スキャン動作(Scan Behavior)] > [グローバル設定の編集(Edit Global Settings)] ページで、[ユーザー定義のパスワードのみを適用(Apply User-defined Passwords Only)] チェックボックスを使用します。 • 「ユーザー定義のパスワードのみを適用しますか? y/n」ステートメントは、CLI の `scanconfig` > `protectedattachmentconfig` サブコマンドの下にあります。 詳細については、次の資料を参照してください。 • このリリースに関連するユーザーガイドの「メッセージフィルタを使用した電子メールポリシーの適用」章の「スキャン動作の設定」セクション。 • このリリースに関連する CLI リファレンスガイドの「コマンド: 参考例」章の「例:パスワードで保護された添付ファイルを開くためのユーザー定義のパスフレーズのみを使用」セクション。

動作における変更

メッセージ追跡:修復アクションの変更	このリリース以前:[メッセージトラッキング(Message Tracking)] > [修復(Remediate)] > [修復アクションの確認(Confirm Remediation Action)] ダイアログボックスでは、[修復バッチ名(Remediation Batch Name)] および [説明(Description)] フィールドに、小文字と大文字のアルファベットおよび 0 ～ 9 までの数字に加えて任意の特殊文字を入力できました。 このリリース以降:[メッセージトラッキング(Message Tracking)] > [修復(Remediate)] > [修復アクションの確認(Confirm Remediation Action)] ダイアログボックスでは、[修復バッチ名(Remediation Batch Name)] および [説明(Description)] フィールドに入力できるのは、小文字と大文字のアルファベット、0 ～ 9 までの数字、および「_」「-」のみです。
監査ログ用に選択されたデフォルトのログレベルの変更	このリリース以前:Web インターフェイスまたは CLI を使用して「監査ログ」ログサブスクリプションを作成すると、デフォルトのログレベルとして「情報」オプションが選択されていました。 このリリース以降:Web インターフェイスまたは CLI を使用して「監査ログ」ログサブスクリプションを作成すると、デフォルトのログレベルとして「デバッグ」オプションが選択されます。必要に応じて、ログレベルのオプションを変更できます。

コンテンツスキャナ：最大ファイルサイズのスキャン制限の変更	このリリース以前：電子メールゲートウェイのコンテンツスキャナは、添付ファイルから抽出されたテキストのサイズが設定された最大ファイルサイズのスキャン制限を超過している場合でも、メッセージの添付ファイルのテキストコンテンツをスキャンしていました。 このリリース以降：コンテンツスキャナは、設定された最大ファイルサイズのスキャン制限に基づいて、メッセージの添付ファイルの抽出されたテキストコンテンツのみをスキャンします。設定された最大ファイルサイズのスキャン制限を超過している残りのテキストコンテンツは、切り捨てられます。 **例**：最大ファイルサイズ制限を 5 MB に設定し、メッセージの添付ファイルから抽出されたテキストコンテンツが 5 MB を超えているとします（たとえば「8 MB」の場合）。コンテンツスキャナはファイルサイズ 5 MB のテキストコンテンツのみをスキャンし、残りのファイルサイズ 3 MB は切り捨てられます。

AsyncOS 14.3.0 リリースへのアップグレード

AsyncOS 14.3.0-032 更新リリースへのアップグレード

次のバージョンから、リリース 14.3.0-032 にアップグレードすることができます。

- 14.0.0-698
- 14.0.1-033
- 14.0.1-305
- 14.0.2-020
- 14.0.3-015
- 14.2.0-616
- 14.2.0-620
- 14.2.1-015
- 14.2.1-020
- 14.3.0-020
- 14.3.0-023

AsyncOS 14.3.0-023 リリースへのアップグレード

リリース 14.3.0-023 へは、次のバージョンからアップグレードできます。

- 13.5.1-277
- 13.7.0-093
- 14.0.0-698
- 14.0.1-033
- 14.0.2-020
- 14.0.2-606
- 14.2.0-616
- 14.2.0-620
- 14.3.0-002
- 14.3.0-017

このリリースでサポートされる VM

このリリースでは、次の VM がサポートされています。

- C100V
- C300V
- C600V

アップグレード後の注意事項

外部脅威フィード パッケージ バージョンの不適切な表示

このリリースにアップグレードした後、電子メールゲートウェイに最新の外部脅威フィード（ETF）パッケージが含まれている場合、システムは Web インターフェイスおよび CLI で ETF パッケージバージョンを実際の ETF パッケージバージョン「2.0.0-005」ではなくデフォルトの「1.0.0-0000001」として表示します。この問題は表示のみに影響し、機能への影響はありません。この問題は今後のリリースで解決される予定です。

不具合 ID：CSCwd49783。

（注） CLI で `threatfeedstatus` コマンドを使用すると、ETF エンジンの現在のバージョンを表示できます。詳細については、このリリースに関連する『CLI Reference Guide』を参照してください。

IP レピュテーションサービスのステータスのモニタリング

アップグレード後、IP レピュテーションのデバッグログに IP アドレス 172.0.0.2 が表示される場合があります。

IP アドレス 172.0.0.2 は、主に IP レピュテーション クラウド サービスの可用性を確認するために使用されます。この IP アドレスは、IP レピュテーション クラウド サービスと電子メールゲートウェイの接続を確認するために内部的に使用されます。IP アドレスは、送受信されるメッセージやユーザーネットワークとは関係ありません。

DLP サービスステータスチェック

このリリースにアップグレードした後、DLP サービスで問題が発生する可能性があります。

ソリューション：CLI で `diagnostic` > `services` > `DLP` > `status` サブコマンドを使用して、電子メールゲートウェイの DLP サービスのステータスを確認します。DLP サービスが実行されていない場合は、既知の問題リストにある CSCvy08110 の不具合の「回避策」セクションを参照してください。既知の問題を表示する方法の詳細については、既知および修正済みの問題のリスト（9 ページ）を参照してください。

電子メールゲートウェイでのパスワードで保護された添付ファイルのスキャン

パスワード保護された添付ファイルをスキャンするように電子メールゲートウェイのコンテンツスキャナを設定する場合、電子メールトラフィックにパスワード保護された添付ファイルが高い割合で含まれていると、パフォーマンスに影響を与える可能性があります。

(スマートライセンスのユーザーのみ)電子メールゲートウェイを Cisco Talos サービスに接続できない

電子メールゲートウェイがスマートライセンスモードで、システム時刻が GMT よりも遅い場合、電子メールゲートウェイで Cisco Talos サービスへの接続に関する問題が発生する可能性があります。

解決策:時刻設定で NTP サーバーを使用するように電子メールゲートウェイを設定していることを確認します。

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、電子メールゲートウェイ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は、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。次のプロンプトを使用します。「`この不整合をどのように解決しますか？(How do you want to resolve this inconsistency?)`」。次の例に示すように、`clustercheck` コマンドを入力します。

```
(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 14.0 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構成されている場合、電子メールゲートウェイ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、電子メールゲートウェイは IMS の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、電子メールゲートウェイは最大タイムアウトおよび最大メッセージサイズの値を使用して、IMS と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電子メールゲートウェイの場合、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ー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（9 ページ）
- 既知および修正済みの問題のリスト（9 ページ）
- 既知および解決済みの問題に関する情報の検索（10 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?pf=prdNm&prdNam=Cisco%20IronPort%20Email%20Security%20Appliance20Software&kw=*&bt=custV&sb=afr&svr=3nH&rls=14.3.0
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch?pf=prdNm&prdNam=Cisco%20IronPort%20Email%20Security%20Appliance%20Software&kw=*&bt=custV&sb=fr&svr=3nH&rls=14.3.0-032

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、14.3)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 Secure Email and Web Manager	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 Secure Email ゲートウェイ	http://www.cisco.com/c/ja_jp/support/security/email-security-appliance/tsd-products-support-series-home.html
Cisco Secure Email クラウドゲートウェイ	https://www.cisco.com/c/en/us/support/security/cloud-email-security/products-user-guide-list.html

マニュアルの内容 （Cisco Content Security 製品）	参照先
Cisco Secure Email Gateway 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、電子メールゲートウェイ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。