



製品およびリリースの概要

この章で説明する内容は、次のとおりです。

- [Web セキュリティアプライアンス の概要 \(1 ページ\)](#)
- [AsyncOS 14.1 の新機能 \(2 ページ\)](#)
- [関連項目 \(2 ページ\)](#)
- [アプライアンス Web インターフェイスの使用 \(2 ページ\)](#)
- [サポートされる言語 \(7 ページ\)](#)
- [Cisco SensorBase ネットワーク \(7 ページ\)](#)

Web セキュリティアプライアンス の概要

Cisco Web セキュリティアプライアンス 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。

AsyncOS 14.1 の新機能

表 1: AsyncOS 14.1 の新機能

機能	説明
Cisco Umbrella シームレス ID	<p>Cisco Umbrella シームレス ID 機能を使用すると、正常に認証された後に、アプライアンスからユーザ識別情報を Cisco Umbrella セキュア Web ゲートウェイ (SWG) にパスすることができます。Cisco Umbrella SWG は、Web セキュリティアプライアンスから受信した認証済み識別情報に基づいて、Active Directory のユーザ情報をチェックします。Cisco Umbrella SWG は、ユーザを認証済みと見なし、定義されたセキュリティポリシーに基づいてユーザにアクセスを提供します。</p> <p>Web セキュリティアプライアンスは、X-USWG-PKH、X-USWG-SK、および X-USWG-Data を含む HTTP ヘッダーを使用して Cisco Umbrella SWG にユーザ識別情報をパスします。</p> <p>(注) Cisco Umbrella シームレス ID ヘッダーは、Web セキュリティアプライアンス上の同じ名前のヘッダーを上書きします。</p> <p>Cisco Umbrella シームレス ID 機能は、Active Directory でのみ認証方式をサポートします。この機能は、LDAP、Cisco Identity Services Engine (ISE)、および Cisco Context Directory Agent (CDA) をサポートしていません。</p> <p>Cisco Umbrella SWG は FTP および SOCKS トラフィックをサポートしていません。</p> <p>「Cisco Umbrella シームレス ID」を参照してください。</p>

関連項目

- <http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-release-notes-list.html>

アプライアンス Web インターフェイスの使用

- [Web インターフェイスのブラウザ要件 \(3 ページ\)](#)
- [仮想アプライアンスでの Web インターフェイスへのアクセスのイネーブル化 \(4 ページ\)](#)

- [アプライアンス Web インターフェイスへのアクセス \(5 ページ\)](#)
- [Web インターフェイスでの変更内容のコミット \(6 ページ\)](#)
- [Web インターフェイスでの変更内容のクリア \(7 ページ\)](#)

Web インターフェイスのブラウザ要件

Web インターフェイスにアクセスするには、ブラウザが JavaScript および Cookie をサポートし、受け入れがイネーブルになっている必要があります。また、Cascading Style Sheet (CSS) を含む HTML ページをレンダリングできる必要があります。

Cisco Web セキュリティアプライアンスは YUI (<http://yuilibrary.com/yui/environments/>) で設定されたターゲット環境に準拠しています。

セッションは、非アクティブな状態が 30 分続くと自動的にタイムアウトします。

Web インターフェイス内の一部のボタンとリンクを使用すると、さらにウィンドウが開きます。そのため、Web インターフェイスを使用するには、ブラウザのポップアップブロックを設定する必要があります。



- (注) アプライアンスの設定を編集する場合は、一度に 1 つのブラウザ ウィンドウまたはタブを使用します。また、Web インターフェイスおよび CLI を同時に使用してアプライアンスを編集しないでください。複数の場所からアプライアンスを編集すると、予期しない動作が発生するので、サポートされません。

GUI にアクセスするには、ブラウザが JavaScript および Cookie をサポートし、受け入れるよう設定されている必要があります。さらに、Cascading Style Sheet (CSS) を含む HTML ページを描画できる必要があります。

表 2: サポートされるブラウザおよびリリース

ブラウザ	Windows 10	MacOS 10.6
Safari	—	7.0 以降
Google Chrome	最新の安定バージョン	最新の安定バージョン
Microsoft Internet Explorer	11.0	—
Mozilla Firefox	最新の安定バージョン	最新の安定バージョン
Microsoft Edge	最新の安定バージョン	最新の安定バージョン

- Internet Explorer 11.0 (Windows 10 のみ)

- Safari 7 以降
- Firefox (最新の安定バージョン)
- Google Chrome (最新の安定バージョン)

ブラウザは、そのブラウザの公式なサポート対象オペレーティング システムに対してのみサポートされます。

インターフェイスの一部のボタンまたはリンクからは追加のウィンドウがオープンされるため、GUIを使用するには、ブラウザのポップアップブロックの設定が必要な場合があります。

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。

仮想アプライアンスでの Web インターフェイスへのアクセスのイネーブル化

デフォルトでは、HTTP および HTTPS インターフェイスは仮想アプライアンスで有効化されません。これらのプロトコルを有効にするには、コマンドラインインターフェイスを使用する必要があります。

ステップ 1 コマンドラインインターフェイスにアクセスします。 [コマンドラインインターフェイスへのアクセス](#) を参照してください。

ステップ 2 `interfaceconfig` コマンドを実行します。

プロンプトで Enter キーを押すと、デフォルト値が受け入れられます。

HTTP および HTTPS のプロンプトを検索し、使用するプロトコルをイネーブルにします。

HTTP および HTTPS の AsyncOS API (モニターリング) のプロンプトを探し、使用するプロトコルをイネーブルにします。

アプライアンス Web インターフェイスへのアクセス

仮想アプライアンスを使用している場合は、[仮想アプライアンスでの Web インターフェイスへのアクセスのイネーブル化 \(4 ページ\)](#) を参照してください。

ステップ 1 ブラウザを開き、Web セキュリティアプライアンスの IP アドレス（またはホスト名）を入力します。アプライアンスが事前に設定されていない場合は、デフォルト設定を使用します。

`https://192.168.42.42:8443`

または

`http://192.168.42.42:8080`

ここで、192.168.42.42 はデフォルト IP アドレス、8080 は HTTP のデフォルトの管理ポートの設定、8443 は HTTPS のデフォルトの管理ポートです。

アプライアンスが現在設定されている場合は、M1 ポートの IP アドレス（またはホスト名）を使用します。

(注) アプライアンスに接続するときはポート番号を使用する必要があります（デフォルトはポート 8080）。Web インターフェイスにアクセスするときにポート番号を指定しないと、デフォルトポート 80 になり、[ライセンスなしプロキシ (Proxy Unlicensed)] エラーページが表示されます。

ステップ 2 (新しい Web インターフェイスのみ) レガシー Web インターフェイスにログインし、[Web セキュリティアプライアンスのデザインが新しくなりました。お試してください! リンクで新しい Web インターフェイスにアクセスできます。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://wsa_appliance.com:<trailblazer-https-port>/ng-login` に移動します。ここで、`wsa_appliance.com` はアプライアンスのホスト名で、`<trailblazer-https-port>` はアプライアンスに設定されている TRAILBLAZER HTTPS ポートです。

- (注)
- 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インターフェイスホスト名を DNS サーバー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、`trailerblazerconfig` 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、[Web セキュリティアプライアンス CLI コマンド](#)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 (モニターリング) ポートは、`interfaceconfig` CLI コマンドで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、[Web セキュリティアプライアンス CLI コマンド](#)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もエンタープライズファイアウォールでブロックされないことを確認してください。

ステップ 3 アプライアンスのログイン画面が表示されたら、アプライアンスにアクセスするためのユーザー名とパスワードを入力します。

デフォルトで、アプライアンスには以下のユーザー名とパスワードが付属します。

- ユーザー名 : **admin**
- パスワード : **ironport**

admin のユーザー名でログインするのが初めての場合は、パスワードをすぐに変更するよう求められます。

ステップ 4 自分のユーザー名での最近のアプライアンスへのアクセス試行 (成功、失敗を含む) を表示するには、アプリケーション ウィンドウの右上の [ログイン (Logged in as)] エントリの前にある [最近のアクティビティ (recent-activity)] アイコン (成功は **i**、失敗は **!**) をクリックします。

Web インターフェイスでの変更内容のコミット

ステップ 1 [変更を確定 (Commit Changes)] ボタンをクリックします。

ステップ 2 選択する場合、[コメント (Comment)] フィールドにコメントを入力します。

ステップ 3 [変更を確定 (Commit Changes)] をクリックします。

(注) すべてのコミットする前に、複数の設定変更を行うことができます。

Web インターフェイスでの変更内容のクリア

ステップ1 [変更を確定 (Commit Changes)] ボタンをクリックします。

ステップ2 [変更を破棄 (Abandon Changes)] をクリックします。

サポートされる言語

AsyncOS は次の言語のいずれかで GUI および CLI を表示できます。

- ドイツ語
- 英語
- スペイン語
- フランス語
- イタリア語
- 日本語
- 韓国語
- ポルトガル語
- ロシア語
- 中国語
- 台湾語

Cisco SensorBase ネットワーク

Cisco SensorBase ネットワークは、世界中の何百万ものドメインを追跡し、インターネットトラフィックのグローバルウォッチリストを維持する脅威の管理データベースです。SensorBase は、既知のインターネットドメインの信頼性の評価をシスコに提供します。Cisco Web セキュリティアプライアンスは、SensorBase データフィードを使用して、Web レピュテーションスコアを向上させます。

SensorBase の利点とプライバシー

Cisco SensorBase ネットワークへの参加は、シスコがデータを収集して、SensorBase 脅威管理 データベースとそのデータを共有することを意味します。このデータには要求属性に関する情報およびアプライアンスが要求を処理する方法が含まれます。

シスコはプライバシーを維持する重要性を理解しており、ユーザー名やパスワードなどの個人情報または機密情報も収集または使用しません。また、ファイル名とホスト名に続く URL 属性は、機密性を保証するために難読化されます。復号化された HTTPS トランザクションでは、SensorBase ネットワークは IP アドレス、Web レピュテーション スコア、および証明書内のサーバー名の URL カテゴリのみを受信します。

SensorBase ネットワークへの参加に同意する場合、アプライアンスから送信されたデータは HTTPS を使用して安全に転送されます。データを共有すると、Web ベースの脅威に対応して、悪意のあるアクティビティから企業環境を保護するシスコの機能が向上します。

Cisco SensorBase ネットワークへの参加の有効化



(注) システムの設定時にデフォルトで [標準 SensorBase ネットワークに参加 (Standard SensorBase Network Participation)] がイネーブルにされています。

ステップ 1 [セキュリティ サービス (Security Services)] > [SensorBase (SensorBase)] を選択します。

ステップ 2 [SensorBase ネットワークに参加 (SensorBase Network Participation)] がイネーブルであることを確認します。

ディセーブルの場合、アプライアンスが収集するデータは SensorBase ネットワーク サーバーには戻されません。

ステップ 3 [加入レベル (Participation Level)] セクションで、以下のレベルのいずれかを選択します。

- [制限 (Limited)]。基本的な参加はサーバー名情報をまとめ、SensorBase ネットワーク サーバーに MD5 ハッシュ パス セグメントを送信します。
- [標準 (Standard)]。拡張された参加は、unobfuscated パス セグメントを使用した URL 全体を SensorBase ネットワーク サーバーに送信します。このオプションは、より強力なデータベースの提供を支援し、継続的に Web レピュテーション スコアの整合性を向上させます。

ステップ 4 [AnyConnect ネットワークへの参加 (AnyConnect Network Participation)] フィールドで、Cisco AnyConnect クライアントを使用して Cisco Web セキュリティアプライアンスに接続するクライアントから収集された情報を含めるかどうかを選択します。

AnyConnect クライアントは、Secure Mobility 機能を使用してアプライアンスに Web トラフィックを送信します。

ステップ 5 [除外されたドメインと IP アドレス (Excluded Domains and IP Addresses)] フィールドで、任意でドメインまたは IP アドレスを入力して、SensorBase サーバーに送信されたトラフィックを除外します。

ステップ 6 変更を送信し、保存します。

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。