AsyncOS 15.5.1 for Cisco Secure Email and Web Manager（Cloud）リリースノート（一般導入）

発行日：2024 年 4 月 30 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）
- アップグレード パス（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（7 ページ）
- このリリースでサポートされる VM（9 ページ）
- 既知および修正済みの問題（10 ページ）
- ソフトウェア ライフサイクル サポート ステートメント（11 ページ）
- サービスとサポート（11 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。

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

機能	説明
Vault サービスのモニタリングとアラートの送信	Cisco Secure Email and Web Manager は、初期化されているかどうかにかかわらず、Vault サービスをモニターし、そのステータスを追跡するようになりました。また、適切なアラートメッセージを送信し、ステータス情報を mail_logs に記録します。 アラートログには、次のいずれかの方法でアクセスできます。 • Web インターフェイスで [システム管理（System Administration）] > [アラート（Alerts）] ページに移動し、[上位アラートの表示（View Top Alerts）] ボタンをクリックします。 • CLI で `displayalerts` コマンドを使用します。 何らかの問題によって Vault サービスの初期化に失敗した場合は、Vault サービスがダウンしていることを示すアラートメッセージを（メール、Web インターフェイス、および CLI で）受信します。Vault サービスを復元するには、Vault Recovery プロセスを実行する必要があります。 （注） AsyncOS 15.5.1 へのアップグレード中にアップグレードが失敗した場合は、upgrade_logs で Vault サービスエラーを確認する必要があります。Vault サービスエラーがあった場合は、Vault サービスを復元するか、設定を保存せずにアップグレードプロセスを続行する必要があります。 アラートメッセージは次のようなシナリオで受信します。 • AsyncOS 15.5.1 へのアップグレード後に Vault サービスの初期化に失敗した場合、メール、Web インターフェイス、および CLI でアラートメッセージを受信します。 • Cisco Secure Email and Web Manager のいずれかのサービスが初期化に失敗した Vault サービスを使用している場合、メール、Web インターフェイス、および CLI でアラートメッセージを受信します。暗号化が有効になっている場合は、常にアラートメールを受信します。暗号化が無効になっている場合は、Vault サービスを使用するサービスが設定されている場合にのみアラートメールを受信します。暗号化ステータスは、`adminaccessconfig` > `encryptconfig` サブコマンドを使用して確認できます。 Vault モニタリングメカニズム は、75 分ごとに Vault サービスをチェックします。ダウンしている場合は、Vault サービスが復元されるまでアラートメッセージを送信します。 成功した Vault 正常性チェックと初期化ログエントリの例については、ユーザーガイドの「Logging」の章にある「Successful Vault Health Check and Initialization」セクションを参照してください。

	Vault サービスを復元するには、Vault Recovery プロセスを実行する必要があります。 **注意** 暗号化（CLI > `adminaccessconfig` > `encryptconfig`）が有効になっている場合は、データの損失を防ぐため、Cisco Secure Email and Web Manager の設定のコピーを常に保存し、維持してください。 Cisco Secure Email and Web Manager の設定を保存する方法の詳細については、Cisco Secure Email and Web Manager の設定の保存（8 ページ）を参照してください。 Vault Recovery プロセスの実行方法については、Vault の問題を解決するための Vault Recovery プロセスの実行（8 ページ）を参照して ください。
Web インターフェイスおよび API サーバーの TLS 1.3 サポート	Cisco Secure Email and Web Manager と API サービスのレガシーまたは新しい Web インターフェイス全体で TLS 通信に TLS 1.3 を使用できます。 詳細については、ユーザーガイドの「Common Administrative Tasks」の章にある「Secure Communication Protocol」セクションを参照してください。
検索フィルタの機能拡張	検索を強化するために、レポートページの下部にある [検索（Search）] リボンのドロップダウンリストに、[次を含む（Contains）] と [次を含まない（Does Not Contain）] という 2 つの新しいフィルタが追加されました。 詳細については、ユーザーガイドの「Using Centralized Email Security Reporting」の章にある「Searching and the Interactive Email Report Pages」セクションを参照してください。

動作における変更

SSH サーバの設定変更	**新規インストールのシナリオ** 次の SSH サーバー設定の変更は、Cisco Secure Email and Web Manager 用の AsyncOS 15.5.1 を初めてインストールする場合に適用されます。 **[非 FIPS モード]** Cisco Secure Email and Web Manager では、次の暗号アルゴリズム、MAC メソッド、ホストキーアルゴリズム、および Kex アルゴリズムがサポートされています。 • 暗号アルゴリズム:`aes128-gcm@openssh.com` および `chacha20-poly1305@openssh.com` • MAC メソッド:`hmac-sha2-256` • ホストキーアルゴリズム:`ecdsa-sha2-nistp256` および `ssh-ed25519` • Kex アルゴリズム:`curve25519-sha256`、`diffie-hellman-group14-sha256`、および `curve25519-sha256@libssh.org` **[FIPS モード]** Cisco Secure Emailand Web Manager では、次の暗号アルゴリズム、MAC メソッド、およびホストキーアルゴリズムがサポートされています。 • 暗号アルゴリズム:`aes128-gcm@openssh.com` • MAC メソッド:`hmac-sha2-256` • ホストキーアルゴリズム:`ecdsa-sha2-nistp256` **(注)** Cisco Secure Email and Web Manager を下位の AsyncOS バージョンから AsyncOS 15.5.1 以降のバージョンにアップグレードすると、サポートする必要があるすべてのアルゴリズムが SSH サーバーに追加されます。
TLS 接続ステータスのログメッセージの変更	TLS 接続ステータスのログメッセージが変更され、次のサービスの証明書の有効期限の日時または証明書の有効期間の開始日時とともに、有効性チェックに関する詳細が含まれるようになりました。 • LDAP • アップデータ • Syslog • TLS を介したアラート • SMTP アウトバウンド(EUQ)

アプリケーション SSH クライアントアルゴリズムのサポート	アプリケーション SSH クライアントアルゴリズムは、次の接続でサポートされます。 • Cisco Secure Email Gateway を Cisco Secure Email and Web Manager に接続する場合。 • Cisco Secure Email and Web Manager から設定をバックアップする場合。 • セカンダリの Cisco Secure Email and Web Manager をプライマリの Cisco Secure Email and Web Manager に追加する場合。 **[非 FIPS モード]** 既存のアルゴリズムに加え、次の暗号アルゴリズム、MAC メソッド、および KEX アルゴリズムがデフォルトで Secure Email and Web Manager に追加されます。 • 暗号アルゴリズム：`aes128-ctr` • MAC メソッド：`hmac-sha2-256` • KEX アルゴリズム：`diffie-hellman-group14-sha256` **[FIPS モード]** 既存のアルゴリズムに加えて、次の暗号アルゴリズムと MAC メソッドがデフォルトで Secure Email and Web Manager に追加されます。 • 暗号アルゴリズム：`aes128-ctr` • MAC メソッド：`hmac-sha2-256`
Splunk データベースファイルの削除	このリリースより前は、Cisco Secure Email and Web Manager はアップグレードプロセス後も Splunk データベースファイルを保持していました。 このリリースへのアップグレード後は、アップグレードプロセスの前に Splunk データベースファイルが存在していた場合、Cisco Secure Email and Web Manager はすべての Splunk データベースファイルを削除します。
パスワードのサブストリングの受け入れ	このリリースより前は、文字列「password」のサブストリング（3 文字以上）を含むパスワードを持つユーザーを追加すると、システムは「pas」、「wor」、「ord」などのサブストリングを受け入れませんでした。 このリリースへのアップグレード後は、文字列「password」のサブストリング（3 文字以上）を含むパスワードを持つユーザーを追加すると、システムは「pas」、「wor」、「ord」などのサブストリングを受け入れ、サブストリングをより包括的に検出するようになります。

/data/db/syslogs ディレクトリからのファイルの削除	このリリースより前は、*/data/db/syslogs* ディレクトリ内のファイルを削除できませんでした。 このリリース以降、`wipedata` CLI コマンドを使用して、*/data/db/syslogs* ディレクトリ内のファイルを削除できます。`wipedata` コマンドを使用して */data/db/syslogs* ディレクトリからファイルを削除すると、Syslog Push を使用してログファイルを取得したい場合は、ログサブスクリプションを [手動(Manual)] に変更し、設定を **Syslog** に戻すようにと知らせる通知メッセージも受信します。

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。

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て、[新しくなったセキュリティ管理アプライアンスをお試しください(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 15.5.1-024 にアップグレードできます。

- 14.2.0-224
- 14.2.0-241
- 14.3.0-120
- 14.3.0-124
- 15.0.0-334
- 15.0.0-413
- 15.5.1-004

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（7 ページ）
- アップグレード前の要件（7 ページ）
- アップグレード後の要件（9 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、ソフトウェア ライフサイクル サポート ステートメント（11 ページ）を参照してください。

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。

- Cisco Secure Email and Web Manager の設定の保存（8 ページ）
- Vault の問題を解決するための Vault Recovery プロセスの実行（8 ページ）
- 既存のデータベースのバックアップ（9 ページ）

Cisco Secure Email and Web Manager の設定の保存

Cisco Secure Email and Web Manager で暗号化が有効になっている場合は、AsyncOS 15.5.1 にアップグレードする前または後に、Cisco Secure Email and Web Manager の設定のコピーを保存することをお勧めします。

Vault Recovery プロセスを実行して Vault サービスを復元した後、保存した Cisco Secure Email and Web Manager の設定をロードして、デバイスの以前の設定を復元できます。

次の方法を使用してデバイスの設定を保存できます。

- [システム管理(System Administration)] > [設定ファイル(Configuration File)] に移動し、[コンフィギュレーション ファイルでパスフレーズを暗号化する(Encrypt passphrases in the Configuration Files)] を選択します。
- CLI で `saveconfig` コマンドを使用し、**2** をタイプして [パスフレーズを暗号化する(Encrypt passphrases)] オプションを選択します。

Vault の問題を解決するための Vault Recovery プロセスの実行

AsyncOS 15.5.1 にアップグレードする前または後に、Cisco Secure Email and Web Manager で Vault 関連の問題が発生した場合は、その問題を解決するために Vault Recovery プロセスを実行する必要があります。次の手順を使用して Vault Recovery を実行します。

1. 次のログイン情報を使用して、直接 SSH 接続で Cisco Secure Email and Web Manager にログインします。

   ユーザー名:**enablediag**

   パスワード:**管理者ユーザーのパスワード**
2. `recovervault` コマンドを実行します。
3. プロンプトが表示されたら、次の一連のサブコマンドを入力します。
   a. `yes`
   b. `1 (encryption enabled) or 2 (encryption disabled)`
4. 管理者ユーザーのログイン情報を使用して Cisco Secure Email and Web Manager にログインし、Vault リカバリプロセスが完了したらデバイスを再起動します。
5. (**暗号化が有効になっている場合のみ**)以前に保存したデバイスの設定のコピーをロードして、以前の設定を復元します。
6. Vault サービスのアラートがないか、Cisco Secure Email and Web Manager を数時間モニターします。

Cisco Secure Email and Web Manager が回復し、Vault が再初期化されます。これで、問題なくデバイスに接続できます。

(注) **暗号化無効**

このシナリオでは、すべてのシステム設定が保持されます。

暗号化有効

このシナリオでは、次の暗号化された変数がデフォルトの工場出荷時の値にリセットされます。

- ログ サブスクリプション(Log Subscriptions)
- SAML 設定

- LDAP 設定
- SNMP 設定
- 更新設定
- ユーザーの構成設定
- SMA アプライアンスの構成設定
- SMA ユーザー設定
- CERTCONFIG 設定
- リモート電源投入設定
- システム時刻設定の NTP 設定

以前の設定を復元する場合は、以前に保存した設定ファイルをロードする必要があります。

既存のデータベースのバックアップ

Cisco Secure Email and Web Manager をアップグレードする前に、Cisco Secure Email and Web Manager の既存のデータベースをバックアップします。

Secure Email and Web Manager のディザスタリカバリの詳細については、ユーザーガイドの「Common Administrative Tasks」の章にある「Backing Up Security Management Appliance」のセクションを参照してください。バックアッププロセスをスケジュールする詳細な手順については、ユーザーガイドの「Common Administrative Tasks」の章の「Scheduling Single or Recurring Backups」のセクション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 15.5.1 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問題に関する情報を検索します。

- バグ検索ツールの要件（10 ページ）
- 既知および修正済みの問題のリスト（10 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?kw=*&pf=prdNm&sb=afr&sts=open&svr=3nH&bt=custV&prdNam=Cisco%20Secure%20Email%20and%20Web%20Manager&rls=15.5.1,15.5.0
修正済みの問題	https://bst.cloudapps.cisco.com/bugsearch?kw=*&pf=prdNm&rls=15.5.1&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問題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（15.5.1 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。

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。

ソフトウェア ライフサイクル サポート ステート メント

ソフトウェアのタイムベースのリリースモデルおよびソフトウェアリリースのサポートタイムラインについては、「Software Lifecycle Support Statement」を参照してください。

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、「ソフトウェア ライフサイクル サポート ステートメント」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。