AsyncOS 13.5 for Cisco Content Security Management Appliances リリースノート

発行日:2020 年 1 月 13 日
改訂日:2024 年 1 月 25 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
新しいハードウェアモデルのサポート	シスコのコンテンツ セキュリティ管理アプライアンス向け AsyncOS 13.5 リリースでは、次のハードウェア モデルをサポートしています。 • M195 • M395 • M695 詳細については、https://www.cisco.com/c/ja_jp/products/collateral/security/content-security-management-appliance/datasheet_C78-721194.html を参照してください。
Cisco Threat Response で Web レポートモジュールを設定する機能	Cisco Threat Response で Web レポートモジュールを設定できるようになりました。 Cisco Threat Response で、[設定(Settings)] > [統合モジュール(Integration Modules)] > [モジュールの設定(Configure Modules)] > [SMA Web - シスコのコンテンツセキュリティ管理アプライアンス - Web(SMA Web - Cisco Content Security Management Appliance - Web)] に移動して、Web レポートモジュールを設定します。 詳細については、https://visibility.amp.cisco.com/を参照してください。
ケースブックを使用した脅威分析の実行	Cisco コンテンツ セキュリティ管理アプライアンスに、ケースブックとピボットメニューのウィジェットが追加されました。 (注) Microsoft Internet Explorer ブラウザを使用してアプライアンスにアクセスしている場合、[ケースブック(Casebook)] ウィジェットを使用することはできません。 [ケースブック(Casebook)] ウィジェットと [ピボット メニュー(Pivot Menu)] ウィジェットを使用して、アプライアンスで次のアクションを実行できます。 • 観測対象をケースブックに追加し、脅威分析の調査を実行します。 • 新しいケース、既存のケース、または Cisco Threat Response ポータルに登録されているその他のデバイス(エンドポイント向け AMP、Cisco Umbrella、Cisco Talos Intelligence など)の監視対象をピボットし、脅威分析のために調査します。 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「Integrating with Cisco Threat Response」の章を参照してください。

Cisco Threat Response ポータルでアプライアンスを登録するときに Cisco Threat Response サーバを選択する機能	アプライアンスを Cisco Threat Response ポータルに登録するときに、Cisco Threat Response ポータルにアプライアンスを接続するための Cisco Threat Response サーバを選択できるようになりました。 このリリースでサポートされている Cisco Threat Response サーバは次のとおりです。 • AMERICAS (api-sse.cisco.com) • EUROPE (api.eu.sse.itd.cisco.com) 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「Integrating with Cisco Threat Response」の章を参照してください。
お気に入りレポートの管理	カスタム レポート ページを作成するには、アプライアンスの新しい Web インターフェイスにある既存のすべての電子メール セキュリティ レポートからチャート(グラフ)とテーブルを構成します。 詳細については、ユーザガイドまたはオンラインヘルプの「Working with Reports on the New Web Interface」の章を参照してください。
Web レポートのスケジュール設定とアーカイブ	アプライアンスの新しい Web インターフェイスで Web レポートをスケジュールし、アーカイブレポートを表示できるようになりました。 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「Using Centralized Web Reporting」の章を参照してください。

SAML 2.0 を使用したシングル サインオン	シスコのコンテンツ セキュリティ管理アプライアンスは SAML 2.0 SSO をサポートするようになりました。これにより、ユーザは組織内で他の SAML 2.0 SSO 対応サービスへのアクセスに使用しているのと同じクレデンシャルでアプライアンスの Web インターフェイスにログインできます。 詳細については、ユーザー ガイドの「Common Administrative Tasks」の章を参照してください。
AsyncOS 13.0 for Cisco E メール セキュリティ アプライアンスの新機能のサポート	• **電子メールレポートのスケジュール設定とアーカイブ**: アプライアンスの新しい Web インターフェイスで電子メールレポートをスケジュール設定し、アーカイブされたレポートを表示できるようになりました。 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「Using Centralized Email Security Reporting」の章を参照してください。 • **[Safe Print] アクションレポートページ**: このレポートページを使用して、次の情報を表示できます。 – ファイル タイプ別の、Safe Print で出力された添付ファイルの数(グラフ形式)。 – ファイル タイプ別の、Safe Print で出力された添付ファイルの概要(表形式)。 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「Using Centralized Email Security Reporting」の章を参照してください。 • **[有効なレポートデータ(Reporting Data Availability)] レポートページ**: アプライアンスの新しい Web インターフェイスで、[有効なレポートデータ(Reporting Data Availability)] レポートページを表示できるようになりました。 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「Using Centralized Email Security Reporting」の章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隔離**: アプライアンスの新しい Web インターフェイスで、ポリシー、ウイルスおよびアウトブレイク隔離を設定できるようになりました。 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「Centralized Policy, Virus, and Outbreak Quarantines」の章を参照してください。 • **Swagger UI のサポート**: Swagger UI を使用すると、Web インターフェイスでの AsyncOS API リソースの設計と管理が容易になります。 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「Setup, Installation, and Basic Configuration」の章を参照してください。 • **Web 使用状況分析**: 統計分析のために Web サイトの使用状況またはアクティビティの送信を有効または無効にすることができるようになりました。詳細については、ユーザー ガイドの「Common Administrative Tasks」の章を参照してください。 • **レポートのエクスポート**: アプライアンスの新しい Web インターフェイスで、電子メールのレポーティングページを PDF(ポータブル ドキュメント ファイル)形式でエクスポートできるようになりました。 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「Working with Reports on the New Web Interface」の章を参照してください。

動作における変更

`sshconfig` CLI コマンドの変更点	このリリースにアップグレードした後は、CLI で sshconfig > sshd コマンドを使用して、SSH サーバー構成時の次の設定を編集できます。 • 公開キー認証アルゴリズム • 暗号アルゴリズム • KEX アルゴリズム • MAC メソッド • 最小サーバ キー サイズ
SSL 設定の変更	このリリースにアップグレードした後は、アプライアンスでエンドユーザーのスパム隔離サービスに対応する SSL 設定を行うことができません。
パスフレーズ設定の変更	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。
レポートのパフォーマンス改善	このリリースにアップグレードすると、セキュリティ管理アプライアンスでこれまで以上に多くの E メール セキュリティ アプライアンスを処理し、電子メールレポートデータの処理もより迅速にできるようになります。
メッセージ トラッキング パフォーマンスの変更	このリリースにアップグレードすると、アプライアンスの新しい Web インターフェイスにメッセージ検索クエリの詳細メッセージが迅速に表示されるようになります。
レガシー Web インターフェイスからのアーカイブされたレポートの表示	このリリースにアップグレードすると、アプライアンスの新しい Web インターフェイスに、レガシー Web インターフェイスで使用可能なアーカイブされたレポートが表示されます。 新しい Web インターフェイスで、[レポートのスケジュール設定とアーカイブ(Schedule & Archive Reports)] ページの [レガシーアーカイブレポートの表示(View Legacy Archived Reports)] タブを使用して、レガシー Web インターフェイスのアーカイブされたレポートを表示できます。

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比較

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
ランディングページ	セキュリティ管理アプライアンスにログインすると、[メールフロー概要（Mail Flow Summary）] ページが表示されます。	アプライアンスにログインすると、[システムステータス（System Status）] ページが表示されます。
製品ドロップダウン	[製品（Product）] ドロップダウンで、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 アプライアンスを切り替えることができます。	[電子メール（Email）] または [ウェブ（Web）] タブを使用して、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を切り替えることができます。
レポートドロップダウン	[レポート（Reports）] ドロップダウンで、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のレポートを表示できます。	[レポート（Reporting）] ドロップダウンメニューで、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のレポートを表示できます。
管理アプライアンスタブ	セキュリティ管理アプライアンスで をクリックして、[管理アプライアンス（Management Appliance）] タブにアクセスします。	レポート、メッセージトラッキング、隔離の有効化と設定、ネットワークアクセスの設定、およびシステムステータスの監視を実行できます。
カスタム レポート	カスタマイズされたレポートを表示するには、[製品（Product）] ドロップダウンから [メール（Email）] を選択し、[レポート（Reports）] ドロップダウンから [お気に入りレポート（My Favorite Reports）] を選択します。	カスタムレポートページは、[メール（Email）] > [レポート（Reporting）] > [マイレポート（My Reports）] で表示できます。
レポートのスケジュール設定とアーカイブ	スケジュール設定されたレポートおよびアーカイブされたレポートを表示するには、[製品（Product）] ドロップダウンから [メール（Email）] を選択し、[モニタリング（Monitoring）] > [スケジュールを設定してアーカイブを作成（Schedule & Archive）] を選択します。	セキュリティ管理アプライアンスで、[メール（Email）] > [レポート（Reporting）] > [スケジュールされたレポート（Scheduled Reports）] ページを使用してレポートをスケジュールすることができ、[メール（Email）] > [レポート（Reporting）] > [アーカイブ レポート（Archived Report）] ページを使用してレポートをアーカイブすることができます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
レポートの概要ページ	セキュリティ管理アプライアンスの [メール レポートの概要（Email Reporting Overview）] ページの新しい Web インターフェイスが、[メールフロー概要（Mail Flow Summary）] ページとして設計し直されました。[メール フロー概要（Mail Flow Summary）] レポートページには、受信および送信メッセージに関する傾向グラフや要約テーブルが表示されます。	セキュリティ管理アプライアンスの [メール レポートの概要（Email Reporting Overview）] ページに、お使いの E メール セキュリティ アプライアンスからのメール メッセージ アクティビティの概要が表示されます。[概要（Overview）] ページには、グラフや、着信および発信メッセージの要約テーブルが表示されます。
高度なマルウェア防御レポートページ	[レポート（Reports）] メニューの [高度なマルウェア防御（Advanced Malware Protection）] レポートページでは、次のセクションを使用できます。 • [概要（Overview）] • [AMP ファイル レピュテーション（AMP File Reputation）] • [ファイル分析（File Analysis）] • [ファイル レトロスペクション（File Retrospection）] • [メールボックスの自動修復（Mailbox Auto Remediation）]	セキュリティ管理アプライアンスの [メール（Email）] > [レポート（Reporting）] ドロップダウンメニューには次の [高度なマルウェア防御（Advanced Malware Protection）] レポートページがあります。 • [高度なマルウェア防御（Advanced Malware Protection）] • [AMP ファイル分析（AMP File Analysis）] • [AMP判定のアップデート（AMP Verdict Updates）] • [メールボックスの自動修復（Mailbox Auto Remediation）]
アウトブレイク フィルタ ページ	新しい Web インターフェイスの [アウトブレイク フィルタリング（Outbreak Filtering）] レポートページでは、[過去 1 年間のウイルスアウトブレイク（Past Year Virus Outbreaks）] および [過去 1 年間のウイルスアウトブレイクの概要（Past Year Virus Outbreak Summary）] を使用できません。	[メール（Email）] > [レポート（Reporting）] > [アウトブレイク フィルタ（Outbreak Filters）] ページには、[過去 1 年間のウイルスアウトブレイク（Past Year Virus Outbreaks）] および [過去 1 年間のウイルスアウトブレイクの概要（Past Year Virus Outbreak Summary）] が表示されます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
スパム隔離（管理者およびエンドユーザ）	新しい Web インターフェイスで [隔離（Quarantine）] > [スパム隔離（Spam Quarantine）] > [検索（Search）] をクリックして [スパム隔離（Spam Quarantine）] ページにアクセスします。 新しい Web インターフェイスでのスパム隔離ポータルへのエンド ユーザのアクセスの詳細については、新しい Web インターフェイスへのアクセス（9 ページ）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隔離	新しい Web インターフェイスで [隔離（Quarantine）] > [その他の隔離（Other Quarantine）] をクリックします。 セキュリティ管理アプライアンス上でポリシー、ウイルス、およびアウトブレイク隔離のみを表示できます。	アプライアンスでは、ポリシー、ウイルス、およびアウトブレイク隔離を表示、設定、および変更できます。
隔離内のメッセージに対するすべてのアクションの選択	隔離で複数（またはすべて）のメッセージを選択し、削除、遅延、リリース、移動などのメッセージアクションを実行できます。	隔離で複数のメッセージを選択して、メッセージアクションを実行することはできません。
添付ファイルの最大ダウンロード制限	隔離されたメッセージの添付ファイルのダウンロードの上限は 25 MB に制限されています。	-
拒否された接続	拒否された接続を検索するには、セキュリティ管理アプライアンスで、[トラッキング（Tracking）] > [検索（Search）] > [拒否された接続（Rejected Connection）] タブをクリックします。	-
クエリ設定	セキュリティ管理アプライアンスでは、メッセージトラッキング機能の [クエリ設定（Query Settings）] フィールドは使用できません。	メッセージトラッキング機能の [クエリ設定（Query Settings）] フィールドで、クエリのタイムアウトを設定できます。

Web インターフェイス ページまたは要素	新しい Web インターフェイス	レガシー Web インターフェイス
有効なメッセージ トラッキング データ	セキュリティ管理アプライアンスで歯車アイコンをクリックして、[メール（Email）] > [メッセージトラッキング（Message Tracking）] > [有効なメッセージトラッキングデータ（Message Tracking Data Availability）] を選択し、[有効なメッセージトラッキングデータ（Message Tracking Data Availability）] ページにアクセスします。	アプライアンスの欠落データ インターバルを表示することができます。
判定チャートと最後の状態の判定	判定チャートに、アプライアンス内の各エンジンによってトリガーされる可能性のあるさまざまな判定の情報が表示されます。 メッセージの最後の状態によって、エンジンのすべての可能な判定の後に、トリガーされる最終判定が決まります。	メッセージの判定チャートと最後の状態の判定は、使用できません。
メッセージの詳細におけるメッセージ添付ファイルとホスト名	メッセージの添付ファイルとホスト名は、セキュリティ管理アプライアンスのメッセージの [メッセージの詳細（Message Details）] セクションに表示されません。	メッセージの添付ファイルとホスト名は、メッセージの [メッセージの詳細（Message Details）] セクションに表示されます。
メッセージの詳細における送信者グループ、送信者 IP、SBRS スコア、およびポリシー一致	メッセージの送信者グループ、送信者 IP、SBRS スコア、およびポリシー一致の詳細は、セキュリティ管理アプライアンスでメッセージの [メッセージの詳細（Message Details）] セクションに表示されます。	メッセージの送信者グループ、送信者 IP、SBRS スコア、およびポリシー一致の詳細は、メッセージの [メッセージの詳細（Message Details）] セクションには表示されません。
メッセージの方向（受信または送信）	メッセージの方向（受信または送信）は、セキュリティ管理アプライアンスのメッセージトラッキング結果ページに表示されます。	メッセージの方向（受信または送信）は、メッセージトラッキング結果ページに表示されません。

新しい Web インターフェイスへのアクセス

新しい Web インターフェイスでは、新しいレポートのモニタリング、隔離、およびメッセージの検索が可能です。

（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>/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 13.5.0-117 へは、次のバージョンからアップグレードできます。

（注） このリリースには Cisco Web セキュリティアプライアンス向け AsyncOS 12.0.1 との互換性があります。

- 11.4.0-800
- 12.0.0-478
- 12.0.1-011
- 12.0.2-001
- 12.5.0-636
- 12.5.0-658
- 13.0.0-239
- 13.5.0-078
- 13.5.0-114

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との互換性

AsyncOS for Email Security と AsyncOS for Web Security のリリースの互換性については、https://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/products-release-notes-list.html から入手可能な互換性マトリクスで詳しく説明されています。

インストールおよびアップグレードに関する注意事項

- 重要な追加資料（12 ページ）
- 仮想アプライアンス（12 ページ）
- アップグレード前の要件（13 ページ）

- アップグレード中の IPMI メッセージ（13 ページ）
- このリリースへのアップグレード（13 ページ）

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（16 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。

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）

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。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との互換性（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 コンテンツ セキュリティ管理アプライアンス 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。

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：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（13 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。

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

- ハードウェアモデル：M190、M195、M390、M395、M690、M695。

  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、https://www.cisco.com/c/en/us/support/docs/field-notices/639/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。
- M160、M360、M660、および X1060
- M170、M370、M370D、M670、および X1070
- M380 および M680

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

既知の問題	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=13.5.0&sb=afr&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager&sts=open
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=13.5.0&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（13.5 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 Content Security 製品のマニュアル:	入手場所
Cisco コンテンツ セキュリティ管理アプライアンス	http://www.cisco.com/c/ja_jp/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Web セキュリティ アプライアンス	http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html
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。