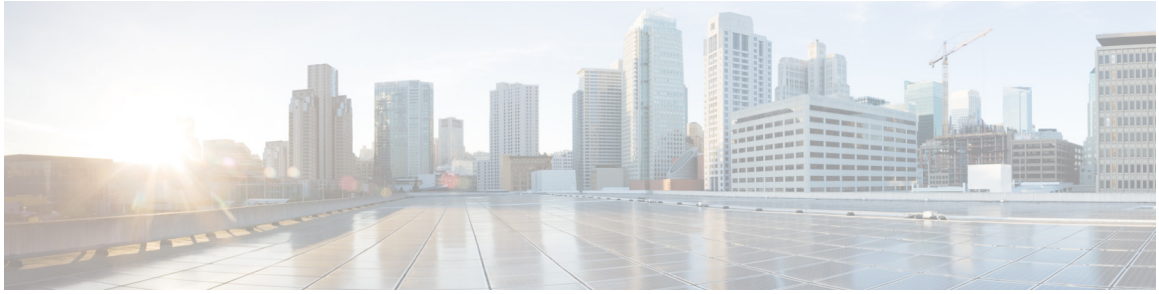

AsyncOS 15.0 for Cisco Secure Email and Web Manager リリースノート（一般導入）

発行日：2023 年 8 月 10 日

目次

（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。

（注） 別の管理者ログインで管理されている Cisco SecureX アカウントをすでに持っている場合は、SSE にデバイスを登録してからスマートライセンス登録を実行することを推奨します。最初にデバイスを SSE に登録せずにスマートライセンス登録を実行しないでください。これは既知の問題（不具合 ID：CSCvy10226）です。

Cisco Systems, Inc.
www.cisco.com

今回のリリースでの変更点

機能	説明
FIPS 認定	Cisco Secure Email and Web Manager は FIPS 認定され、FIPS 140-2 認定の暗号化モジュール、Cisco Common Crypto Module を統合しました（FIPS 140-2 認定 #4036）。 （注） Cisco Secure Email and Web Manager の FIPS 認定は、電子メールゲートウェイの統合にのみ適用され、Cisco Secure Web Appliance の統合には適用されません。 （注） Secure Email and Web manager が FIPS モードの場合、TLS v1.0 方式はサポートされません。
	SSH サーバーとクライアントの設定 次の SSH サーバー設定は、Cisco Secure Email and Web Manager 用の AsyncOS 15.0 を初めてインストールする場合、および FIPS モードが有効な場合にサポートされます。 **[SSH サーバー設定]** 次の暗号アルゴリズム、ホストキーアルゴリズム、KEX アルゴリズム、および MAC メソッドは、デフォルトで Secure Email and Web Manager でサポートされています。 • **暗号アルゴリズム**：`aes128-ctr`、`aes256-ctr`、`aes128-cbc`、`aes192-cbc`、および `aes256-cbc` • **ホストキーアルゴリズム**：`rsa-sha2-256` • **KEX アルゴリズム**：`diffie-hellman-group14-sha1`、`ecdh-sha2-nistp256`、`ecdh-sha2-nistp384`、および `ecdh-sha2-nistp521` • **MAC メソッド**：`hmac-sha1`

	[SSH クライアント設定] 次の暗号アルゴリズム、ホストキーアルゴリズム、KEX アルゴリズム、および MAC メソッドは、デフォルトで Secure Email and Web Manager でサポートされています。 • **暗号アルゴリズム**：`aes128-ctr`、`aes192-ctr`、`aes256-ctr`、`aes128-cbc`、`aes192-cbc`、`aes256-cbc`、`aes128-gcm@openssh.com`、および `aes256-gcm@openssh.com` • **ホストキーアルゴリズム**：`rsa-sha2-256` • **KEX アルゴリズム**：`diffie-hellman-group14-sha1`、`ecdh-sha2-nistp256`、`ecdh-sha2-nistp384`、および `ecdh-sha2-nistp521` • **MAC メソッド**：`hmac-sha1` この機能の詳細については、ユーザーガイドの「FIPS Management」の章を参照してください。
単一ログライン（SLL）	SLL 機能は、電子メールトラッキングデータを単一ログラインまたはフラット化モデルとして作成、インデックス付け、および保存します。したがって、クエリを実行してすぐに応答を取得できます。この機能は、高速応答、低メモリ、および CPU 使用率により、トラッキングクエリまたは検索のパフォーマンスを向上させます。 この機能は、アップグレード後の電子メールトラッキングデータにのみ適用されます。
CRL ソースの設定	Secure Email and Web Manager は、ユーザーの証明書が失効していないことを確認するために、証明書検証の一環として証明書失効リスト（CRL）と呼ばれる失効した証明書のリストを確認します。サーバー上でこのリストを最新のバージョンに保つ必要があります。Secure Email and Web Manager はユーザーが作成したスケジュールでこれをダウンロードします。リストは手動で更新することもできます。 次の方法を使用して CRL ソースを設定できます。 • レガシー Web インターフェイスで、[ネットワーク（Network）] > [CRL ソース（CRL Sources）] > [CRL ソースの追加（Add CRL Source）] > [CRL（証明書失効リスト）ソースの追加（Add CRL (Certificate Revocation Lists) Source）] ウィンドウに移動します。 • CLI の `Certconfig` > `CRL` サブコマンドを使用します。 CRL ソースの設定の詳細については、ユーザーガイドの「Common Administrative Tasks」の章にある「Configuring CRL Sources」のセクションを参照してください。

古い Splunk データの削除	Secure Email and Web Manager 15.0 以降にアップグレードし、電子メールトラッキングデータが Splunk データベースに含まれている場合、アップグレードを続行すると、システムによって Splunk データベースとバイナリが削除されます。 （注） Secure Email and Web Manager 13.6.2 リリース以降、Splunk データベースは電子メールトラッキングデータの保存に使用されなくなりました。新しい電子メールトラッキングデータはすべて、Lucene データベースに保存されます。Secure Email and Web Manager 15.0 にアップグレードすると、Secure Email and Web Manager 13.6.2 へのアップグレード前のすべてのトラッキングデータが削除され、回復できなくなります。 Secure Email and Web Manager 15.0 以降へのアップグレード中に、システムが Splunk データベースを削除することを示す警告メッセージが、CLI または Secure Email and Web Manager の Web インターフェイスに表示されます。 **警告メッセージの例** *"From the Secure Email and Web Manager 13.6.2 version onwards, we have moved to a newer storage system for email tracking data. Generally, the old data is replaced with new data in the new storage system automatically. However, in some scenarios (for example, late upgrades, low mail flow and tracking data, and so on), there could be traces of old data still present in the old storage system that is no longer supported.* *In your case, it is 19 MB, which was last updated on 11 Aug 2022.* *You can take a back up of the email tracking data (if required). You can use the backupconfig command in the CLI to perform the backup action. For more information, see the 'Scheduling Single or Recurring Backups' section in the 'Common Administrative Tasks' chapter of the user guide.* *If you proceed with this upgrade process, your Splunk email tracking data will be deleted.* *You can choose to proceed with the upgrade or abort the upgrade.* *Do you agree to proceed with this upgrade? [Y]"* （注） 警告メッセージは、オンプレミスの管理者ユーザーにのみ表示されます。

	（注） Splunk データベースのデバッグ情報を収集するために使用される [デバッグ（debug）] サブメニューは、CLI の `Diagnostic > Tracking` サブコマンドから削除されます。
最初の製造元の値にネットワーク設定をリセット	最後の Reload サブコマンド（ネットワーク設定をリセットする）の実行ステータスを表示する新しいサブコマンド `Reload Status` が `Diagnostic` コマンドに追加されました。 このコマンドの詳細については、ユーザーガイドの「Common Administrative Tasks」の章にある「Diagnostic - Reload command」および「Diagnostic - Reload Status command」のセクションを参照してください。
TLS 通信中のピア証明書の X.509 検証の実行	ピア証明書の X.509 検証を実行するように Secure Email and Web Manager を設定できます。X.509 検証は、次のサービスに適用されます。 • アウトバウンド SMTP • LDAP • アップデータ • TLS を介したアラート • syslog サーバ • スマート ライセンシング サーバー • SSE コネクタ • SSE サーバー 次の方法を使用して、ピア証明書の X.509 検証を設定できます。 • Web インターフェイスの [システム管理（System Administration）] > [SSL 設定（SSL Configuration）] > [SSL 設定（SSL Configuration）] ページに移動します。 • CLI の `sslconfig` コマンドを実行します。 詳細については、ユーザーガイドの「Common Administrative Tasks」の章にある「X.509」のセクションを参照してください。
Secure Email and Web Manager 仮想アプライアンスモデルの新しい RAM 値	AsyncOS 15.0 リリース以降では、KVM または VMWare ESXi を介して展開された M600V Secure Email and Web Manager 仮想アプライアンスモデルに新しい RAM 値があります。 仮想アプライアンスに適用可能な新しい RAM 値の詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。

Microsoft Hyper-V Server 2019 のサポート	Secure Email and Web Manager 15.0 は、Microsoft Hyper-V Server 2019 をサポートします。
Hyper-V の第 2 世代展開のサポート	AsyncOS 15.0 リリース以降では、Secure Email and Web Manager で Hyper-V の第 2 世代展開のみがサポートされます。 （注） Hyper-V 第 2 世代展開でサポートされるモデルは、**M600V** のみです。 Hyper-V の第 2 世代展開のサポートの詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。
Azure プラットフォームでの第 2 世代展開のサポート	AsyncOS 15.0 リリース以降では、Secure Email and Web Manager で Azure プラットフォームでの第 2 世代展開がサポートされます。 （注） Azure 第 2 世代展開でサポートされるモデルは、**M600V** のみです。 （注） 第 2 世代のイメージは、Azure プラットフォームに展開した後に起動しません。第 2 世代のイメージが展開された後、仮想マシンを再起動する必要があります。 Azure プラットフォームでの第 2 世代展開の詳細については、『Cisco Secure Email Virtual Gateway and Cisco Secure Email and Web Manager Virtual on Microsoft on Azure Deployment Guide』を参照してください。
AWS 展開でサポートされるモデル	AsyncOS 15.0 リリース以降、AWS 展開でサポートされるモデルは **M600V** のみです。 詳細については、『Deploying Cisco Secure Email Gateway, Secure Web, and Secure Email and Web Manager Virtual Appliances on Amazon Elastic Compute Cloud on Amazon Web Services Guide』を参照してください。

動作における変更

SSH サーバーとクライアントの設定の変更	[アップグレードのシナリオ] Cisco Secure Email and Web Manager を下位の AsyncOS バージョンから AsyncOS 15.0 バージョン以降にアップグレードする場合は、次の SSH サーバーとクライアントの設定の変更が適用されます。 [非 **FIPS** モードのみ]：Secure Email and Web Manager が FIPS モードでない場合、次の SSH サーバーおよびクライアントの設定の変更が適用されます。 **[SSH サーバー設定の変更]** • 次の暗号アルゴリズム、MAC メソッド、KEX アルゴリズム、およびホストキーアルゴリズムは、デフォルトで Secure Email and Web Manager から削除されます。 – **暗号アルゴリズム**：`rijndael-cbc@lysator.liu.se`、`3des-cbc`、`blowfish-cbc`、`cast128-cbc`、`arcfour`、`arcfour128`、および `arcfour256` – **MAC メソッド**：`hmac-md5`、`umac-64@openssh.com`、`hmac-ripemd160`、`hmac-ripemd160@openssh.com`、`hmac-sha1-96`、`hmac-md5-96` – **KEX アルゴリズム**：`diffie-hellman-group-exchange-sha256`、`diffie-hellman-group-exchange-sha1`、`diffie-hellman-group1-sha1` – **ホストキーアルゴリズム**：`rsa1` • [最小サーバーキーサイズ（Minimum Server Key Size）] オプションは、デフォルトで Secure Email and Web Manager の CLI から削除されます。 • ホストキーアルゴリズム：`rsa-sha2-256` は、デフォルトで Secure Email and Web Manager に追加されます。 [**SSH** クライアント設定の変更] • 次の暗号アルゴリズム：`aes128-gcm@openssh.com` および `aes256-gcm@openssh.com` は、デフォルトで Secure Email and Web Manager に追加されます。 • ホストキーアルゴリズム：`rsa-sha2-256` は、デフォルトで Secure Email and Web Manager に追加されます。

	[SCP プッシュの変更] このリリースより前は、[システム管理（System Administration）] -> [ログサブスクリプション（Log Subscription）] ページで SCP プッシュを設定すると、システムによって `ssh-dss` キーが生成されていました。`ssh-dss` キーは、リモートサーバーにログをプッシュするようにリモートサーバーで設定されていました。 このリリースにアップグレードして FIPS モードを有効にした後、[システム管理（System Administration）] -> [ログサブスクリプション（Log Subscription）] ページで SCP プッシュを設定すると、システムによって `ssh-rsa` キーが生成されます。`ssh-rsa` キーは、リモートサーバーにログをプッシュするようにリモートサーバーで設定される必要があります。 **（注）** Secure Email and Web Manager 15.0 にアップグレードし、FIPS モードを有効にした後、いずれかのログに再度登録して、新しい `ssh-rsa` キーを取得し、リモートサーバーで `ssh-rsa` キーを設定する必要があります。 ログサブスクリプションの詳細については、ユーザーガイドの「Logging」の章にある「Configuring Log Subscriptions」セクションを参照してください。 **[バナーテキストの変更]** [システムアップグレード（System Upgrade）] バナーテキストに、アップグレードプロセス後に暗号、キー、Kex、および MAC の脆弱なアルゴリズムがシステムによって削除されることを通知する注記が追加されます。

[新規インストールシナリオ]

次の SSH サーバー設定の変更は、Cisco Secure Email and Web Manager 用の AsyncOS 15.0 を初めてインストールする場合にのみ適用されます。

[非 **FIPS** モードのみ]：Secure Email and 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-ctr`、`aes192-ctr`、`aes256-ctr`、`aes128-cbc`、`aes192-cbc`、および `aes256-cbc`
- **MAC メソッド**：`hmac-sha1`
- **ホストキーアルゴリズム**：`rsa-sha2-256`、`ssh-rsa`、および `ssh-dss`（デフォルトでは無効）

  （注） CLI で `sshconfig` > `sshd` > `setup` サブコマンドを使用して、`ssh-dss` 暗号アルゴリズムを手動で有効にする必要があります。

- **KEX アルゴリズム**：`diffie-hellman-group14-sha1`、`ecdh-sha2-nistp256`、`ecdh-sha2-nistp384`、および `ecdh-sha2-nistp521`

[**FIPS モードのみ**]：FIPS モードを有効にするには、まず CLI で `sshconfig` > `sshd` > `setup` サブコマンドを使用して、非 FIPS 準拠の次の暗号アルゴリズムおよびホストキーアルゴリズムを無効にします。

- 暗号アルゴリズム：`aes192-ctr`
- ホストキーアルゴリズム：`ssh-rsa`

（注） ホストキーアルゴリズム：`rsa-sha2-256` が新しく追加され、デフォルトで Secure Email and Web Manager で有効になっています。

X.509 証明書の変更	[アップグレードのシナリオ] Secure Email and Web Manger 15.0 以降のバージョンにアップグレードすると、安全性の低い X.509 証明書を削除するか保持するか尋ねられます。 通知メッセージ セキュア管理アプライアンス 15.0.x 以降のバージョンでは、安全性の低い署名アルゴリズムが設定されている x509 証明書があれば削除します。(From Secure Management Appliance 15.0.x and later versions, we will go ahead and delete x509 certificates that have less secure signature algorithm if any configured.)これらの x509 証明書は、GUI ページの [ネットワーク(Network)] -> [証明書(Certificates)]、または CLI ページの certconfig を使用して設定できます。(These x509 certificates can be configured from Network-> Certificates from GUI page and via certconfig from CLI page.) 注:これらの安全性の低い x509 証明書の削除をスキップすることもできますが、推奨されません。(Note: You can still choose to skip deletion of these less secure x509 certificates but it is not recommended.)アップグレードを続行しますか?[y]/[n](Do you want to proceed with the upgrade?[y]/[n]) y 安全性の低い署名アルゴリズムが設定されている場合、x509 証明書の削除をスキップしますか?[n]/[y]:(Do you wish to skip the deletion of x509 certificates with less secure signature algorithm if any configured?[n]/[y]:) N 設定を処理しています... cert-1: Thu Dec 22 13:48:08 2022 getCertDb: Caught exception IOError or OSError(Processing configuration... cert-1: Thu Dec 22 13:48:08 2022 getCertDb: Caught exception IOError or OSError) 設定を処理しています... cert(Processing configuration... cert) 警告:次の x509 証明書は、署名アルゴリズムの安全性が低いため削除されます。(WARNING: The following x509 certificates are deleted because their signature algorithm is less secure.): ['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP']
	[新規インストールシナリオ] 次の X.509 証明書用署名アルゴリズムの変更は、Cisco Secure Email and Web Manager 用の AsyncOS 15.0 を初めてインストールする場合にのみ適用されます。 • x509 証明書の次の署名アルゴリズムは、サポートされなくなりました:`sha1withrsaencryption`、`dsawithsha1`、`sha224withrsaencryption`、`ecdsa-with-sha1`、`ecdsa-with-sha224`、`md2withrsaencryption`、`md4withrsaencryption`、`md5withrsaencryption`、`ripemd128withrsaencryption`、`ripemd160withrsaencryption`、および `ripemd256withrsaencryption`。 • ECDSA 署名アルゴリズムを持つ x509 証明書の以下の曲線はサポートされていません:`secp224r1`、`secp192r1`、`brainpoolP160r1`、`brainpoolP192r1`、`secp160r1`、`secp160r2`、`secp192k1`、`secp224k1`、`secp256k1`、`sect163k1`、`sect163r2`、`sect193r1`、`sect193r2`、`sect233k1`、`sect233r1`、`sect239k1`、`sect283k1`、`sect283r1`、`sect409k1`、`sect409r1`、`sect571k1`、および `sect571r1`.

X.509 証明書の変更	[証明書のアップロードシナリオ] 安全性の低い署名アルゴリズムを使用して X.509 証明書をアップロードすると、ABC アルゴリズムを使用した X.509 証明書の安全性が低いことを示すエラーメッセージが表示されます。 エラー メッセージ エラー:ripemd160WithRSA ダイジェストを使用した x509 証明書は低い安全性です。(Error: The x509 certificates with ripemd160WithRSA digest are less secure.)
	[構成ファイルのロードシナリオ] **CLI を使用した構成ファイルのロード** CLI を使用して構成ファイルをロードすると、安全性の低い署名アルゴリズムを使用した X.509 証明書が削除されるという警告が表示されます。 警告メッセージ 警告:次の x509 証明書は、署名アルゴリズムの安全性が低いため削除されます:['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP']。(WARNING: The following x509 certificates are deleted because their signature algorithm is less secure: ['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP'].) **GUI を使用した構成ファイルのロード** GUI を使用して構成ファイルをロードすると、安全性の低い署名アルゴリズムを使用した X.509 証明書が削除されるという警告が表示されます。 警告メッセージ 警告:次の x509 証明書は、署名アルゴリズムの安全性が低いため削除されます:['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP']。(Warnings: The following x509 certificates are deleted because their signature algorithm is less secure: ['SMTP Outbound', 'HTTPS', 'SMTP Inbound', 'LDAP'].)
最初の製造元の値にネットワーク設定をリセット	このリリースより前は、Diagnostic > Reload サブコマンドを使用して、すべてのユーザー設定を削除し、デバイス全体をリセットしていました。 このリリースにアップグレードした後、以前の機能とともに、このサブコマンドはネットワーク設定を最初の製造元の値にリセットします。
JWT トークン:エラーメッセージの変更	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。 このリリースにアップグレードした後は、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す。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。

SPoG 機能の変更	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。 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。 （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。
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。 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。
Secure Email and Web Manager と syslog サーバー間の通信で TLSv1.0 のサポートなし	このリリース以前は、Secure Email and Web Manager は、syslog サーバーで有効になっている TLS バージョンに関係なく、TLSv1.0 を使用して syslog サーバーと通信していました。 このリリース以降、Secure Email and Web Manager は、syslog サーバーで有効になっている最も高い TLS バージョンを使用します。たとえば、syslog サーバーの最も高い TLS バージョンが 1.2 の場合、Secure Email and Web Manager は TLSv1.2 を使用して syslog サーバーと通信します。 （注） TLSV1.0 は、安全でない TLS 方式であるため、現在はサポートされていません。
Syslog ディスクバッファサイズの警告メッセージ	このリリース以降、Secure Email and Web Manager 14.2 リリースから Secure Email and Web Manager 15.0 リリースにアップグレードすると、syslog ディスクバッファサイズが 10 GB に設定され、syslog ディスクバッファデータのサイズが 1 GB を超えている場合、Secure Email and Web Manager の CLI および Web インターフェイスに警告メッセージが表示されます。 警告メッセージを無視してアップグレードプロセスを続行することも、アップグレードを中止することもできます。アップグレードプロセスを中止する場合は、Secure Email and Web Manager を syslog サーバーに接続し、syslog ディスクバッファデータをドレインしてから、アップグレードプロセスを実行できます。

フェーズ 2 バックアッププロセスの通知メッセージ	このリリース以前は、フェーズ 2 バックアッププロセスのサービスタスクが進行中で、完了までに 2 時間を超えた場合、管理者に通知メッセージが送信されませんでした。 このリリースにアップグレードした後、フェーズ 2 バックアッププロセスでサービスタスクが進行中で、完了までに 2 時間を超える場合、バックアッププロセスのステータスと、完了までに時間がかかるサービス名を知らせる通知メッセージが管理者に送信されます。
[タイムゾーン（Time Zone）] -> [国（Country）] フィールドの変更	このリリース以降、[タイムゾーン（Time Zone）] -> [国（Country）] フィールドで使用可能な [米国（United States）] オプションは、[アメリカ合衆国（United States of America）] に変更されました。

新しい Web インターフェイスへのアクセス

（注） 次世代のユーザーインターフェイスは、Trailblazer が有効になっている場合に最適なため、Trailblazer を有効にして新しいインターフェースにアクセスすることをお勧めします。

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 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、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るようになりました。

- `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。

アップグレード パス

- リリース 15.0.0-334 へのアップグレード（一般導入）（15 ページ）
- リリース 15.0.0-333 へのアップグレード（限定導入）更新（15 ページ）
- リリース 15.0.0-317 へのアップグレード（限定導入）（15 ページ）

リリース 15.0.0-334 へのアップグレード（一般導入）

次のバージョンからリリース 15.0.0-334 にアップグレードできます。

- 14.3.0-120
- 14.3.0-124
- 14-3-0-126
- 14.2.0-203
- 14.2.0-212
- 14.2.0-217
- 14.2.0-224

リリース 15.0.0-333 へのアップグレード（限定導入）更新

次のバージョンからリリース 15.0.0-333 にアップグレードできます。

- 15.0.0-317
- 14.3.0-120
- 14.3.0-124
- 14-3-0-126
- 14.2.0-203
- 14.2.0-212
- 14.2.0-217
- 14.2.0-224

リリース 15.0.0-317 へのアップグレード（限定導入）

次のバージョンからリリース 15.0.0-317 にアップグレードできます。

- 14.2.0-203
- 14.2.0-212
- 14.2.0-217
- 14.2.0-224
- 14.3.0-120
- 14.3.0-124
- 14.3.0-126
- 15.0.0-281

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

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（22 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

（注） M600V 仮想アプライアンスの RAM サイズが 8 GB から 16 GB に増加しました。仮想アプライアンスがこの要件を満たしていない場合は、アラートが表示されます。

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（16 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（17 ページ）
- 既存の設定のバックアップ（17 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（18 ページ）
- 既存のデータベースのバックアップ（18 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（16 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 Secure Email and Web Manager 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 15.0 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 Secure Email and Web Manager を AsyncOS 15.0 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 Secure Email and Web Manager 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 Secure Email and Web Manager User Guide』を参照してください。

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（17 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（17 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。
  - スパムの隔離、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。

アップグレード後の要件

アップグレード後に次の重要なタスクを実行します。

- スパム通知 URL の変更（20 ページ）
- 次期 AsyncOS リリースにおけるシスコ スマート ソフトウェア ライセンシングの必須使用（20 ページ）

スパム通知 URL の変更

Cisco Secure Email and Web Manager 15.0 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。

次期 AsyncOS リリースにおけるシスコ スマート ソフトウェア ライセンシングの必須使用

Cisco Secure Email and Web Manager の次の AsyncOS リリース（AsyncOS 15.0 リリース以降のすべてのリリース）から、シスコ スマート ソフトウェア ライセンシングを使用する必要があります。

（注） 次の AsyncOS リリースから、クラシックライセンスはサポートされなくなります。クラシックライセンスモードでは、新しい機能ライセンスを注文したり、既存の機能ライセンスを更新したりすることはできなくなります。

前提条件：Cisco Smart Software Manager ポータルでスマートアカウントを作成し、Cisco Secure Email and Web Manager でシスコ スマート ソフトウェア ライセンシングを有効にしてください。詳細については、ユーザーガイドの「Common Administrative Tasks」の章にある「Smart Software Licensing」のセクションを参照してください。

結果：シスコ スマート ソフトウェア ライセンシングを有効にすると、Cisco Secure Email and Web Manager を AsyncOS 15.0 から次期 AsyncOS リリースにシームレスにアップグレードし、スマートライセンスモードで既存の機能ライセンスを引き続き使用できます。

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問題に関する情報を検索します。

- バグ検索ツールの要件 (21 ページ)
- 既知および修正済みの問題のリスト (21 ページ)
- 既知および解決済みの問題に関する情報の検索 (22 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=15.0.0&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=15.0.0&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(15.0 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 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
Cisco Secure Web Appliance	http://www.cisco.com/c/ja_jp/support/security/web-security-appliance/tsd-products-support-series-home.html
Cisco Secure 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

Cisco Secure 製品のマニュアル:	入手場所
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。