ハイブリッド SWG を備えた AsyncOS 14.6 for Cisco Secure Web Appliance リリースノート

初版：2023 年 5 月 11 日

Secure Web Appliance について

Cisco Secure Web Appliance はインターネットトラフィックを代行受信してモニターし、ポリシーを適用することによって、マルウェア、機密データの漏洩、生産性の低下などのインターネットベースの脅威から内部ネットワークを保護します。

最新情報

- AsyncOS 14.6.0-108（限定導入）の新機能 （1 ページ）

AsyncOS 14.6.0-108（限定導入）の新機能

このリリースでは次の機能が導入されました。

<table>
<tr><th>機能</th><th colspan="2">説明</th></tr>
<tr><td>Cisco Umbrella</td><td colspan="2">AsyncOS 14.6 は、Cisco Secure Web Appliance（SWA）を備えた Cisco Umbrella をサポートします。Cisco Umbrella と Cisco Secure Web Appliance の統合により、Cisco Umbrella から Cisco Secure Web Appliance への共通 Web ポリシーの展開が容易になります。

Cisco Secure Web Appliance に対する Cisco Umbrella の管理対象プロファイルを編集または削除することはできません。名前の先頭に「umbrella<space>」が付いたプロファイルまたはポリシーを作成することはできません。例：umbrella abc。

Cisco Umbrella のポリシー規則のシーケンスは、Cisco Secure Web Appliance へのポリシー変換中に保持されます。

Cisco Umbrella Web ポリシーの AD ユーザーまたは AD グループは、ポリシーメンバー定義セクションの [選択されたグループおよびユーザー（Selected Groups and Users）] として Cisco Secure Web Appliance ポリシーで設定する必要があります。

統合が成功すると、次の Web ポリシーが変換され、Cisco Umbrella から Cisco Secure Web Appliance にプッシュされます。

<table><tr><th>Cisco Umbrella から</th><th>Cisco Secure Web Appliance へ</th></tr><tr><td>ルールセット アイデンティティ</td><td>グローバル識別プロファイル</td></tr><tr><td>接続先リスト</td><td>カスタムおよび外部 URL カテゴリ</td></tr><tr><td>Web ポリシー（ルール）</td><td>アクセスポリシー</td></tr><tr><td>HTTPS 検査</td><td>復号ポリシー</td></tr><tr><td>Microsoft 365 の互換性</td><td>カスタムおよび外部 URL カテゴリ</td></tr><tr><td>ルールセットのブロックページ設定</td><td>ユーザ通知</td></tr></table>
ユーザーガイドの「Integrate Cisco Secure Web Appliance with Cisco Umbrella」の項を参照してください。</td></tr>
</table>

前提条件

このリリースには次の前提条件があります。

- Umbrella ハイブリッドサービスに正常に接続するには、SWA でシスコの信頼されたルート証明書バンドル：2.2 を更新する必要があります。
- SWA で Umbrella サービスからのポリシープッシュを正常に設定するには、SWA の 107 の URL カテゴリを更新する必要があります。
- SWA で HTTPS プロトコルを手動で有効にする必要があります。

- AD が Umbrella と統合されている場合、SWA で AD レルムを手動で設定する必要があります。
- SWA をハイブリッドポリシー機能と統合するには、アクティブな Umbrella Web ポリシーライセンスが必要です。

新しい Web インターフェイスへのアクセス

新しい Web インターフェイスは、モニタリング レポートとトラッキング Web サービスの新しい外観を提供します。新しい Web インターフェイスには次の方法でアクセスできます。

- レガシー Web インターフェイスにログインし、[Secure Web Appliance をクリックして新しい外観を試してみてください（Secure Web Appliance is getting a new look. Try it!!）] のリンクをクリックします。このリンクをクリックすると、Web ブラウザの新しいタブが開き、`https://wsa01-enterprise.com:<trailblazer-https-port>/ng-login` に移動します。ここでは、`wsa01-enterprise.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` は、新しい Web インターフェイスにアクセスするためにアプライアンスに設定されている TRAILBLAZER HTTPS ポートです。

重要

- アプライアンスのレガシー Web インターフェイスにログインする必要があります。
- 指定したアプライアンスのホスト名を DNS サーバが解決できることを確認します。
- デフォルトでは、新しい Web インターフェイスでは、TCP ポート 6080、6443、および 4431 が動作可能である必要があります。これらのポートがエンタープライズ ファイアウォールでブロックされていないことを確認します。
- 新しい Web インターフェイスにアクセスするためのデフォルト ポートは 4431 です。これは、**trailblazerconfig** CLI コマンドを使用してカスタマイズできます。**trailblazerconfig** CLI コマンドの詳細については、ユーザガイドの「コマンドライン インターフェイス」の章を参照してください。
- 新しい Web インターフェイスでは、HTTP および HTTPS の AsyncOS API（モニタリング）ポートも必要です。デフォルトでは、これらのポートは 6080 および 6443 です。AsyncOS API（モニタリング）ポートは、**interfaceconfig** CLI コマンドを使用してカスタマイズすることもできます。**Interfaceconfig** CLI コマンドの詳細については、ユーザ ガイドの「コマンドライン インターフェイス」の章を参照してください。

これらのデフォルトポートを変更した場合は、新しい Web インターフェイスのカスタマイズされたポートがエンタープライズ ファイアウォールでブロックされていないことを確認します。

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 11.8 以降）にアクセスすることをお勧めします。

- Google Chrome
- Mozilla Firefox

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 11.8 以降）でサポートされている解像度は、1280x800 ～ 1680x1050 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。

リリースの分類

各リリースは、リリースのタイプ（ED：初期導入、GD：全面導入など）によって識別されています。これらの用語の説明については、http://www.cisco.com/c/dam/en/us/products/collateral/security/web-security-appliance/content-security-release-terminology.pdfを参照してください。

このリリースでサポートされているハードウェア

このビルドは、サポートされている既存のすべてのプラットフォーム上でのアップグレードに使用できますが、拡張パフォーマンスのサポートは次のハードウェアモデルでのみ使用できます。

- Sx90/F
- Sx95/F

仮想モデル：

- S100v
- S300v

  システムの CPU およびメモリ要件は、12.5 リリース以降で変更されています。詳細については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。
- S600v
- S1000v

（注） アプライアンスに付属の Cisco SFP を使用します。

アップグレードパス

AsyncOS 14.6.0-108 へのアップグレード （5 ページ）

AsyncOS 14.6.0-108 へのアップグレード

次のバージョンから Cisco Web セキュリティアプライアンス向け AsyncOS リリース 14.6.0-108 にアップグレードできます。

（注） アップグレード中は、デバイス（キーボード、マウス、管理デバイス（Raritan）など）をアプライアンスの USB ポートに接続しないでください。

- 12.5.1-043
- 12.5.5-008
- 14.0.1-053
- 14.0.4-005
- 14.5.0-537
- 14.5.1-016
- 14.6.0-081

アップグレード後の要件

アプライアンスを Cisco Threat Response に登録していない場合は、14.6.0-108 にアップグレードした後で次の手順を実行する必要があります。

手順

ステップ 1 管理者アクセス権を使用して、Cisco Threat Response ポータルでユーザアカウントを作成します。

新しいアカウントを作成するには、URL：https://visibility.amp.cisco.com を使用して Cisco Threat Response ポータルにログインし、[Cisco セキュリティアカウントの作成（Create a Cisco Security Account）] をクリックします。新しいユーザ アカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。

ステップ 2 アプライアンスを Security Services Exchange（SSE）クラウドポータルに登録するには、自身の地域に対応する SSE ポータルからトークンを生成します。

SSE クラウドポータルへの登録時に、アプライアンスの Web ユーザインターフェイスから、地域に基づいて次の FQDN を選択します。

- 米国（api-sse.cisco.com）
- 欧州（api.eu.sse.itd.cisco.com）
- APJC（api.apj.sse.itd.cisco.com）

ステップ 3 Security Services Exchange ポータルのクラウドサービスにある Cisco Threat Response が有効になっていることを確認します。アプライアンスを Security Services Exchange ポータルに登録するには、FQDN api-sse.cisco.com（米国）のファイアウォールの HTTPS（インとアウト）443 ポートが開いていることを確認します。

仮想アプライアンスの展開については、『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、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

互換性の詳細

- セキュリティ管理のための Cisco AsyncOS との互換性 （6 ページ）
- クラウド コネクタ モードでの IPv6 と Kerberos は使用不可 （6 ページ）
- IPv6 アドレスの機能サポート （7 ページ）
- アップグレード後の要件 （5 ページ）

セキュリティ管理のための Cisco AsyncOS との互換性

Cisco コンテンツ セキュリティ管理リリース向け AsyncOS とこのリリースとの互換性については、http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-release-notes-list.html にある互換性のマトリックスを参照してください。

（注） このリリースは、現在使用可能なセキュリティ管理リリースと互換性がなく、使用することはできません。互換性のあるセキュリティ管理リリースは間もなく利用可能になります。

クラウド コネクタ モードでの IPv6 と Kerberos は使用不可

アプライアンスがクラウド コネクタ モードで設定されている場合、Web インターフェイスのページに「IPv6 アドレスと Kerberos 認証用のオプションは使用できません（unavailable options for IPv6 addresses and Kerberos authentication）」と表示されます。使用できるように見えても、それらのオプションはクラウド コネクタ モードではサポートされていません。クラウド コネ

クタ モードでは、IPv6 アドレスまたは Kerberos 認証を使用するようにアプライアンスを設定しようとしないでください。

IPv6 アドレスの機能サポート

IPv6 アドレスをサポートする特性と機能は次のとおりです。

- コマンド ラインと Web インターフェイス。アプライアンスにアクセスするには、http://[2001:2:2::8]:8080 または https://[2001:2:2::8]:8443 を使用します。
- IPv6 データ トラフィックでのプロキシ アクションの実行（HTTP/HTTPS/SOCKS/FTP）
- IPv6 DNS サーバ
- WCCP 2.01（Cat6K スイッチ）とレイヤ 4 透過リダイレクション
- アップストリーム プロキシ
- 認証サービス
  - Active Directory（NTLMSSP、Basic、および Kerberos）
  - LDAP
  - SaaS SSO
  - CDA による透過的ユーザ識別（CDA との通信は IPv4 のみ）
  - クレデンシャルの暗号化
- Web レポートと Web トラッキング
- 外部 DLP サーバ（アプライアンスと DLP サーバ間の通信は IPv4 のみ）
- PAC ファイル ホスティング
- プロトコル：管理サーバを介した NTP、RADIUS、SNMP、および syslog

IPv4 アドレスを必要とする特性と機能は次のとおりです。

- 内部 SMTP リレー
- 外部認証
- ログ サブスクリプションのプッシュ方式：FTP、SCP、および syslog
- NTP サーバ
- ローカル アップデート サーバ（アップデート用のプロキシ サーバを含む）
- 認証サービス
- AnyConnect セキュア モビリティ
- Novell eDirectory 認証サーバ
- エンドユーザ 通知のカスタム ロゴのページ

- Web セキュリティアプライアンスとセキュリティ管理アプライアンス間の通信
- 2.01 より前の WCCP バージョン
- SNMP

アップグレード後の要件

アプライアンスを Cisco Threat Response に登録していない場合は、14.6.0-108 にアップグレードした後で次の手順を実行する必要があります。

手順

ステップ 1 管理者アクセス権を使用して、Cisco Threat Response ポータルでユーザアカウントを作成します。

新しいアカウントを作成するには、URL：https://visibility.amp.cisco.com を使用して Cisco Threat Response ポータルにログインし、[Cisco セキュリティアカウントの作成（Create a Cisco Security Account）] をクリックします。新しいユーザ アカウントを作成できない場合は、Cisco TAC に連絡してサポートを受けてください。

ステップ 2 アプライアンスを Security Services Exchange（SSE）クラウドポータルに登録するには、自身の地域に対応する SSE ポータルからトークンを生成します。

SSE クラウドポータルへの登録時に、アプライアンスの Web ユーザインターフェイスから、地域に基づいて次の FQDN を選択します。

- 米国（api-sse.cisco.com）
- 欧州（api.eu.sse.itd.cisco.com）
- APJC（api.apj.sse.itd.cisco.com）

ステップ 3 Security Services Exchange ポータルのクラウドサービスにある Cisco Threat Response が有効になっていることを確認します。アプライアンスを Security Services Exchange ポータルに登録するには、FQDN api-sse.cisco.com（米国）のファイアウォールの HTTPS（インとアウト）443 ポートが開いていることを確認します。

仮想アプライアンスの展開については、『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、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

仮想アプライアンスの展開

仮想アプライアンスの展開については、『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、

http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html から入手できます。

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

手順

ステップ 1 アップグレード後の要件（5ページ）で説明されているマニュアルを使用して、このAsyncOSリリースで仮想アプライアンスをセットアップします。

（注） セキュリティサービスの更新が成功したことを確認します。

ステップ 2 ハードウェア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ハードウェア アプライアンスから設定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設定ファイルをロードします。

ハードウェアと仮想アプライアンスのIPアドレスが異なる場合は、設定ファイルをロードする前に、[ネットワーク設定のロード（Load Network Settings）]を選択解除します。

ステップ 5 変更を保存します。

ステップ 6 [ネットワーク（Network）]>[認証（Authentication）]に移動し、ドメインに再度参加します。そうしないと、アイデンティティは機能しません。

AsyncOS for Web のアップグレード

始める前に

- RAIDコントローラ ファームウェアの更新を含むアップグレード前の要件を実行します。
- 管理者としてログインします。

手順

ステップ 1 [システム管理（System Administration）]>[構成ファイル（Configuration File）]ページで、Secure Web Applianceから XML 構成ファイルを保存します。

ステップ 2 [システム管理（System Administration）]>[システムアップグレード（System Upgrade）]ページで、[アップグレードオプション（Upgrade Options）]をクリックします。

ステップ 3 [ダウンロードとインストール（Download and install）]または[ダウンロードのみ（Download only）]のいずれかを選択できます。

使用可能なアップグレードのリストから選択します。

ステップ 4 [続行（Proceed）]をクリックします。

[ダウンロードのみ（Download only）] を選択した場合は、アップグレードがアプライアンスにダウンロードされます。

ステップ 5 [ダウンロードとインストール（Download and install）] を選択した場合は、アップグレードが完了したら、[今すぐリブート（Reboot Now）] をクリックして、Cisco Secure Web Appliance をリブートします。

（注） ブラウザがアップグレードしたバージョンの AsyncOS に新しいオンライン ヘルプのコンテンツをロードすることを確認するには、ブラウザを終了してから開いてオンライン ヘルプを表示します。これにより、期限切れのコンテンツのブラウザ キャッシュがクリアされます。

重要：アップグレード後に必要なアクション

アップグレード後にアプライアンスが正常に機能し続けるようにするには、次の事項に対処する必要があります。

- シスコが推奨する暗号スイートへのデフォルト プロキシ サービス暗号スイートの変更
- 仮想アプライアンス：SSH セキュリティ脆弱性の修正に必要な変更
- ファイル分析：クラウドで分析結果の詳細を表示するために必要な変更
- ファイル分析：分析対象のファイル タイプの確認
- 正規表現のエスケープされていないドット

シスコが推奨する暗号スイートへのデフォルト プロキシ サービス暗号スイートの変更

AsyncOS 9.1.1 以降では、プロキシサービスに使用可能なデフォルトの暗号スイートは、セキュアな暗号スイートのみを含むように変更されます。

ただし、AsyncOS 9.x.x 以降のリリースからアップグレードする場合、デフォルトのプロキシサービスの暗号スイートは変更されません。セキュリティを強化するために、アップグレード後に、デフォルトのプロキシサービス暗号スイートをシスコが推奨する暗号スイートに変更することをお勧めします。次の手順を実行します。

手順

ステップ 1 Web インターフェイスを使用してアプライアンスにログインします。

ステップ 2 [システム管理（System Administration）] > [SSL設定（SSL Configuration）] をクリックします。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 [プロキシサービス（Proxy Services）] で、[使用する暗号（CIPHER(s) to Use）] フィールドを次のフィールドに設定します。

```
EECDH:DSS:RSA:!NULL:!eNULL:!aNULL:!EXPORT:!3DES:!SEED:!CAMELLIA:!SRP:!IDEA:!DHE-DSS-AES256-SHA:!AES256-SHA:DHE-RSA-AES128-SHA:TLS_AES_256_GCM_SHA384
```

注意 上記の文字列を改行またはスペースを含まない単一の文字列として貼り付けてください。

ステップ 5 変更を送信し、保存します。

CLI で **sslconfig** コマンドを使用して、上記の手順を実行することもできます。

仮想アプライアンス：SSH セキュリティ脆弱性の修正に必要な変更

このセクションの要件は AsyncOS 8.8 で導入されました。

次のセキュリティ脆弱性は、アプライアンスに存在する場合、アップグレード中に修正されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport

（注） このパッチは、2015 年 6 月 25 日より前にダウンロードまたはアップグレードされた仮想アプライアンス リリースにのみ必要です。

アップグレード前にこの問題を修正しなかった場合は、修正されたことを示すメッセージがアップグレード中に表示されます。このメッセージが表示された場合、アップグレード後にアプライアンスを完全な動作順序に戻すには次のアクションを実行する必要があります。

- SSH ユーティリティの既知のホスト リストから、アプライアンスの既存のエントリを削除します。その後、アプライアンスに SSH 接続し、新しいキーを使用して接続を受け入れます。
- SCP プッシュを使用して、リモート サーバ（Splunk を含む）にログを転送する場合は、リモート サーバからアプライアンスの古い SSH ホスト キーをクリアします。
- 展開に Cisco コンテンツ セキュリティ管理アプライアンスが含まれている場合は、そのアプライアンスのリリース ノートに記載されている重要な手順を参照してください。

ファイル分析：クラウドで分析結果の詳細を表示するために必要な変更

複数のコンテンツ セキュリティ アプライアンス（Web、電子メール、または管理）を展開しており、組織内の任意のアプライアンスからアップロードされたすべてのファイルについてクラウド内の詳細なファイル分析結果を表示する場合は、アップグレード後に各アプライアンスでアプライアンス グループを設定する必要があります。アプライアンス グループを設定するには、ユーザ ガイド（PDF）の「File Reputation Filtering and File Analysis」の章を参照してください（この PDF は AsyncOS 8.8 のオンライン ヘルプよりも最新です）。

ファイル分析：クラウドで分析結果の詳細を表示するために必要な変更

複数のコンテンツ セキュリティ アプライアンス（Web、電子メール、または管理）を展開しており、組織内の任意のアプライアンスからアップロードされたすべてのファイルについてクラウド内の詳細なファイル分析結果を表示する場合は、アップグレード後に各アプライアンス

でアプライアンス グループを設定する必要があります。アプライアンス グループを設定するには、ユーザ ガイド（PDF）の「File Reputation Filtering and File Analysis」の章を参照してください（この PDF は AsyncOS 8.8 のオンライン ヘルプよりも最新です）。

ファイル分析：分析対象のファイル タイプの確認

AsyncOS 8.8 でファイル分析クラウド サーバの URL が変更されました。その結果、分析可能なファイル タイプがアップグレード後に変更された可能性があります。変更がある場合は、アラートが表示されます。分析用に選択したファイルタイプを確認するには、[セキュリティ サービス（Security Services）] > [マルウェア対策およびレピュテーション（Anti-Malware and Reputation）] を選択し、Advanced Malware Protection の設定を確認します。 >

正規表現のエスケープされていないドット

正規表現のパターンマッチング エンジンにアップグレードすると、システムの更新後に既存のパターン定義でエスケープされていないドットに関するアラートが表示されることがあります。ドットの後に 64 文字以上を返すパターン内のエスケープされていないドットは、Velocity パターンマッチング エンジンによって無効化されます。その影響についてのアラートがユーザーに送信され、パターンを修正または置換するまで、更新のたびにアラートは送信され続けます。一般に、長い正規表現内のエスケープされていないドットは問題を引き起こす可能性があるため、避ける必要があります。

マニュアルの更新

Web サイト（www.cisco.com）にあるユーザ ガイドは、オンライン ヘルプよりも最新である場合があります。この製品のユーザ ガイドとその他のドキュメントを入手するには、オンライン ヘルプの [PDFの表示（View PDF）] ボタンをクリックするか、「関連資料 （16 ページ）」に示す URL にアクセスしてください。

既知および修正済みの問題

- バグ検索ツールの要件
- 既知および修正済みの問題のリスト
- 既知および解決済みの問題に関する情報の検索

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

- 修正済みの問題
- 既知の問題

既知および解決済みの問題に関する情報の検索

Cisco Bug Search Tool を使用して、既知および解決済みの不具合に関する現在の情報を検索します。

始める前に

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://tools.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）] > [Webセキュリティ（Web Security）] > [Cisco Webセキュリティアプライアンス（Cisco Web Security Appliance）] > [Cisco Secure Web Appliance] をクリックし、[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（x.x.x 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、[リリース（Releases）] 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、[リリース（Releases）] 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。

既知の動作

このリリースでは、次の既知の制限事項があります。

- デフォルトでは、Secure Web Appliance（SWA）の Umbrella 設定のソースインターフェイスは [管理（Management）] に設定されています。ソースインターフェイスを [データ（Data）] に変更するには、ハイブリッドポリシーを有効にする前に、変更を送信してコミットする必要があります。

- 変換は、ルールアクションの[許可（Allow）]、[ブロック（Block）]、および[警告（Warn）]でサポートされています。
- 変換は、コンテンツカテゴリと接続先リストでサポートされています。
- AD ユーザー、AD グループ、およびパブリックネットワークに関連付けられた内部ネットワークの変換がサポートされています。
- SWA では、1 つのグローバルな Umbrella がプッシュした識別プロファイルが常に使用可能です。
- SWA 管理者によって設定されたポリシーは、Umbrella からのポリシープッシュの後に最優先に移行されます。
- Umbrella で設定されたポリシーは、Umbrella の下に登録されているすべての SWA にプッシュされます。
- Umbrella によってプッシュされた復号ポリシーでは、WBRS は無効になります。
- Umbrella によってプッシュされた復号ポリシーは、デフォルトでは [複合（Decrypt）] アクションに設定されています。
- [エンドユーザー通知（End-User Notification）] ページは、グローバル設定として SWA で常に有効になります。
- SWA では、[エンドユーザー通知（End-User Notification）] ページは、Umbrella の最初のルールセットで最初に選択されたブロックページにのみ設定されます。
- 最初のルールセットの選択されたブロックページの外観の変更は、3 時間ごとに変換されます。
- Umbrella によってプッシュされた識別プロファイルと顧客カテゴリでは、これらのプロファイルまたはカテゴリが Umbrella から削除されると、管理者が設定したポリシーは SWA 側から無効になります。
- Umbrella ORG への SWA 登録は、特定の ORG に割り当てられたシート数に制限されています。これは、Umbrella ユーザーインターフェイスの次のパスに表示されます：[管理者（Admin）] > [ライセンス（Licensing）] > [シート数（Number of seats）]。
- SWA が Umbrella ORG に登録されている場合は、SMA ポリシーを SWA にプッシュできません。
- Umbrella に統合された内部ネットワークと AD がない場合、Umbrella はプロファイル、ポリシー、およびカスタム URL カテゴリを SWA にプッシュできません。
- 登録およびハイブリッドサービスの有効化に使用された API キーが期限切れの場合、Umbrella でハイブリッドポリシーまたは登録された SWA を再度有効にするまで、接続が閉じられません。
- 次のルールは変換でサポートされていません：アプリケーション設定、ルールスケジュール、および保護されたバイパス。

- SWA が Umbrella によって管理されている場合、SWA にプッシュされた SMA ポリシーは受け入れられません。
- 設定の保存と読み込みの機能が、Umbrella の設定では機能しません。
- 次のルールセット設定では、変換はサポートされていません。
  - ルールセット アイデンティティ - Chromebook、G Suite OU、G Suite ユーザー、トンネル、ローミングコンピュータ、内部ネットワークのすべてのトンネル
  - テナント制御
  - ファイル分析
  - ファイルタイプ制御
  - HTTPS インスペクション - 選択的復号リストのアプリケーションのみ
  - PAC ファイル
  - SafeSearch
  - ルールセットロギング
  - SAML
  - セキュリティ設定

既知の制限事項

このリリースでは、次の既知の制限事項があります。

- 次のシナリオで、ポリシー変換がトリガーされません。
  - ルールセットの名前の変更。
  - ルールで選択された接続先リストの名前の変更。
  - HTTP インスペクション中に選択された選択的復号リストの名前の変更。
  - HTTPS インスペクションに使用される選択的復号リストのカテゴリの追加または削除。
  - HTTPs インスペクションでの、カテゴリのみを含む選択的復号リストの選択。
  - ルールセットまたはルールの AD ユーザーまたはグループの追加または削除。
  - Umbrella ダッシュボードの AD の統合または削除。
- ルールセット アイデンティティが複数のルールセットで同じである場合、同じアイデンティティの最初のルールセットのみが、一貫して HTTPS インスペクション設定を変換します。

- エンドユーザー通知の [カスタムURLへのリダイレクト（Redirect to Custom URL）] テキストボックスの形式で、整形式のホスト名または IPV4 アドレスのみがサポートされます。Umbrella のブロックページで構成された他の URL 形式を SWA にプッシュすると、ポリシープッシュが失敗し、次のエラーメッセージが表示されます：「http/httpsのURLは適切なホスト名またはIPv4アドレスで構成されていなければなりません。任意でポート番号を含めることはできますが、クエリ文字列（'?...'）は含めないでください。'コード' : '400'、'説明' : '400 = 不正なリクエスト構文またはサポートされていないメソッド'。（An http/https URL must consist of a well-formed hostname or IPv4 address, may optionally include a port, but may not contain a querystring ('?...').'.", 'code': '400', 'explanation': '400 = Bad request syntax or unsupported method.'）」
- ルールセットで AD グループが選択されていて、ルールが一致しない場合、そのルールに対してアクセスポリシーが作成されません。
- Umbrella から Secure Web Appliance（SWA）にプッシュされる復号ポリシーについて、選択的復号リストで選択されたカテゴリとドメインがパススルーに設定されます。定義済みおよびカスタムの URL カテゴリの場合、SWA でアクセスポリシーは適用されませんが、ルールは Umbrella の同じ設定に適用されます。
- Umbrella で Microsoft 365 互換性が有効になっている場合、Umbrella から SWA にプッシュされる復号ポリシーがパススルーに設定されます。その結果、Microsoft 365 エンドポイントのすべてのカテゴリでパススルーが有効になります。
- 信頼できる AD が WSA で設定されておらず、この AD に対して Umbrella レベルでグループが選択されている場合、WSA レベルで設定する必要があることを示すエラーメッセージが表示されます。
- ルールセットとルールで異なるマスクを持つネットワークが選択されている場合、変換はサポートされません。

関連資料

資料	参照先
Cisco Secure Web Appliance ユーザーガイド	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html
シスコのコンテンツセキュリティ管理アプライアンスユーザーガイド	https://www.cisco.com/c/en/us/support/security/content-security-management-appliance/series.html
仮想アプライアンスインストールガイド	https://www.cisco.com/c/en/us/support/security/email-securityappliance/products-installation-guides-list.html

資料	参照先
Secure Web Appliance のリリースノート、ISE 互換性マトリックス、および暗号	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html
Cisco Secure Email and Web Manager と Cisco Secure Web Appliance の互換性マトリックス	https://www.cisco.com/c/dam/en/us/td/docs/security/security_management/sma/sma_all/web-compatibility/index.html
API ガイド	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-programming-reference-guides-list.html
Umbrella との Secure Web Appliance の統合	https://docs.umbrella.com/umbrella-user-guide/docs/umbrella-integration-with-secure-web-appliance

サポート

シスコサポートコミュニティ

シスコサポートコミュニティは、シスコのお客様、パートナー、および従業員向けのオンラインフォーラムです。Webセキュリティに関する一般的な問題や、特定のシスコ製品に関する技術情報について話し合う場を提供します。このフォーラムにトピックを投稿して質問したり、他のシスコユーザーと情報を共有したりできます。

Webセキュリティと関連管理については、シスコサポートコミュニティにアクセスしてください。

https://supportforums.cisco.com/community/5786/web-security

カスタマー 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：http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html [英語] を参照してください。

従来の IronPort のサポートサイト：http://www.cisco.com/web/services/acquisitions/ironport.html [英語] を参照してください。

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。

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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。

翻訳について
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。