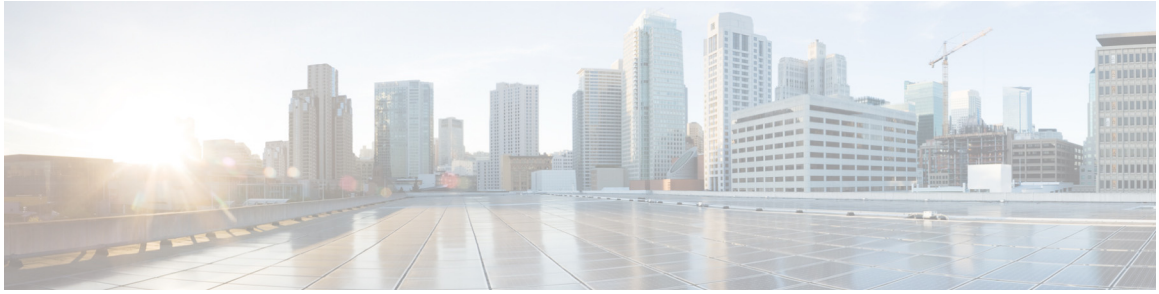

Cisco Secure Email and Web Manager 用 AsyncOS 13.8.1 リリースノート：MD（メンテナンス導入）

初版：2022 年 7 月 4 日

目次

- 今回のリリースでの変更点（2 ページ）
- 動作における変更（4 ページ）
- 新しい Web インターフェイスへのアクセス（5 ページ）
- AsyncOS 13.8.1 へのアップグレード（7 ページ）
- インストールおよびアップグレードに関する注意事項（8 ページ）
- このリリースでサポートされているハードウェア（13 ページ）
- 既知および修正済みの問題（13 ページ）
- 関連資料（15 ページ）
- サービスとサポート（15 ページ）

（注） AsyncOS 13.8.0 には、次の SSL 設定変更が含まれています。

- SSL v2.0 および SSL v3.0 方式はサポートされていません。
- TLS v1.0 方式は無効です。

アップグレード後にサービスがスムーズに機能するように、アップグレードする前に TLS v1.1 または TLS v1.2 に切り替えることをお勧めします。詳細については、SSL 設定の変更（11 ページ）を参照してください。

Cisco Systems, Inc.
www.cisco.com

（注） **重要** Cisco Content Security Management 13.8.1-068 へのアップグレードを実行した後で以前のバージョンに戻すことはできません。

今回のリリースでの変更点

機能	説明
AsyncOS API を使用したログ情報の取得	AsyncOS API を使用して、アプライアンスから次のログ詳細を取得できるようになりました。 • サブスクリプションの詳細を記録します。 • 特定のログサブスクリプションのすべてのログファイル。 • ファイル名または URL を使用したログファイル。 詳細については、『AsyncOS API 13.8.1 for Cisco Security Management Appliances - Getting Started Guide』の「*Logging APIs*」の項を参照してください。
監査ログを使用した認証、許可、アカウンティングのイベント（AAA: Authentication、Authorization、および Accounting）の記録	Cisco コンテンツセキュリティ管理アプライアンスは、AAA（認証、許可、アカウンティング）のイベントを記録する新しいタイプのログサブスクリプション「監査ログ」をサポートしています。監査ログの詳細の一部を次に示します。 • ユーザー - ログオン • ユーザー - ログオンに失敗しました、パスワードが正しくありません • ユーザー - ログオンに失敗しました、ユーザー名が不明です • ユーザー - ログオンに失敗しました、アカウントの有効期限が切れています • ユーザー - ログオフ • ユーザー - ロックアウト • ユーザー - アクティブ化済み • ユーザー - パスワードの変更 • ユーザー - パスワードのリセット • ユーザー - セキュリティ設定/プロファイルの変更 • ユーザー - 作成済み • ユーザー - 削除済みまたは変更済み • ユーザー設定：ユーザーが行った設定変更 • グループ/ロール - 削除済みまたは変更済み • グループ/ロール - 権限の変更 • 隔離 - 隔離内のメッセージに対して実行されるアクション。 詳細については、『User Guide for AsyncOS 13.8.1 for Cisco Content Security Management Appliances』の「*Using Audit Logs*」を参照してください。

AsyncOS API のコンテンツセキュリティ管理アプライアンスでの OpenID Connect 1.0 の設定	Cisco コンテンツセキュリティ管理アプライアンスは、OpenID Connect 1.0 認証で ID プロバイダ(IDP)を使用するアプリケーションまたはクライアントとの統合をサポートし、アプライアンスで使用可能な AsyncOS API とシームレスに接続します。現在、お使いのアプライアンスは、Microsoft AD FS のみを使用して OpenID Connectで認定されています。 詳細については、『User Guide for AsyncOS 13.8.1 for Cisco Content Security Management Appliances』の「*Common Administrative Tasks*」を参照してください。
コンテンツ セキュリティ管理アプライアンスでの URL 検索	NG レポートの [Web インタラクション トラッキング(Web Interaction Tracking)] ページの検索バーで [次で始まる(Starts With)] および [完全一致(Exact Match)] のフィルタオプションを、選択した時間範囲内で使用して、着信 URL と発信 URL の両方で URL 検索を実行できるようになりました。検索結果は、カンマ区切り値(.CSV)ファイルにエクスポートしたり、望ましい方法で結果を表示するためにソートしたりできます。

動作における変更

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。
事例集の機能	AsyncOS 13.6.2 では、事例集は次のページでスタンドアロンウィジェットになっていました。電子メールの [サービスステーテス(Service Status)] ページおよび Web の [モニタリング(Monitoring)] ページ。AsyncOS 13.6.2 よりも前は、事例集は新しい Web インターフェイスのすべてのページでスタンドアロンウィジェットになっていました。 このリリースにアップグレードすると、事例集は Cisco SecureX Ribbon に含まれます。
自動隔離キューの修復	このリリースにアップグレードした後、アプライアンスは、ユーザーの介入なしに破損したメッセージを破棄することで、破損した隔離キューを自動的に修復しようとします。ただし、Cisco テキストメールログ (mail_logs)で自動修復が失敗した場合は、Cisco TAC にお問い合わせください。
パスフレーズの変更	新しいユーザーアカウントでは、3 文字以上の繰り返し文字または連続文字を含むパスフレーズを使用できません。
スパム隔離の変更	• このリリースよりも前は、隔離へのアクセスに証明書なしのログインを有効にするオプションは、[スパム隔離の編集(Edit Spam Quarantine)] > [スパム通知(Spam Notifications)] > [メッセージ本文(Message Body)] で使用できました。 このリリースにアップグレードした後は、[スパム隔離の編集(Edit Spam Quarantine)] > [スパム通知(Spam Notifications)] > [隔離アクセス(Quarantine Access)] でこのオプションを使用できるようになります。 • このリリースにアップグレードした後は、CLI で `spamdigestconfig` コマンドを使用して次のオプションを設定できます。 – スパム通知でリンクの有効期限を設定します。これらのリンクは、指定された期間後に自動的に期限切れになります。 – スパム通知内のすべての隔離メッセージを表示するためにリンクを表示するか非表示にするかを選択します。また、スパム通知でリンク表示を選択している場合は、エンドユーザーにスパム隔離へのアクセスの前に認証を強制できるようになりました。
SSL 設定の変更	SSL 設定の変更(11 ページ)を参照してください。
アップグレード	**重要:** Cisco Content Security Management 13.8.1-068 へのアップグレードを実行した後で以前のバージョンに戻すことはできません。
トンネルサービス	アップグレードを実行した場合、以前のバージョンに戻してアプライアンスを再起動すると、すべてのトンネルおよびサービスアクセスが無効になります。サービスを再度有効にする必要があります。

設定マスター	**以前の動作** 設定マスターページでユーザーが設定マスターを変更する場合は、必ず確定する必要がありました。 **動作の変更** 設定マスターページでユーザーが CM を変更する場合、CM がロードされたことを示すポップアップウィンドウで [OK] ボタンをクリックすると、黄色の確定ボタンは表示されません。
サブ設定マスター	**以前の動作** サブ設定マスターが上書きされ、セカンダリ設定マスターで誤ってプッシュされます。 **動作の変更** **(注)** 次のものを同時に使用して設定変更を実行しないでください。 • 同じブラウザ上の複数のタブ。 • 同じシステムまたは 2 つの異なるシステム上の複数のブラウザ。 また、予期しない動作が発生する可能性があるため、Web インターフェイスと CLI セッションを同時に使用しないでください。 サブ設定マスターを同時に切り替えたり、変更したりすることは推奨されていません。また、変更中は設定マスターをプッシュしないでください。 ただし、2 人のユーザーが同時にログインした場合、または同じユーザーが 2 つの異なるブラウザからログインし、設定マスターで同時に変更を実行した場合は、2 番目のユーザーにエラー ID メッセージが表示されます。

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、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 1440x900 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ときに、`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先駆者の HTTPS ポートです。

- `trailblazerconfig` CLI コマンドが無効になっているときに、`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。

AsyncOS 13.8.1 へのアップグレード

- AsyncOS 13.8.1-101 - MD(メンテナンス導入)へのアップグレード
- AsyncOS 13.8.1-701 へのアップグレード:LD(限定導入)
- AsyncOS 13.8.1-090 - MD(メンテナンス導入)へのアップグレード
- AsyncOS 13.8.1-074 - MD(メンテナンス導入)へのアップグレード
- AsyncOS 13.8.1-068 - MD(メンテナンス導入)へのアップグレード

AsyncOS 13.8.1-101 - 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 13.8.1-101 にアップグレードすることができます。

- 12.0.1-017
- 12.0.2-007
- 12.5.0-683
- 12.5.0-696
- 12.8.1-002
- 13.0.0 - 277
- 13.6.2-090
- 13.8.1 - 090

AsyncOS 13.8.1-701 へのアップグレード:LD(限定導入)

次のバージョンから、リリース 13.8.1-701 にアップグレードすることができます。

- 13.8.1-052
- 13.8.1 - 090

AsyncOS 13.8.1-090 - 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 13.8.1-090 にアップグレードすることができます。

- 12.0.1-011
- 12.0.1-017
- 12.0.2-005
- 12.0.2-007
- 12.5.0-683
- 12.8.1-002
- 13.0.0 - 277
- 13.6.2 - 078
- 13.8.1-068
- 13.8.1-074

AsyncOS 13.8.1-074 - 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 13.8.1-074 にアップグレードすることができます。

- 12.0.1-011
- 12.0.1-017
- 12.0.2-005
- 12.0.2-007
- 12.5.0-683
- 12.8.1-002
- 13.0.0-249
- 13.6.2-052
- 13.6.2-058
- 13.8.1-068

AsyncOS 13.8.1-068 - 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 13.8.1-068 にアップグレードすることができます。

- 12.0.1-011
- 12.0.1-017
- 12.0.2-005
- 12.0.2-007
- 12.5.0-683
- 12.8.1-002
- 13.0.0-249
- 13.6.2-052
- 13.8.0-344
- 13.8.1-052
- 13.8.1-063

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(9 ページ)
- 仮想アプライアンス(9 ページ)
- アップグレード前の要件(10 ページ)
- アップグレード中の IPMI メッセージ(12 ページ)
- このリリースへのアップグレード(12 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(15 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(9 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(10 ページ)
- 既存の設定のバックアップ(10 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(10 ページ)
- SSL 設定の変更(11 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(8 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 13.0 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 セキュリティ コンテンツ管理アプライアンスを AsyncOS 13.8.0 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。

SSL 設定の変更

AsyncOS 13.8.0 には、Web インターフェイス、LDAP、およびアップデータサービスの次の SSL 設定変更が含まれています。

- SSL v2.0 および SSL v3.0 方式はサポートされていません。
- TLS v1.0 方式は、アップグレード後に無効になります。

次の表に、アップグレード前とアップグレード後のシナリオを示します。

シナリオ	TLS バージョン	アップグレード前	アップグレード後
1	TLS 1.0	対応	N
	TLS 1.1	N	対応
	TLS 1.2	N	対応
2	TLS 1.0	N	N
	TLS 1.1	対応	対応
	TLS 1.2	N	N
3	TLS 1.0	N	N
	TLS 1.1	N	N
	TLS 1.2	対応	対応
4	TLS 1.0	N	N
	TLS 1.1	対応	対応
	TLS 1.2	対応	対応
5	TLS 1.0	対応	N
	TLS 1.1	対応	対応
	TLS 1.2	対応	対応
6	TLS 1.0	対応	N
	TLS 1.1	対応	対応
	TLS 1.2	N	N

次の点を考慮してください。

- アップグレード後にこれらのサービスがスムーズに機能するように、アップグレードする前に TLS v1.1 または TLS v1.2 に切り替えることをお勧めします。
- これらのサービスに TLS v1.0 を使用するには、アップグレード後にこのプロトコルバージョンを有効にします。ただし、セキュリティを強化するために、TLS v1.1 または TLS v1.2 に切り替えることをお勧めします。

[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` コマンドを使用して、SSL 設定を変更できます。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(10 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(9 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

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 (13 ページ)
- 既知および修正済みの問題のリスト (14 ページ)
- 既知および解決済みの問題に関する情報の検索 (14 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/search?kw=*&pf=prdNm&pfVal=282941571&rls=13.8.1&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=282941571&rls=13.8.1&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://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(release)] フィールドに、リリースのバージョン(13.8 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s	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s	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s	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 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。

シスコおよびシスコのロゴは、米国およびその他の国におけるシスコおよびその関連会社の商標または登録商標です。シスコ の商標の一覧は、www.cisco.com/go/trademarks でご確認いただけます。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

このマニュアルで使用している IP アドレスと電話番号は、実際のアドレスと電話番号を示すものではありません。マニュアル内の例、コマンド表示出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2022 Cisco Systems, Inc. All rights reserved.