



AsyncOS 14.3 for Cisco Secure Email and Web Manager リリースノート (クラウドリリースのみ)

発行日: 2022 年 9 月 29 日



(注) AsyncOS 14.3 for Cisco Secure Email and Web Manager のリリースは、クラウドリリースのみです。

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 \(2 ページ\)](#)
- [アップグレード パス \(5 ページ\)](#)
- [インストールおよびアップグレードに関する注意事項 \(5 ページ\)](#)
- [このリリースでサポートされる VM \(5 ページ\)](#)
- [既知および修正済みの問題 \(6 ページ\)](#)
- [関連資料 \(7 ページ\)](#)
- [サービスとサポート \(7 ページ\)](#)



(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。





今回のリリースでの変更点

機能	説明
AMP の設定のカスタムユーザーロール	<p>管理者は、すべての電子メールゲートウェイまたは選択したレポートグループの AMP 関連レポートを表示するため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ユーザーに割り当てることができます。</p> <p>管理者は、[システム管理者 (System Administrator)] > [ユーザーロール (User Role)] > [電子メールユーザーロールの追加 (Add Email User Role)] に移動し、[電子メールレポート (Email Reporting)] フィールドの [レポートグループのデータへのアクセス (Access to data in Reporting Group)] または [すべての電子メールアプライアンスのデータへのアクセス (Access to data in all Email Appliances)] で [AMP レポート (AMP Reports)] を選択して、AMP カスタムユーザーロールを作成できます。</p> <p>詳細については、「管理タスクの分散」の章の「電子メールレポートイングへのアクセス」セクションを参照してください。</p>

動作における変更

Print および Clear サブコマンドが Certconfig コマンドで使用可	<p>このリリース以前は、インバウンド、アウトバウンド、HTTPS 管理アクセス、および LDAPS サービス用にインストールされた各種証明書やキーの印刷や消去ができませんでした。</p> <p>このリリースへのアップグレード後は、インバウンド、アウトバウンド、HTTPS 管理アクセス、および LDAPS サービス用にインストールされた各種証明書やキーの印刷や消去ができます。</p> <p>CLI で Certconfig > Print または Clear サブコマンドを使用して、インストールされた各種証明書やキーの印刷や消去ができます。</p>
JWT トークン: エラーメッセージの変更	<p>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。</p> <p>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せん。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。</p>

SPoG 機能の変更	<p>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。</p> <p>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。</p> <p></p> <p>(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。</p>
メッセージ追跡:修復アクションの変更	<p>このリリース以前は、[修復アクションの確認(Confirm Remediation Action)] ダイアログボックスの [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。</p> <p>このリリース以降は、[修復アクションの確認(Confirm Remediation Action)] ダイアログボックスの [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。その他の特殊文字は使用できません。</p>
Syslog ディスクバッファサイズ構成の変更	<p>このリリース以前は、syslog プッシュ ログ サブスクリプションに許可された最大 syslog ディスクバッファサイズは 10 GB でした。</p> <p>このリリース以降は、syslog プッシュ ログ サブスクリプションに許可される最大 syslog ディスクバッファサイズは 1 GB です。</p> <p>(AsyncOS アップグレードのみに適用):アップグレード前に既存の設定値が 1 GB を超えている場合、システムはアップグレード中に最大ディスクバッファサイズ値を自動的に 1 GB に減らします。</p> <p></p> <p>(注) アップグレード中に、割り当てられたその他のディスククォータが設定された制限を超えた場合は、最大ディスクバッファサイズ値(既存の設定値が 1 GB を超える場合)を減らして、割り当てられたその他のディスククォータスペースを解放して、アップグレードプロセスを続行する必要があります。</p>

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。

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。

- URL `https://example.com:4431/ng-login` を使用できます。
`example.com` はアプライアンスのホスト名を示します。
- 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。

エンドユーザーは、新しい Web インターフェイスのスパムの隔離にアクセスできます。スパムの隔離にログインするには、次の URL を使用します。

`https://example.com:4431/euq-login`

`example.com` はアプライアンスのホスト名を示します。



(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

次のバージョンからリリース 14.3.0-115 にアップグレードできます。

- 14.0.0-404
- 14.0.0-418
- 14.1.0-199
- 14.1.0-239
- 14.1.0-250
- 14.2.0-206
- 14.3.0-068

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\(5 ページ\)](#)
- [アップグレード後の要件\(5 ページ\)](#)

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\(7 ページ\)](#)を参照してください。

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 14.3 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る VM

このリリースでは、次の VM がサポートされています。

- 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 \(6 ページ\)](#)
- [既知および修正済みの問題のリスト \(6 ページ\)](#)
- [既知および解決済みの問題に関する情報の検索 \(6 ページ\)](#)

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=14.3.0&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=282941571&rls=14.3.0&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://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ガイド PDF の「More Information」の章に記載されています。

Cisco Secure 製品のマニュアル:	入手場所
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 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
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.