システム設定

この章で説明する内容は、次のとおりです。

システム管理タスクの実行

この章で説明する内容は、次のとおりです。

システム管理の概要

S シリーズ アプライアンスは、システム管理用の各種のツールを提供します。[システム管理（System Administration）] タブの機能は、以下のタスクの管理を支援します。

- アプライアンスの設定
- 機能キー
- ユーザー アカウントの追加、編集、および削除
- AsyncOS ソフトウェアのアップグレードとアップデート
- システム時刻

アプライアンス設定の保存、ロード、およびリセット

Secure Web Appliance のすべての設定は、1 つの XML コンフィギュレーション ファイルで管理できます。

アプライアンス設定の表示と印刷

Procedure

ステップ 1 [システム管理（System Administration）] > [設定のサマリー（Configuration Summary）] を選択します。
ステップ 2 必要に応じて、[設定のサマリー（Configuration Summary）] ページを表示または印刷します。

アプライアンス設定ファイルの保存

Procedure

ステップ 1 [システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

ステップ 2 [設定ファイル（Configuration File）] のオプションを設定します。

オプション	説明
ファイル処理オプションの指定	生成された設定ファイルの処理方法を選択します。 • [表示または保存するローカルコンピュータにファイルをダウンロード（Download file to local computer to view or save）] • [ファイルをこのアプライアンス（wsa_example.com）に保存（Save file to this appliance (example.com)）] • [ファイルをメールで送信（Email file to）]（1 つまたは複数の電子メール アドレスを指定します）。
パスフレーズ処理オプションの指定	• **[設定ファイルでパスフレーズをマスクする（Mask passphrases in the Configuration Files）]** ：エクスポートまたは保存されるファイルで、元のパスフレーズを「*****」に置き換えます。パスフレーズがマスクされた設定ファイルを直接 AsyncOS for Web にリロードすることはできません。 • [設定ファイル内のパスワードを暗号化する（Encrypt passphrases in the Configuration Files）]：FIPS モードが有効にされている場合、このオプションが使用可能になります。FIPS モードの有効化については、FIPS モードの有効化または無効化 , on page 65を参照してください。
ファイル命名オプションの選択	設定ファイルに名前を付ける方法を選択します。 • **[システムにより生成されたファイル名を使用（Use system-generated file name）]** • **[ユーザー定義ファイル名を使用：（Use user-defined file name:）]**

ステップ 3 [Submit] をクリックします。

アプライアンス設定ファイルのロード

Caution 設定をロードすると、現在の設定がすべて完全に削除されます。以下の操作を実行する前に設定を保存することを強く推奨します。

以前のリリースから最新のリリースに設定をロードすることは推奨しません。パスをアップグレードすると構成時の設定を保持できます。

手動で変更した構成ファイルをロードすると、パフォーマンスと機能の問題が発生する可能性があります。

Note 互換性のあるコンフィギュレーションファイルが、アプライアンスの現在インストールされているバージョンより URL カテゴリのセットの古いバージョンに基づいている場合、コンフィギュレーション ファイルのポリシーと ID が自動的に変更される場合があります。

Note 設定ファイルをロードするときに証明書検証エラーが発生した場合は、証明書のルート CA を Secure Web Appliance の信頼されたルートディレクトリにアップロードしてから、設定ファイルを再度ロードします。ルート CA をアップロードする方法については、証明書の管理, on page 70を参照してください。

Procedure

ステップ 1 [システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

ステップ 2 [設定をロード（Load Configuration）] オプションとロードするファイルを選択します。（注）

Note

- パスフレーズがマスクされているファイルはロードできません。
- ファイルには以下のヘッダーが必要です。

```
<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE config SYSTEM "config.dtd">
```

また、正しくフォーマットされた config セクションも必要です。

```
<config> ...your configuration information in valid XML </config>
```

ステップ 3 [ロード（Load）] をクリックします。

ステップ 4 表示される警告を確認します。処理の結果を確認したら、[続行（Continue）] をクリックします。

アプライアンス設定の出荷時デフォルトへのリセット

アプライアンス設定をリセットするときに、既存のネットワーク設定を保持するかどうかを選択できます。

このアクションでは、コミットする必要はありません。

Before you begin

アプライアンスから任意の場所に設定を保存します。

Procedure

ステップ 1 [システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

ステップ 2 下方向にスクロールして、[構成のリセット（Reset Configuration）] セクションを表示します。

ステップ 3 ページに表示された情報を読み、オプションを選択します。

ステップ 4 [リセット（Reset）] をクリックします。

設定ファイルのバックアップの保存

設定ファイルバックアップ機能により、すべての変更でアプライアンスの設定が記録され、現在の設定ファイルよりも古い設定ファイルが、リモートに配置されたバックアップサーバーに FTP または SCP で送信されます。

手順

ステップ 1 [システム管理（System Administration）] > [設定ファイル（Configuration File）] を選択します。

ステップ 2 [設定のバックアップの有効化（Enable Config Backup）] チェックボックスをオンにします。

ステップ 3 設定ファイルにパスフレーズを含める場合は [はい（Yes）] を選択します。設定ファイルからパスフレーズを除外する場合は [いいえ（No）] を選択します。

ステップ 4 取得方法を選択します。次のオプションを使用できます。

- [リモートサーバー上のFTP（FTP on Remote Server）]：FTP ホスト名、ディレクトリ、ユーザー名、およびパスフレーズを入力します。
- [リモートサーバー上のSCP（SCP on Remote Server）]：SCP ホスト名、ポート番号、ディレクトリ、およびユーザー名を入力します。
- [ホストキーチェック（Host Key Checking）]：SSH は、使用されたすべてのホストの ID のデータベースを SSH が自動的に維持およびチェックします。ホストキーは、ディレクトリ */.ssh/known_hosts* にあるユーザーのホームディレクトリに保存されます。

  [リモートサーバー上のSCP（SCP on Remote Server）] を選択し、[ホストキーチェックを有効化（Enable Host Key Checking）] を選択する場合、次のオプションを使用できます。

- [自動（Automatic）]：ホストキーは Cisco Secure Web Appliance によって自動的に設定されます。
- [手動（Manual）]：ホストキーはユーザーが手動で入力できます。

変更を送信すると、Cisco Secure Web Appliance はリモートホスト上の承認されたキーファイルに追加する SSH キーを提供します。これにより、構成ファイルを Cisco Secure Web Appliance からリモートホストにアップロードできます。33 その結果、SSH は接続したことのあるすべてのホストの識別情報を含むデータベースを維持し、チェックします。ホストキーは、ディレクトリ */.ssh/known_hosts* にあるユーザーのホームディレクトリに保存されます。

ステップ 5 [送信（Submit）] をクリックします。

CLI コマンドの `configbackup` を使用して設定ファイルバックアップ機能を有効にすることもできます。

Cisco Secure Web Appliance ライセンス

スマート ソフトウェア ライセンシング

概要（Overview）

スマート ソフトウェア ライセンシングを使用すると、Cisco Secure Web Applianceのライセンスをシームレスに管理およびモニターできます。スマート ソフトウェア ライセンスをアクティブ化するには、Cisco Smart Software Manager（CSSM）でアプライアンスを登録する必要があります。CSSMは、購入して使用するすべてのシスコ製品についてライセンスの詳細を管理する一元化されたデータベースです。スマートライセンスを使用すると、製品認証キー（PAK）を

使用して Web サイトで個別に登録するのではなく、単一のトークンで登録することができます。

アプライアンスを登録すると、アプライアンスのライセンスを追跡し、CSSMポータル経由でライセンスの使用状況を監視できます。アプライアンスにインストールされているスマートエージェントは、アプライアンスと CSSM を接続し、ライセンスの使用状況に関する情報を CSSM を渡して、CSSM が使用状況を追跡できるようにします。

Cisco Smart Software Manager については、
Https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

始める前に

- ご利用のアプライアンスからインターネットに接続できることを確認します。
- Cisco Smart Software Manager ポータル（https://software.cisco.com/#module/SmartLicensing）でシスコ セールス チームに問い合わせるか、Cisco Smart Software Manager サテライトをネットワークにインストールしてください。

  Cisco Smart Software Manager のユーザー アカウントの作成または Cisco Smart Software Manager サテライトのインストールの詳細については、「https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html」を参照してください。

  ライセンスの使用状況に関する情報を直接インターネットに送信したくないユーザの場合、CSSM 機能のサブセットを提供する Smart Software Manager サテライトをオンプレミスにインストールすることもできます。サテライトアプリケーションをダウンロードして導入した後は、インターネットを使用して CSSM にデータを送信せずに、ライセンスをローカルで安全に管理できます。CSSMサテライトは、情報をクラウドに定期的に送信します。

（注） Smart Software Manager サテライトを使用する場合、Smart Software Manager サテライト Enhanced Edition 6.1.0 を使用してください。

- アプライアンスのシステム クロックを CSSM のシステム クロックと同期させる必要があります。アプライアンスのシステム クロックと CSSM のシステム クロックのずれは、スマート ライセンス操作の失敗の原因となります。

（注） インターネットに接続してプロキシ経由で CSSM に接続する場合、**[システム管理（System Administration）] > [アップグレードとアップデートの設定（Upgrade and Update Settings）]** を使用して、アプライアンスに設定されているプロキシと同じプロキシを使用する必要があります。

（注） 仮想ユーザーの場合、新しい PAK ファイル（新規または更新）を受信するたびに、ライセンス ファイルを生成し、アプライアンスのファイルをロードします。ファイルをロードした後は、PAK をスマート ライセンスに変換する必要があります。スマート ライセンス モードでは、ファイルのロード中、ライセンス ファイルの機能キー セクションは無視され、証明書情報のみが使用されます。

ライセンス予約

Cisco Smart Software Manager（CSSM）ポータルに接続せずに、Cisco Secure Web Appliance で有効になっている機能のライセンスを予約できます。これは主に、インターネットや外部デバイスとの通信がない高度にセキュリティ保護されたネットワーク環境に Cisco Secure Web Appliance を展開するユーザーにとって有益です。

機能ライセンスは、次のいずれかのモードで予約できます。

- [特定ライセンスの予約（SLR）（Specific License Reservation (SLR)）]：このモードを使用して、特定の期間の個々の機能（「HTTPS 復号」など）のライセンスを予約できます。
- [永久ライセンスの予約（PLR）（Permanent License Reservation (PLR)）]：このモードを使用して、すべての機能のライセンスを永久に予約できます。

Cisco Secure Web Appliance でライセンスを予約する方法の詳細については、機能ライセンスの予約 （15 ページ）を参照してください。

アプライアンスに対してスマート ソフトウェア ライセンシングを有効にするには、次の手順を実行する必要があります。

	操作内容	詳細情報
ステップ 2	Cisco Smart Software Manager でのアプライアンスの登録	Cisco Smart Software Manager でのアプライアンスの登録 （10 ページ）
（オプション）ステップ 3	必要に応じて、Cisco Secure Web Appliance で機能ライセンスを予約することができます。	機能ライセンスの予約 （15 ページ）
ステップ 3	ライセンス（機能キー）の要求	ライセンスの要求 （13 ページ）

スマート ソフトウェア ライセンシングのイネーブル化

手順

ステップ 1 **[システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]** を選択します。

ステップ 2 [スマート ソフトウェア ライセンシングの有効化（Enable Smart Software Licensing）] をクリックします。

スマート ソフトウェア ライセンシングの詳細については、**スマート ソフトウェア ライセンシングの詳細** のリンクをクリックします。

ステップ 3 スマート ソフトウェア ライセンシングについての情報を読んだ後、**[OK]** をクリックします。

ステップ 4 変更を保存します。

次のタスク

スマート ソフトウェア ライセンシングを有効すると、クラシック ライセンス モードのすべての機能がスマート ライセンス モードでも自動的に使用可能になります。クラシック ライセンス モードの既存ユーザーの場合、CSSM でアプライアンスを登録せずに、スマート ソフトウェア ライセンシング機能を使用できる 90 日間の評価期間があります。

有効期限および評価期間の期限の前に、一定の間隔（90 日前、60 日前、30 日前、15 日前、5 日前、および最終日）で通知が表示されます。評価期間の間または終了後に、CSSM でアプライアンスを登録できます。

（注）

- クラシック ライセンス モードにおけるアクティブなライセンスを持たない仮想アプライアンスの新規ユーザーの場合、スマート ソフトウェア ライセンシング機能を有効にしても、評価期間は提供されません。クラシック ライセンス モードにおけるアクティブなライセンスを持つ仮想アプライアンスの既存ユーザーのみに、評価期間が提供されます。新規仮想アプライアンス ユーザーがスマート ライセンス機能の評価を希望する場合には、シスコ セールス チームに連絡し、スマート アカウントに評価ライセンスを追加してください。評価ライセンスは、登録後に評価目的で使用されます。
- アプライアンスでスマート ライセンシング機能を有効にすると、スマート ライセンシングからクラシック ラインセンシングモードにロールバックすることができなくなります。
- スマート ライセンス機能を有効にすると、次の機能が自動的に再起動されます。
  - Secure Web Appliance Web レピュテーションフィルタ（Web Reputation Filters）
  - Secure Web Appliance ウイルス対策（Sophos）
  - Secure Web Appliance ウイルス対策（Webroot）
  - Secure Web Appliance Web プロキシと DVS エンジン
- AsyncOS バージョン 15.0 では、新しい Cisco Secure Web Appliance 仮想展開に対してスマートライセンスを有効にできます。クラシックライセンスは必須ではありません。詳細については、「Overview of Smart Licencing」セクションにある前提条件を参照してください。

Cisco Smart Software Manager でのアプライアンスの登録

アプライアンスを Cisco Smart Software Manager（CSSM）に登録するには、[システム管理（System Administration）] メニューでスマート ソフトウェア ライセンシング機能を有効にする必要があります。

（注）

- 複数のアプライアンスを単一のインスタンスで登録することはできません。アプライアンスを 1 つずつ登録する必要があります。
- 初回登録の有効期間は 1 年です。登録の更新は、アプライアンスが CSSM に接続できる場合、6 か月ごとに自動的に実行されます。

手順

ステップ 1 **[システム管理（System Administration）] > [スマート ソフトウェア ライセンシング（Smart Software Licensing）]** を選択します。

ステップ 2 [スマートライセンスの登録（Smart License Registration）] オプションを選択します。

ステップ 3 [確認（Confirm）] をクリックします。

ステップ 4 [トランスポート設定（Transport Settings）] を変更する場合には、**[編集（Edit）]** をクリックします。次のオプションを使用できます。

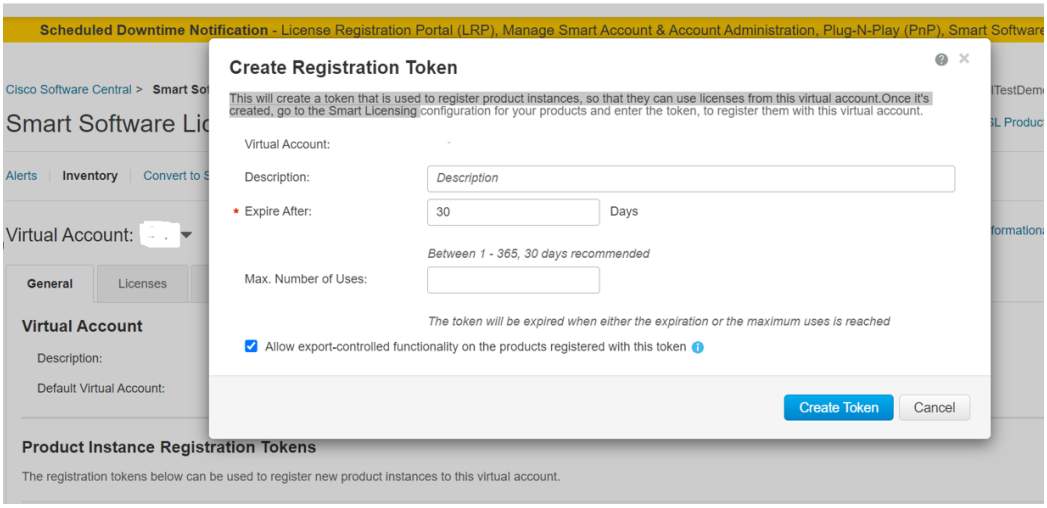
- **[直接（Direct）]**：アプライアンスを HTTPS 経由で Cisco Smart Software Manager に直接接続します。このオプションは、デフォルトで選択されます。
- **[トランスポートゲートウェイ（Transport Gateway）]**：アプライアンスをトランスポート ゲートウェイまたは Smart Software Manager サテライト経由で Cisco Smart Software Manager に接続します。このオプションを選択した場合、トランスポート ゲートウェイまたは Smart Software Manager サテライトの URL を入力してから [OK] をクリックする必要があります。このオプションは HTTP および HTTPS をサポートします。FIPS モードの場合、トランスポート ゲートウェイは HTTPS のみをサポートします。

  トランスポート ゲートウェイについては、
  Https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html
  を参照してください。

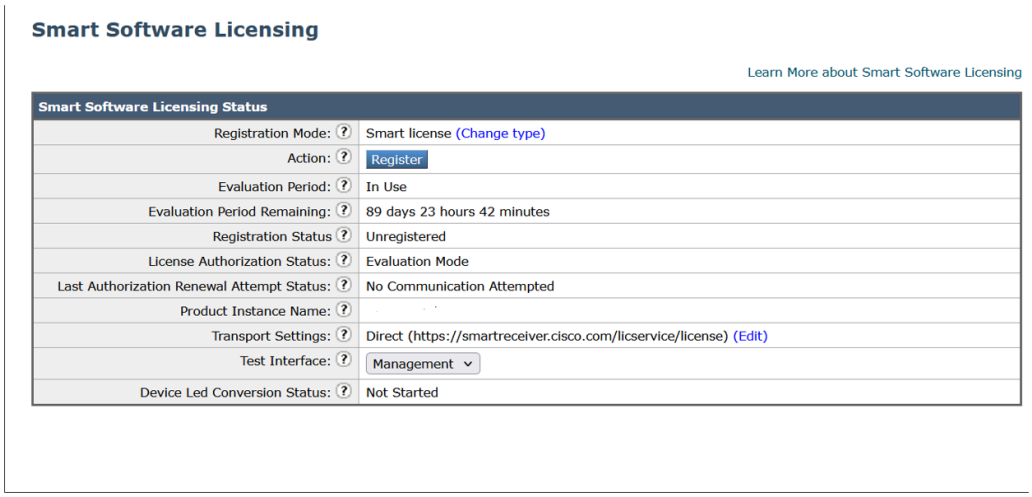
ステップ 5 （オプション）[テストインターフェイス（Test Interface）]：スマートライセンス機能用にアプライアンスを登録するときに、[管理インターフェイス（Management interface）] または [データインターフェイス（Data interface）] を選択します。これは、分割ルーティングを有効にし、スマートライセンス用に登録する場合にのみ適用されます。

（注）
分割ルーティングが有効になっていない場合は、[テストインターフェイス（Test Interface）] ドロップダウンリストで [管理インターフェイス（Management interface）] オプションのみを使用できます。

ステップ 6 ログイン クレデンシャルを使用して、Cisco Smart Software Manager ポータル（https://software.cisco.com/#module/SmartLicensing）にアクセスしてください。新しいトークンを作成するには、このポータルの [仮想アカウント（Virtual Account）] ページに移動して [全般（General）] タブにアクセスします。アプライアンス用の製品インスタンス登録トークンをコピーします。製品インスタンス登録トークンの作成については、
https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

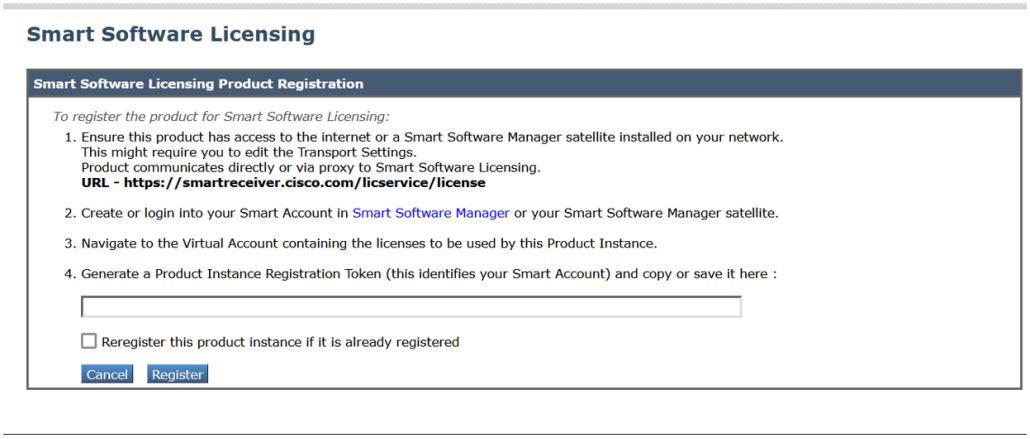


ステップ 7 アプライアンスに戻り、[登録（Register）] をクリックします。



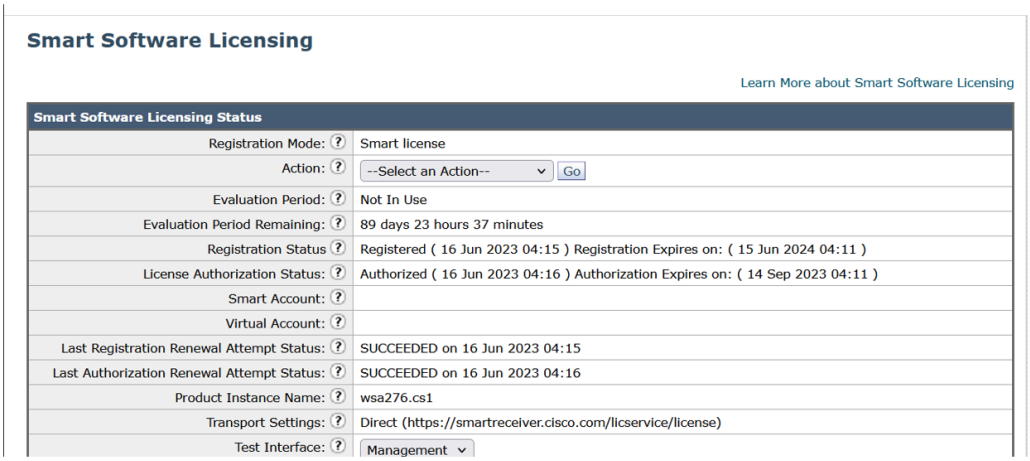
ステップ 8 **製品インスタンス登録トークン**をテキストボックスに貼り付けます。

[スマートソフトウェアライセンシング（Smart Software Licensing）] ページで、[すでに登録されている場合は、この製品インスタンスを再登録します（Reregister this product instance if it is already registered）] チェックボックスをオンにして、アプライアンスを再登録することもできます。



次のタスク

製品登録プロセスには数分かかります。[スマートソフトウェアライセンシング（Smart Software Licensing）] ページで登録ステータスを表示できます。



ライセンスの要求

登録プロセスが正常に完了した後、アプライアンスの機能のライセンスを要求しなければならない場合があります。

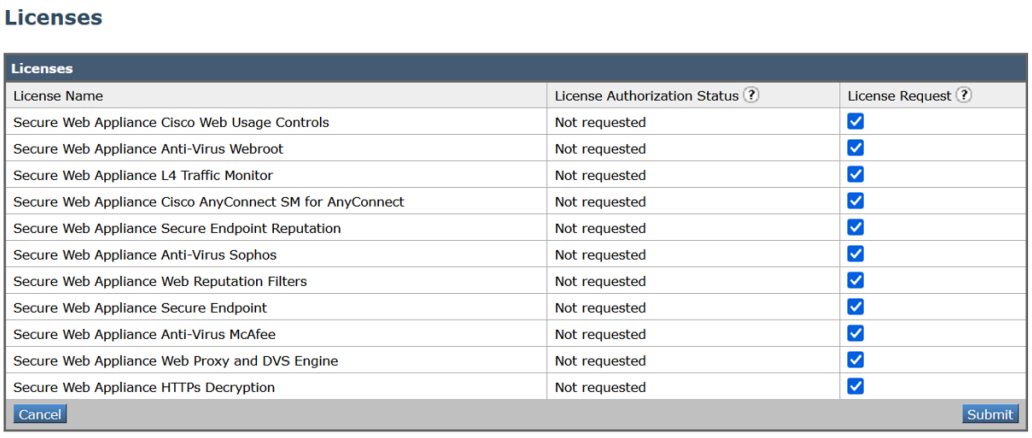
手順

ステップ 1 **[システム管理（System Administration）] > [ライセンス（Licenses）]** を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 要求するライセンスに対応する [ライセンスの要求/リリース（License Request/Release）] 列のチェック ボックスをオンにします。

ステップ 4 [送信（Submit）] をクリックします。



次のタスク

ライセンスは、期限超過また期限切れになるとコンプライアンス違反（OOC）モードになり、各ライセンスに30日間の猶予期間が提供されます。有効期限およびOOC猶予期間の期限の前に、一定の間隔（30日前、15日前、5日前、および最終日）で通知が表示されます。

OOC猶予期間の有効期限が過ぎると、ライセンスは使用できず、機能を利用できなくなります。機能にもう一度アクセスするには、CSSMポータルでライセンスをアップデートして、認証を更新する必要があります。

ライセンスのリリース

手順

ステップ1 **[システム管理（System Administration）] > [ライセンス（Licenses）]** を選択します。

ステップ2 [設定の編集（Edit Settings）] をクリックします。

ステップ3 リリースするライセンスに対応する [ライセンスの要求（License Request）] 列のチェック ボックスをオフにします。

ステップ4 [Submit] をクリックします。

Cisco Smart Software Manager からのアプライアンスの登録解除

手順

ステップ1 **[システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]** を選択します。

ステップ2 [アクション（Action）] ドロップダウン リストから、[登録解除（Deregister）] を選択し、[実行（Go）] をクリックします。

ステップ3 [Submit] をクリックします。

Cisco Smart Software Manager でのアプライアンスの再登録

手順

ステップ1 **[システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]** を選択します。

ステップ2 [アクション（Action）] ドロップダウン リストから、[登録（Register）] を選択し、[実行（Go）] をクリックします。

次のタスク

登録プロセスについては、Cisco Smart Software Manager でのアプライアンスの登録 （10 ページ） を参照してください。

回避できないシナリオにおいては、アプライアンスの設定をリセットした後にアプライアンスを登録することができます。

転送設定の変更

CSSM でアプライアンスを登録する前にのみ、トランスポート設定を変更できます。

（注） スマート ライセンス機能が有効になっている場合にのみ、トランスポート設定を変更できます。アプライアンスがすでに登録されている場合、トランスポート設定を変更するには、アプライアンスの登録を解除する必要があります。トランスポート設定を変更した後に、アプライアンスを再登録する必要があります。

トランスポート設定を変更する方法については、Cisco Smart Software Manager でのアプライアンスの登録 （10 ページ） を参照してください。

認証と証明書の更新

Cisco Smart Software Manager でアプライアンスを登録した後に、証明書を更新できます。

（注） アプライアンスが正常に登録された後にのみ、認証を更新できます。

手順

ステップ 1 **[システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]** を選択します。

ステップ 2 **[アクション（Action）]** ドロップダウン リストから、適切なオプションを選択します。

- **認証を今すぐ更新**
- **証明書を今すぐ更新**

ステップ 3 [移動（Go）] をクリックします。

次のタスク

機能ライセンスの予約

- ライセンス予約の有効化 （16 ページ）

表 *1*: ライセンスのステータス

ステータス	説明
コンプライアンスで予約済み	アプライアンスはライセンスの要求を正常に実行し、ライセンスの使用を承認されています。
未承認	アプライアンスはライセンスを予約していません。

ライセンス予約の有効化

始める前に

Cisco Secure Web Appliance でスマート ライセンシング モードが有効になっていることを確認します。

（注） CLI で `license_smart` > `enable_reservation` サブコマンドを使用して、機能ライセンスを予約することもできます。

（注） 認証コードをすでにインストールし、スマートライセンシングを有効にしている場合、デバイスは有効に予約された登録済み状態に自動的に移行します。

手順

ステップ 1 Cisco Secure Web Applianceで [システム管理（System Administration）] > [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページに移動します。

ステップ 2 [特定/永久ライセンス予約（Specific/Permanent License Reservation）] オプションを選択します。

ステップ 3 [確認（Confirm）] をクリックします。

次のタスク

ライセンス予約の登録 （17 ページ）

ライセンス予約の登録

手順

ステップ 1 Cisco Secure Web Applianceで [システム管理（System Administration）] > [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページに移動します。

ステップ 2 [登録（Register）] をクリックします。

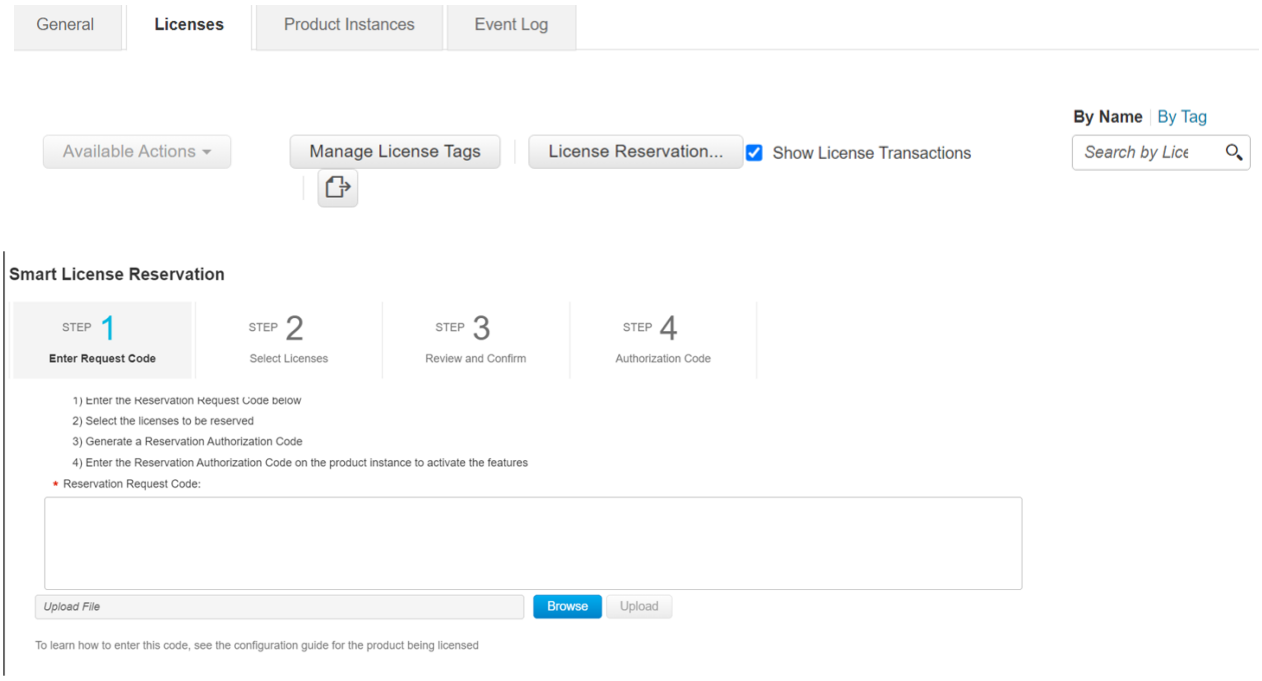
ステップ 3 [コードをコピー（Copy Code）] をクリックして、リクエストコードをコピーします。

（注）
リクエストコードを CSSM ポータルで使用して承認コードを生成します。

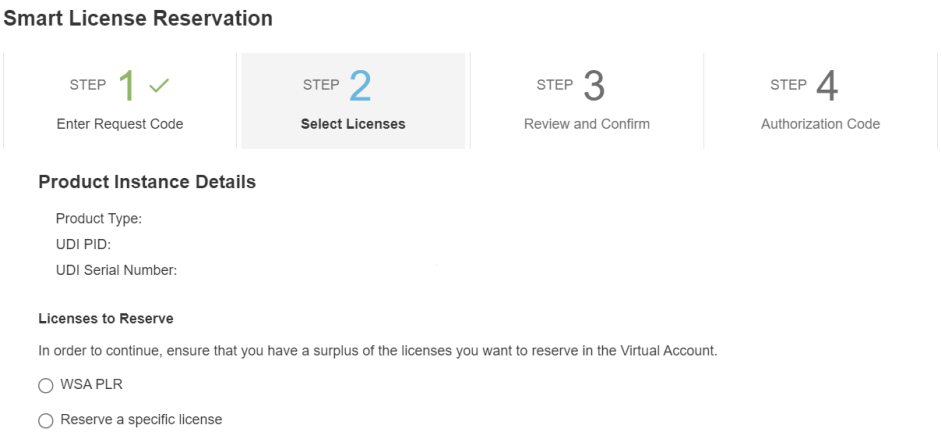
ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 CSSM ポータルに移動して、特定の機能またはすべての機能のライセンスを予約するための承認コードを生成します。

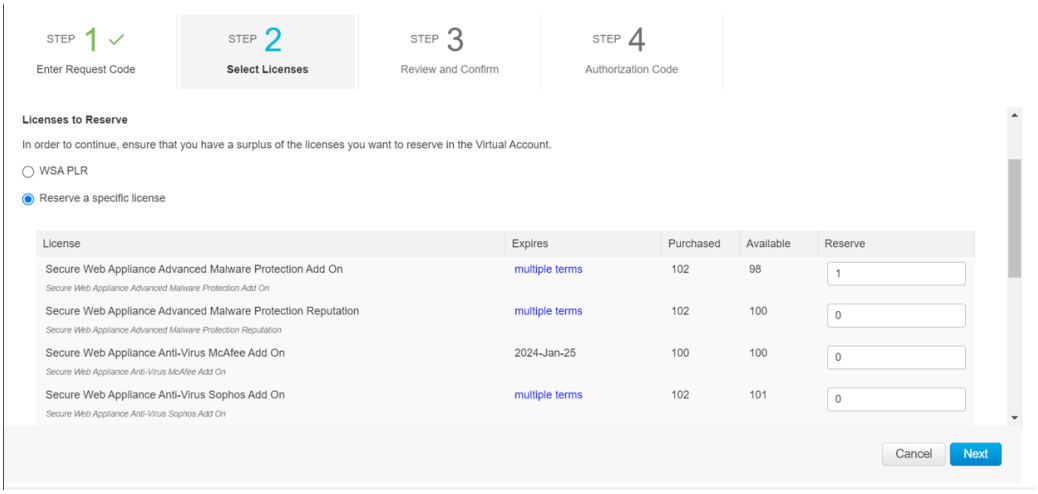
（注）
承認コードの生成方法の詳細については、スマート ソフトウェア ライセンシング オンライン ヘルプ（cisco.com） にあるヘルプドキュメントの *Inventory: License Tab* > *Reserve Licenses* セクションを参照してください。



ステップ 6 [SLR/PLR] を選択し、[次へ（Next）] をクリックします。



ステップ 7 CSSM ポータルで、SLR オプションに必要なライセンスを選択し、[次へ（Next）] をクリックします。



ステップ 8 次のいずれかの方法で、CSSM ポータルから取得した承認コードを Cisco Secure Web Appliance に貼り付けます。

- [承認コードをコピーして貼り付ける（Copy and Paste authorizationc code）] オプションを選択し、[承認コードをコピーして貼り付ける（Copy and Paste authorization code）] オプションの下のテキストボックスに承認コードを貼り付けます。
- [システムから承認コードをアップロード（Upload authorization code from the system）] オプションを選択し、[ファイルの選択（Choose File）] をクリックして承認コードをアップロードします。

ステップ 9 [承認コードをインストール（Install Authorization Code）] をクリックします。

インストール予約のバッチコマンドはサポートされていません。

（注）
承認コードがインストールされるまで、24 時間ごとにアラートが送信されます。

リクエストコードをキャンセルする方法：

承認コードがインストールされる前に予約プロセスをキャンセルするには、*CANCEL_REQUEST_CODE* コマンドを使用します。予約処理の状態をクリアします。

（注）
CSSM ポータルで承認コードを生成したが、アプライアンスでリクエストコードをキャンセルした場合、CSSM ポータルで生成したライセンスはアプライアンスにインストールできません。承認コードの削除については、TAC にお問い合わせください。

必要なライセンス予約（SLR または PLR）は、 Cisco Secure Web Appliance にインストールされています。

ライセンスのステータスは、SLR 用に予約されたライセンスの [コンプライアンスで予約済み（Reserved in Compliance）] 状態に移行します。PLR の場合、すべてのライセンスが [コンプライアンスで予約済み（Reserved in Compliance）] に移行します。

次のタスク

- （SLR のみに適用）：必要に応じて、ライセンス予約を更新できます。詳細については、ライセンス予約の更新 （19 ページ）を参照してください。
- （SLR および PLR に適用）：必要に応じて、ライセンス予約を削除できます。詳細については、ライセンス予約の削除 （20 ページ）を参照してください。
- （SLR および PLR に適用）：必要に応じて、ライセンス予約を無効化できます。詳細については、ライセンス予約の無効化 （21 ページ）を参照してください。

ライセンス予約の更新

新しい機能のライセンスを予約したり、機能の既存のライセンス予約を変更したりできます。

（注） 特定ライセンス予約のみを更新でき、永久ライセンス予約は更新できません。

（注） CLI で `license_smart > reauthorize` サブコマンドを使用して、ライセンス予約を更新することもできます。

手順

ステップ 1 CSSM ポータルに移動して、すでに予約済みのライセンスを更新するための承認コードを生成します。

（注）

承認コードの生成方法の詳細については、スマート ソフトウェア ライセンシング オンライン ヘルプ（cisco.com）にあるヘルプドキュメントの *Inventory: Product Instances Tab* > *Update Reserved Licenses* セクションを参照してください。

ステップ 2 Cisco Secure Web Applianceで [システム管理（System Administration）] > [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページに移動します。

ステップ 3 [アクション（Action）] ドロップダウンリストから [再承認（Reauthorize）] を選択し、[実行（GO）] をクリックします。

ステップ 4 次のいずれかの方法で、CSSM ポータルから取得した承認コードを Cisco Secure Web Appliance に貼り付けます。

- [承認コードをコピーして貼り付ける（Copy and Paste authorizationc code）] オプションを選択し、[承認コードをコピーして貼り付ける（Copy and Paste authorization code）] オプションの下のテキストボックスに承認コードを貼り付けます。
- [システムから承認コードをアップロード（Upload authorization code from the system）] オプションを選択し、[ファイルの選択（Choose File）] をクリックして承認コードをアップロードします。

ステップ 5 [再承認（Re-authorize）] をクリックします。

ステップ 6 [コードをコピー（Copy Code）] をクリックして、確認コードをコピーします。

（注）
CSSM ポータルで確認コードを使用して、ライセンス予約を更新します。

ステップ 7 [OK] をクリック

ステップ 8 Cisco Secure Web Appliance から取得した確認コードを CSSM ポータルに貼り付けます。

（注）
確認コードの追加方法の詳細については、スマート ソフトウェア ライセンシング オンライン ヘルプ（cisco.com）にあるヘルプドキュメントの *Inventory: Product Instances Tab* > *Update Reserved Licenses* セクションを参照してください。

ライセンス予約が更新されます。

ライセンスのステータスは、SLR 用に予約されたライセンスの [コンプライアンスで予約済み（Reserved in Compliance）] 状態に移行します。ライセンスが連続して予約されていない場合、ライセンスの状態は [未承認（Not-Authorized）] 状態に移行します。

ライセンス予約の削除

Cisco Secure Web Appliance で有効になっている特定のライセンス予約または永久ライセンスの予約を削除できます。

（注） CLI で `license_smart` > `return_reservation` サブコマンドを使用して、ライセンスの予約を削除することもできます。

（注） 予約済みライセンスを削除するとアラートが送信されます。

手順

ステップ 1 Cisco Secure Web Applianceで [システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）] ページに移動します。

ステップ 2 [アクション（Action）] ドロップダウンリストから [リターンコード（Return code）] を選択し、[実行（GO）] をクリックします。

ステップ 3 [コードをコピー（Copy Code）] をクリックして、リターンコードをコピーします。

（注）
CSSM ポータルにリターンコードを貼り付けて、ライセンス予約を削除します。

ステップ 4 [OK] をクリック

ステップ 5 Cisco Secure Web Appliance から取得したリターンコードを CSSM ポータルで使用します。

（注）
リターンコードの追加方法の詳細については、スマート ソフトウェア ライセンス オンライン ヘルプ（cisco.com） にあるヘルプ ドキュメントの *Inventory: Product Instances Tab* > *Removing a Product Instance* セクションを参照してください。

Cisco Secure Web Appliance で有効化されている機能のライセンス予約が削除され、すべてのライセンスが評価期間中になります。

次のタスク

- ライセンス予約の更新 （19 ページ） で確認コードの詳細を確認します。
- （SLR および PLR に適用）：必要に応じて、ライセンス予約を無効化できます。詳細については、ライセンス予約の無効化 （21 ページ）を参照してください。

ライセンス予約の無効化

Cisco Secure Web Appliance でライセンス予約を無効化できます。

（注） CLI で `license_smart` > `disable_reservation` サブコマンドを使用して、ライセンス予約を無効にすることもできます。

- 予約リクエストが開始されたが認証コードがインストールされていない場合、予約リクエストはデバイス上でキャンセルされます。

- 認証コードがインストールされている場合、予約リクエストは削除されません。「license smart reservation return」コマンドを使用して認証コードを削除するように警告メッセージが表示されます。このメッセージは、ライセンスの予約機能が無効になっている可能性があるが、認証コードがインストールされたままであることを意味します。この状態はshowコマンドに反映されます。

（注） コードを返して予約を無効化するか、コマンドを使用して予約を無効化できます。

- 認証コードがインストールされると、アプライアンスは認証状態になります。無効化すると、ステータスは有効化モードに移行します。

手順

ステップ 1 Cisco Secure Web Applianceで [システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）] ページに移動します。

ステップ 2 [登録モード（Registration Mode）] フィールドで [タイプの変更（Change Type）] をクリックします。

ステップ 3 [登録モードの変更（Change registration mode）] ダイアログボックスで [送信（Submit）] をクリックします。

ライセンス予約は、 Cisco Secure Web Appliance で無効化されます。

ライセンス失効通知：ライセンスの有効期限が切れる前

ライセンスの有効期限が切れる前のアラートの頻度は、60、30、15、5、2、および1日です。

ライセンス失効通知：ライセンスの有効期限が切れた後

ライセンスの有効期限が切れると、ライセンス失効通知が送信されます。SLR/PLR ライセンスのライセンス状態は、有効期限が切れた後も **[コンプライアンスで予約済み（Reserved in Compliance）]** のままになります。ライセンスの有効期限が切れると、クリティカル システム アラートがトリガーされ、電子メールが送信されます。

（注） ライセンス失効通知は、特定ライセンス予約のみが対象です。永久ライセンス予約では送信されません。

CLI で `license_smart` > `reauthorize` サブコマンドを使用して、ライセンス予約を更新することもできます。

ライセンスの有効期限が切れると、次のメッセージが表示されます。

「*Cisco Secure Web Appliance Secure Endpoint* アドオンの有効期限が切れています。（*The Secure Web Appliance Secure Endpoint Add on entitlement expired.*）」

再承認するためのメッセージがお客様に送信されます。

手順

ステップ 1 CSSM ポータルに移動して、すでに予約済みのライセンスを更新するための承認コードを生成します。

（注）
承認コードの生成方法の詳細については、スマート ソフトウェア ライセンシング オンライン ヘルプ（cisco.com） にあるヘルプドキュメントの *Inventory: Product Instances Tab > Update Reserved Licenses* セクションを参照してください。

ステップ 2 Cisco Secure Web Applianceで [システム管理（System Administration）] > [スマート ソフトウェア ライセンシング（Smart Software Licensing）] ページに移動します。

ステップ 3 [再承認（Re-authorize）] をクリックします。

スマート エージェントの更新

アプライアンスにインストールされているスマート エージェントのバージョンを更新するには、次の手順を実行します。

手順

ステップ 1 **[システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）]** を選択します。

ステップ 2 **[スマートエージェントの更新ステータス（Smart Agent Update Status）]** セクションで、**[今すぐ更新（Update Now）]** をクリックし、プロセスに従います。

（注）
CLI コマンド `saveconfig` を使用して、または **[システム管理（System Administration）] > [設定サマリー（Configuration Summary）]** を使用して Web インターフェイス経由で設定変更を保存しようとすると、スマート ライセンス関連の設定は保存されません。

アラート

次のシナリオで通知が送信されます。

- スマート ソフトウェア ライセンシングが正常に有効化された
- スマート ソフトウェア ライセンシングの有効化に失敗した

- 評価期間が開始された
- 評価期間が終了した（評価期間中および期間終了時に一定の間隔で送信）
- 正常に登録された
- 登録に失敗した
- 正常に認証された
- 認証に失敗した
- 正常に登録解除された
- 登録解除に失敗した
- ID 証明書が正常に更新された
- ID 証明書の更新に失敗した
- 認証の有効期限が切れた
- ID 証明書の有効期限が切れた
- コンプライアンス違反猶予期間の期限が切れた（コンプライアンス違反猶予期間中および期間終了時に一定の間隔で送信）
- 機能の有効期限に関する最初のインスタンスが発生した

コマンドライン インターフェイス

- license_smart （24 ページ）
- show_license （34 ページ）
- cloudserviceconfig

license_smart

- 説明 （25 ページ）
- 使用方法 （25 ページ）
- 例：Smart Software Manager でのアプライアンスの登録 （25 ページ）
- 例：スマート ライセンスのステータス （26 ページ）
- 例：スマート ライセンスのステータスの概要 （26 ページ）
- 例：スマート トランスポート URL の設定 （27 ページ）
- 例：ライセンスの要求 （27 ページ）
- 例：ライセンスのリリース （27 ページ）
- 例：ライセンス予約の有効化 （28 ページ）

- 例：ライセンス予約の登録 （29 ページ）
- 例：ライセンス予約の更新 （31 ページ）
- 例：ライセンス予約の削除 （32 ページ）
- 例：ライセンス予約の無効化 （32 ページ）

説明

スマート ソフトウェア ライセンス機能の設定

使用方法

確定：このコマンドは「commit」が必要です。

バッチ コマンド：このコマンドはバッチ形式をサポートしています。詳細については、`help license_smart` コマンドを入力して、インライン ヘルプを参照してください。

例：スマート エージェント サービス用ポートの設定

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[]> setagentport

Enter the port to run smart agent service.
[65501]>
```

例：スマート ライセンスの有効化

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
 []> enable
After enabling Smart Licensing on your appliance, follow below steps to activate
the feature keys (licenses):

a) Register the product with Smart Software Manager using license_smart > register command
 in the CLI.
b) Activate the feature keys using license_smart > requestsmart_license command in the
CLI.

Note: If you are using a virtual appliance, and have not enabled any of the
features in the classic licensing mode; you will not be able to activate the
licenses, after you switch to the smart licensing mode. You need to first register
your appliance, and then you can activate the licenses (features) in the smart licensing
 mode.
Commit your changes to enable the Smart Licensing mode on your appliance.
All the features enabled in the Classic Licensing mode will be available in the Evaluation
 period.
Type "Y" if you want to continue, or type "N" if you want to use the classic licensing
mode [Y/N] []> y

> commit

Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
```

例：Smart Software Manager でのアプライアンスの登録

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> register
Reregister this product instance if it is already registered [N]> n

Enter token to register the product:
[]>
ODRlOTM5MjItOTQzOS00YjY0LWExZTUtZTdmMmY3OGNlNDZmLTE1MzM3Mzgw%0AMDEzNTR8WlpCQ1lMbGVMQWRx

OXhuenN4OWZDdktFckJLQzF5V3VIbzkyTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status
 of registration.
```

例：スマート ライセンスのステータス

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode

Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

例：スマート ライセンスのステータスの概要

```
example.com> license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> summary

FeatureName                                  LicenseAuthorizationStatus
Web Security Appliance Cisco                 Eval
Web Usage Controls
```

```
Web Security Appliance Anti-Virus Webroot   Eval
Web Security Appliance Anti-Virus Sophos    Eval
```

例：スマート トランスポート URL の設定

```
example.com> license_smart

Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> url

1. DIRECT - Product communicates directly with the cisco license servers
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software
manager satellite.

Choose from the following menu options:
[1]> 1
Note: The appliance uses the Direct URL
(https://smartreceiver.cisco.com/licservice/license) to communicate with Cisco
Smart Software Manager (CSSM) via the proxy server configured using the updateconfig
command.
Transport settings will be updated after commit.
```

例：ライセンスの要求

（注） 仮想アプライアンスのユーザーは、ライセンスを要求またはリリースする場合、そのアプライアンスを登録する必要があります。

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> requestsmart_license

Feature Name                                    License Authorization Status
1. Web Security Appliance Anti-Virus Sophos     Not Requested
2. Web Security Appliance                       Not requested
   L4 Traffic Monitor

Enter the appropriate license number(s) for activation.
Separate multiple license with comma or enter range:
[]> 1
Activation is in progress for following features:
Web Security Appliance Anti-Virus Sophos
Use license_smart > summary command to check status of licenses.
```

例：ライセンスのリリース

```
example.com> license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> releasesmart_license

Feature Name                                  License Authorization Status
1. Web Security Appliance Cisco               Eval
   Web Usage Controls
2. Web Security Appliance                     Eval
   Anti-Virus Webroot
3. Web Security Appliance                     Eval
   L4 Traffic Monitor
4. Web Security Appliance Cisco               Eval
   AnyConnect SM for AnyConnect
5. Web Security Appliance Advanced            Eval
   Malware Protection Reputation
6. Web Security Appliance                     Eval
   Anti-Virus Sophos
7. Web Security Appliance                     Eval
   Web Reputation Filters
8. Web Security Appliance Advanced            Eval
   Malware Protection
```

例：ライセンス予約の有効化

この例では、license_smart > enable_reservation サブコマンドを使用して、 Cisco Secure Web Appliance でライセンスの予約を有効化できます。

```
example.com > license_smart

Choose the operation you want to perform:

REQUESTSMART_LICENSE - Request licenses for the product.
RELEASESMART_LICENSE - Release licenses of the product.
REGISTER - Register the product for Smart Licensing.
URL - Set the Smart Transport URL.
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure
Web Appliance.
[]> ENABLE_RESERVATION
Would you like to reserve license,then type "Y" else type "N" [Y/N] []> N

License reservation is not enabled.

Choose the operation you want to perform:

REQUESTSMART_LICENSE - Request licenses for the product.
RELEASESMART_LICENSE - Release licenses of the product.
REGISTER - Register the product for Smart Licensing.
URL - Set the Smart Transport URL.
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure
Web Appliance.
[]> ENABLE_RESERVATION
Would you like to reserve license,then type "Y" else type "N" [Y/N] []> Y
```

```
License reservation is enabled
[]>
```

例：ライセンス予約の登録

この例では、license_smart > enable_reservation サブコマンドを使用して、 Cisco Secure Web Appliance でライセンスの予約を有効化できます。

```
example.com > license_smart

Choose the operation you want to perform:

STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
 Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance. []>
REQUEST_CODE
The generation of the request code is initiated...
Copy the request code obtained on your Secure Web Appliance and paste it in the Cisco
Smart Software Manager portal to select the required license
Request code: CG-xxxxxxxxxxxxxxx-39

Choose the operation you want to perform:

STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
 Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance.
INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your Secure Web Appliance.
CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Web Appliance.
[]> INSTALL_AUTHORIZATION_CODE
Paste via CLI
Import the Authorization Code from a file How would you like to install Authorization
Code? [1]> 1
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version><piid>3c54a7ce-3b9c-
450e-9338-2f16e5801155</piid><timestamp>1650362032178</timestamp><entitlements>
<entitlement><tag>regid.2018-05.com.cisco.WSA_MUS,1.0_d3f3389a-cdc4-48e3-bc84-8b590ea2d908
</tag><count>1</count><startDate>2022-Apr-08 UTC</startDate><endDate>2022-May-08 UTC
</endDate><licenseType>TERM</licenseType><displayName>
Web Security Appliance Cisco AnyConnect SM for AnyConnect</displayName><tagDescription>
Web Security Appliance Cisco AnyConnect SM for AnyConnect</tagDescription>
<subscriptionID></subscriptionID></entitlement></entitlements>
</authorizationCode><signature>MEYCIQCiylVlTxBDYxxSaqexFExK4ThHVvXEJprhgK83j72FAAIhAJBqyc450uxiZ1pA
/phZ/PR/Xfl7e3rxc2AZCY3GH0O2</signature><udi>P:WSA,S:2AE28096313B</udi></specificPLR>^D

The SPECIFIC license reservation is successfully installed on your Secure Web Appliance

Choose the operation you want to perform:

STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
 Web Appliance.
REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Web Appliance.
CONFIRM_CODE - Provide the confirmation code generated on your Secure Web Appliance.
RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
```

```
 Web Appliance.
[]>
```

リクエストコード生成後のアプライアンスのステータス

```
[]> STATUS

Smart Licensing is : Enabled

License Reservation is: Enabled
Reservation Type: IN_PROGRESS
Return Code: CAt6Dx-G8K1Qn-dEY8qs-EFQyyA-nk5NFY-s6hZNi-PnpxMb-rxjGWV-QjP
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 54 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: wsa281.cs1
```

設置後のアプライアンスのステータス

```
[]> STATUS

Smart Licensing is : Enabled

License Reservation is: Enabled
Reservation Type: SPECIFIC
Evaluation Period: Not In Use
Evaluation Period Remaining: 83 days 3 hours 32 minutes
Registration Status: Registered ( 28 Apr 2022 04:42 )
Last Registration Renewal Attempt Status: SUCCEEDED on 28 Apr 2022 04:42
License Authorization Status: Not Authorized ( 28 Apr 2022 04:42 )
Last Authorization Renewal Attempt Status: SUCCEEDED on 28 Apr 2022 04:42
Product Instance Name: wsa281.cs1
Status of the Install Authorization Code :
```

要求コードのキャンセル

```
Choose the operation you want to perform:

STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
 Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance.
INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your Secure Web Appliance.
CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Web Appliance.
[]> CANCEL_REQUEST_CODE
If you want to cancel the generated request code, the authorization code generated from
 the Cisco Smart Software Manager portal will be locked.

Are you sure you want to cancel the request code? [Y/N] [N]> N

The request code is not cancelled

Choose the operation you want to perform:

STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
 Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance.
INSTALL_AUTHORIZATION_CODE - Install the authorization code for specific or permanent
license reservations on your Secure Web Appliance.
```

```
CANCEL_REQUEST_CODE - Cancel the request code generated on your Secure Web Appliance.
[]> CANCEL_REQUEST_CODE
If you want to cancel the generated request code, the authorization code generated from
 the Cisco Smart Software Manager portal will be locked.

Are you sure you want to cancel the request code? [Y/N] [N]> Y

The cancellation of the request code is initiated...
The request code is cancelled successfully

Choose the operation you want to perform:

STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
 Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance.
```

キャンセル後のアプライアンスのステータス

```
[]> STATUS

Smart Licensing is : Enabled

License Reservation is: Enabled
Reservation Type: NONE
Return Code: CAt6Dx-G8K1Qn-dEY8qs-EFQyyA-nk5NFY-s6hZNi-PnpxMb-rxjGWV-QjP
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: wsa281.cs1
```

例：ライセンス予約の更新

この例では、`license_smart > reauthorize` サブコマンドを使用して、新しい機能のライセンスを予約したり、機能の既存のライセンス予約を変更したりできます。

```
example.com > license_smart

Choose the operation you want to perform:
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
 Web Appliance.
REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Web Appliance.
CONFIRM_CODE - Provide the confirmation code generated on your Secure Web Appliance.
RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Web Appliance. []> REAUTHORIZE
[]> reauthorize
Paste via CLI
Import the Authorization Code from a file How would you like to install Authorization
Code? [1]>
Paste the Authorization code now.
Press CTRL-D on a blank line when done.
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piid>3c54a7ce-3b9c-450e-9338-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
</authorizationCode><signature>
MEUCIH5ypYX6GMB9wgZy+8tT4q+JqLlqU/05JlOyS/25gpH8AiEAjEubvaYMy0Vm2DV45TIFUY09c7OZ/JUXQBHIMcT4yDk=</signature>
<udi>P:WSA,S:2AE28096313B</udi></specificPLR>
^D
```

```
The SPECIFIC license reservation is successfully installed on your Secure Web Appliance
Copy the confirmation code obtained from Smart Agent and add it to the Cisco Smart
Software Manager portal to update the specific reservation.
Confirmation code: fxxxxfeb

CONFIRMATION CODE:
Choose the operation you want to perform:

STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
 Web Appliance.
REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Web Appliance.
CONFIRM_CODE - Provide the confirmation code generated on your Secure Web Appliance.
RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Web Appliance. []> CONFIRM_CODE
Copy the confirmation code obtained on your Secure Web Appliance and paste it in the
Cisco Smart Software Manager portal to update the specific license reservation.
Confirmation Code: fxxxxfeb
[]>
```

例：ライセンス予約の削除

この例では、license_smart > return_reservation サブコマンドを使用して、 Cisco Secure Web Appliance で有効になっている機能の特定または永続的なライセンスの予約を削除できます。

```
example.com > license_smart

Choose the operation you want to perform:

STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
 Web Appliance.
REAUTHORIZE - Install the authorization code to update specific or permanent license
reservations on your Secure Web Appliance.
CONFIRM_CODE - Provide the confirmation code generated on your Secure Web Appliance.
RETURN_RESERVATION - Remove the specific or permanent license reservations on your Secure
 Web Appliance.
[]> RETURN_RESERVATION
After you return the license reservation, you cannot use any of the product features,
if
the evaluation period has exceeded 90 days. After the 90 days evaluation period,
you must register your product with Cisco Smart Software Manager to continue
to use the product features. [N]> Y

The generation of the return code is initiated...
Copy the return code obtained on your Secure Web Appliance and paste it in the Cisco
Smart Software Manager portal.
Return Code: CLFSav-xxxxxxxxxxxxxxxxxxxxxxxxxxxx-Ef2
[]>
```

例：ライセンス予約の無効化

この例では、license_smart > disable_reservation サブコマンドを使用して、 Cisco Secure Web Appliance でライセンスの予約を無効化できます。

```
example.com > license_smart

Choose the operation you want to perform:
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
DISABLE_RESERVATION - Disable specific or permanent license reservations on your Secure
```

```
 Web Appliance.
REQUEST_CODE - Provide the request code generated on your Secure Web Appliance. []>
DISABLE_RESERVATION
Do you want to disable the specific or permanent reservation? [Y/N] []> Y

License reservation is disabled
Choose the operation you want to perform:

REQUESTSMART_LICENSE - Request licenses for the product.
RELEASESMART_LICENSE - Release licenses of the product.
REGISTER - Register the product for Smart Licensing.
URL - Set the Smart Transport URL.
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure
Web Appliance. []> STATUS
Smart Licensing is : Enabled

License Reservation is: Disabled
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 46 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: wsa281.cs1
Transport Settings: Direct (https://smartreceiver-stage.cisco.com/licservice/license)
Device Led Conversion Status: Not Started

Choose the operation you want to perform:

REQUESTSMART_LICENSE - Request licenses for the product.
RELEASESMART_LICENSE - Release licenses of the product.
REGISTER - Register the product for Smart Licensing.
URL - Set the Smart Transport URL.
STATUS - Show overall Smart Licensing status.
SUMMARY - Show Smart Licensing status summary.
ENABLE_RESERVATION - Enable specific or permanent license reservations on your Secure
Web Appliance. []>
[]>
```

例：Device Led Conversion（DLC）プロセスの手動による有効化

この例では、`license_smart` > `conversion_start` サブコマンドを使用して、 Cisco Secure Web Appliance で Device Led Conversion（DLC）を手動で有効化できます。

DLC 失敗のサンプルコード：

```
example.com > license_smart

Deregister the Secure Web Appliance from the Cisco Smart Software Manager portal to
enable the license reservation

Choose the operation you want to perform:
- URL - Set the Smart Transport URL.
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- DEREGISTER - Deregister the product from Smart Licensing.
- REREGISTER - Reregister the product for Smart Licensing.
- RENEW_AUTH - Renew authorization of Smart Licenses in use.
- RENEW_ID - Renew registration with Smart Licensing.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.
- CONVERSION_START - To manually convert the classic license keys to smart licensing.
[]> conversion_start
```

show_license

説明

スマート ライセンスのステータスとステータスの概要を表示します。

例：スマート ライセンスのステータス

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> status
Smart Licensing is: Enabled
Evaluation Period: In Use
Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered
License Authorization Status: Evaluation Mode
Last Authorization Renewal Attempt Status: No Communication Attempted
Product Instance Name: example.com
Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

例：スマート ライセンスのステータスの概要

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.

[]> summary

FeatureName                          LicenseAuthorizationStatus
Web Security Appliance Cisco         Eval
Web Usage Controls
Web Security Appliance               Eval
Anti-Virus Webroot
Web Security Appliance               Eval
Anti-Virus Sophos
```

cloudserviceconfig

（注） SLR/PLR を介してスマートライセンスを登録すると、クラウドサービスは有効化されず、自動登録は行われません。このサポートは、トークン登録を通じて登録されたスマートライセンスにのみ適用されます。

- 例： Secure Web Applianceでの Cisco Cloud Services の無効化
- 例：Cisco Cloud Services ポータルへの Secure Web Applianceの登録
- 例：Cisco Cloud Services ポータルへの Secure Web Applianceの自動登録
- 例：Cisco Cloud Services ポータルからの Secure Web Applianceの登録解除
- 例： Secure Web Applianceを Cisco Cloud Services ポータルに接続する Cisco Secure Cloud Server の選択
- 例：証明書とキーのダウンロード
- 例：クライアント証明書 updateconfig

説明

cloudserviceconfig コマンドは次の目的で使用します。

- Secure Web Applianceで Cisco Cloud Services ポータルを有効にします。
- Secure Web Applianceで Cisco Cloud Services ポータルを無効にします。
- Cisco Cloud Services ポータルに Secure Web Applianceを登録します。
- Cisco Cloud Services ポータルに Secure Web Applianceを自動的に登録します。
- Cisco Cloud Services ポータルから Secure Web Applianceの登録を解除します。
- Cisco Secure Cloud サーバーを選択して、 Secure Web Applianceを Cisco Cloud Services ポータルに接続します。
- Cisco Talos Intelligence Services ポータルから Cisco Cloud Services 証明書とキーをダウンロードします。
- クライアント証明書とキーをアップロードします。

（注） このコマンドは、スマートライセンスモードでのみ適用できます。

使用方法

- **確定**：このコマンドに commit は必要ありません。
- **バッチ コマンド**：このコマンドはバッチ形式をサポートしています。

例： Secure Web Applianceでの Cisco Cloud Services の有効化

次に、`cloudserviceconfig > enable` サブコマンドを使用して、 Secure Web Applianceで Cisco Cloud Services を有効にする例を示します

```
example.com > cloudserviceconfig
Choose the operation you want to perform:
- ENABLE - The Cisco Cloud Service is currently disabled on your appliance.
[]> enable
```

```
The Cisco Cloud Service is currently enabled on your appliance.
Currently configured Cisco Secure Cloud Server is: api.apj.sse.itd.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 1
Selected Cisco Secure Cloud Server is api-sse.cisco.com.
Make sure you run "commit" to make these changes active.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:23:19 2020 GMTexample.com >
```

例： Secure Web Applianceでの Cisco Cloud Services の無効化

次に、`cloudserviceconfig` > `disable` サブコマンドを使用して、 Secure Web Applianceで Cisco Cloud Services を無効にする例を示します。

```
example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> disable
The Cisco Cloud Service is currently disabled on your appliance.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:01:07 2020 GMT
example.com >
```

例：Cisco Cloud Services ポータルへの Secure Web Applianceの登録

次に、`cloudserviceconfig` > `register` サブコマンドを使用して、Cisco Cloud Services ポータルに Secure Web Applianceを登録する例を示します。

（注） このサブコマンドは、スマート ソフトウェア ライセンシングが有効になっていない状態で、Secure Web Applianceが Cisco Smart Software Manager に登録されていない場合にのみ使用できます

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> register

Enter a registration token key to register your appliance
[]> c51fa32bd9a31227eaab50dea873062c
```

```
Registering
The Web Security appliance is successfully registered with the Cisco Cloud Service portal.
example.com >
```

例：Cisco Cloud Services ポータルへの Secure Web Applianceの自動登録

次に、`cloudserviceconfig` > `autoregister` コマンドを使用して、Cisco Cloud Services ポータルに Secure Web Applianceを登録する例を示します。

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- AUTOREGISTER - register the appliance with the Cisco Cloud Service portal automatically
 using SL Payload.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> autoregister

The Web Security appliance successfully auto-registered with the Cisco Cloud Service
portal.
```

例：Cisco Cloud Services ポータルからの Secure Web Applianceの登録解除

次に、`cloudserviceconfig` > `deregister` サブコマンドを使用して、Cisco Cloud Services ポータルから Secure Web Applianceの登録を解除する例を示します。

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:

Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- DEREGISTER - To deregister the appliance from the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> deregister

Do you want to deregister your appliance from the Cisco Cloud Service portal.
If you deregister, you will not be able to access the Cloud Service features. [N]> y

The Web Security appliance successfully deregistered from the Cisco Cloud Service portal.
example.com >
```

例： Secure Web Applianceを Cisco Cloud Services ポータルに接続する Cisco Secure Cloud Server の選択

次に、`cloudserviceconfig` > `settrs` サブコマンドを使用して、 Secure Web Applianceを Cisco Cloud Services ポータルに接続するために必要な Cisco Secure Cloud Server を選択する例を示します。

```
example.com > cloudserviceconfig
The appliance is not registered with the Cisco Cloud Service portal.
Currently configured Cisco Cloud Server is api-sse.cisco.com
Choose the operation you want to perform:
- DISABLE - The Cisco Cloud Service is currently enabled on your appliance.
- REGISTER - To register the appliance with the Cisco Cloud Service portal.
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud
Service portal.
[]> settrs
Currently configured Cisco Secure Cloud Server is: api-sse.cisco.com
Available list of Cisco Secure Cloud Servers:
1. AMERICAS (api-sse.cisco.com)
```

```
2. APJC (api.apj.sse.itd.cisco.com)
3. EUROPE (api.eu.sse.itd.cisco.com)
Enter Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.:
[]> 3
Selected Cisco Secure Cloud Server is api.eu.sse.itd.cisco.com.
Make sure you run "commit" to make these changes active.
example.com > commit
Please enter some comments describing your changes:
[]> commit changes
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Tue Dec 29 13:37:40 2020 GMT
```

例：Cisco Talos Intelligence Services ポータルからの Cisco Cloud Services 証明書とキーのダウンロード

次に、`cloudserviceconfig > fetchcerificate` サブコマンドを使用して、Cisco Talos Intelligence Services ポータルから Cisco Cloud Services 証明書とキーをダウンロードする例を示します。

（注） このサブコマンドは、既存の Cisco Cloud Services 証明書の有効期限が切れている状態で、Cisco Smart Software Manager に Secure Web Applianceを登録している場合にのみ使用できます。

```
example.com > cloudserviceconfig

Registration/deregistration of the device with cloud service:


Choose the operation you want to perform:
- FETCHCERTIFICATE - Download the Cisco Talos certificate and key
- SETTRS - Set the Cisco Secure Cloud Server to connect to the Cisco Cloud Service portal.
- STATUS - Check the appliance registration status with the Cisco Cloud Service portal.
[]> fetchcertificate

Successfully downloaded the Cisco Talos certificate and key
example.com >
```

例：クライアント証明書 updateconfig

次に、`Updateconfig > clientcertificate` サブコマンドを使用して証明書とキーをアップロードする例を示します。

```
example.com > updateconfig

Service (images):                   Update URL:
-------------------------------------------------------------------------------
Web Reputation Filters              Cisco Servers
Support Request updates             Cisco Servers
Timezone rules                      Cisco Servers
How-Tos Updates                     Cisco Servers
HTTPS Proxy Certificate Lists       Cisco Servers
Cisco AsyncOS upgrades              Cisco Servers
Smart License Agent Updates         Cisco Servers

Service (list):                     Update URL:
-------------------------------------------------------------------------------
Web Reputation Filters              Cisco Servers
Support Request updates             Cisco Servers
Timezone rules                      Cisco Servers
How-Tos Updates                     Cisco Servers
HTTPS Proxy Certificate Lists       Cisco Servers
Cisco AsyncOS upgrades              Cisco Servers
Smart License Agent Updates         Cisco Servers
```

```
Update interval for Web Reputation and Categorization: 5m
Update interval for all other services: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Routing table for updates: Management
    The following services will use this routing table:
    - Web Reputation Filters
    - Support Request updates
    - Timezone rules
    - How-Tos Updates
    - HTTPS Proxy Certificate Lists
    - Cisco AsyncOS upgrades
    - Smart License Agent Updates

Upgrade notification: enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- CLIENTCERTIFICATE - Upload the client certificate and key.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> clientcertificate

Current Cisco certificate is valid for 179 days

Do you like to overwrite the existing certificate and key [Y|N] ? []> y

Paste the certificate.
Press CTRL-D on a blank line when done.
^D
```

証明書と秘密キーの詳細を貼り付けます。証明書とキーは正常に保存されます。

AsyncOS 14.0 以降のスマート ソフトウェア ライセンス キー ポイント

- スマート ソフトウェア ライセンスを有効にして登録すると、Cisco Cloud Service が有効になり、自動的に登録されます。
- Cisco Cloud Services 証明書の有効期限が切れている場合は、CLI で `cloudserviceconfig > fetchcertificate` サブコマンドを使用して Cisco Talos Intelligence Services ポータルから新しい証明書をダウンロードできます。
- スマートライセンスが評価モードの場合、Cisco Cloud Services の自動登録は実行できません。

仮想アプライアンスのライセンス

Cisco Web Security 仮想アプライアンスでは、ホスト上で仮想アプライアンスを実行する追加ライセンスが必要です。

仮想アプライアンスのライセンスの詳細については、『*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。

Note 仮想アプライアンスのライセンスをインストールする前に、テクニカル サポートのトンネルを開くことはできません。

ライセンスの期限が切れた後、アプライアンスは、180 日間セキュリティ サービスなしで、Web プロキシとして動作を継続します。この期間中、セキュリティ サービスは更新されません。

ライセンスの期限切れに関する警告を受信するように、アプライアンスを設定できます。

関連項目

- アラートの管理, on page 53

仮想アプライアンスのライセンスのインストール

『*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 [英語] から入手できます。

リモート電源再投入の有効化

Before you begin

- 専用のリモート電源再投入（RPC）ポートをセキュア ネットワークに直接、ケーブル接続します。詳細については、お使いのアプライアンス モデルのハードウェア ガイドを参照してください。このドキュメントの場所については、ドキュメントセットを参照してください。
- ファイアウォールを通過するために必要なポートを開くなど、アプライアンスがリモートアクセス可能であることを確認します。
- この機能を使用するには、専用のリモート電源再投入インターフェイスの一意の IPv4 アドレスが必要です。このインターフェイスは、このセクションで説明されている手順でのみ設定可能です。ipconfig コマンドを使用して設定することはできません。
- アプライアンスの電源を再投入するには、Intelligent Platform Management Interface（IPMI）バージョン2.0をサポートするデバイスを管理できるサードパーティ製ツールが必要です。このようなツールを使用できるように準備されていることを確認します。
- コマンドライン インターフェイスへのアクセスに関する詳細については、を参照してください。 コマンドライン インターフェイス

RPC を設定して変更を確定したら、10 ～ 15 分待ってから呼び出しを RPC に送信します。この待機時間中に、 Secure Web Appliance が RCP サービスを初期化します。

アプライアンスシャーシの電源をリモートでリセットする機能は、x80、x90、x95 シリーズのハードウェアでのみ使用できます。

アプライアンスの電源をリモートでリセットする場合は、このセクションで説明されている手順を使用して、この機能を事前に有効にし、設定しておく必要があります。

Procedure

ステップ 1 SSH またはシリアル コンソール ポートを使用して、コマンドライン インターフェイスにアクセスします。

ステップ 2 管理者権限を持つアカウントを使用してログインします。

ステップ 3 以下のコマンドを入力します。

```
remotepower
setup
```

ステップ 4 プロンプトに従って、以下の情報を指定します。

- この機能専用の IP アドレスと、ネットマスクおよびゲートウェイ。
- 電源の再投入コマンドを実行するために必要なユーザ名とパスフレーズ。

  これらのクレデンシャルは、アプライアンスへのアクセスに使用する他のクレデンシャルに依存しません。

ステップ 5 `commit` を入力して変更を保存します。

ステップ 6 設定をテストして、アプライアンスの電源をリモートで管理できることを確認します。

ステップ 7 入力したクレデンシャルが、将来、いつでも使用できることを確認します。たとえば、この情報を安全な場所に保管し、このタスクを実行する必要がある管理者が、必要なクレデンシャルにアクセスできるようにします。

What to do next

関連項目

- ハードウェア アプライアンス：アプライアンスの電源のリモート リセット

ユーザー アカウントの管理

以下のタイプのユーザーは、アプライアンスにログインして、アプライアンスを管理できます。

- **ローカル ユーザー。**アプライアンス自体にローカルにユーザーを定義できます。
- **外部システムに定義されたユーザー。**アプライアンスにログインするユーザーを認証するために、外部 LDAP または RADIUS サーバーに接続するようにアプライアンスを設定できます。

Note Webインターフェイスにログインするか、SSHを使用するなどの任意の方法を使用して、アプライアンスにログインできます。

関連項目

- ローカル ユーザー アカウントの管理, on page 42
- RADIUS ユーザー認証, on page 45
- LDAP サーバーによる外部認証の設定

ローカル ユーザー アカウントの管理

Secure Web Applianceに任意の数のユーザをローカルに定義できます。

デフォルトのシステム admin アカウントは、すべての管理者権限を持っています。admin アカウントのパスフレーズは変更できますが、このアカウントを編集したり削除することはできません。

Note adminユーザーのパスフレーズを紛失した場合は、シスコ サポート プロバイダに問い合わせしてください。詳細については、「管理者パスワードをリセットし、管理者ユーザーアカウントをロック解除する」を参照してください。

ローカル ユーザー アカウントの追加

Before you begin

すべてのユーザーアカウントが従うべきパスフレーズ要件を定義します。管理ユーザーのパスフレーズ要件の設定 , on page 48を参照してください。

Procedure

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] を選択します。

ステップ 2 [ユーザーの追加（Add User）] をクリックします。

ステップ 3 以下のルールに注意して、ユーザー名を入力します。

- ユーザー名に小文字、数字、およびダッシュ（-）記号を使用することはできますが、最初の文字をダッシュにすることはできません。
- ユーザー名は 16 文字以下です。
- ユーザー名としてシステムで予約されている特殊名（「operator」や「root」など）を指定することはできません。

- 外部認証も使用する場合は、ユーザー名が外部認証されたユーザー名と重複しないようにしてください。

ステップ 4 ユーザーの氏名を入力します。

ステップ 5 ユーザー タイプを選択します。

ユーザ タイプ	説明
管理者（Administrator）	すべてのシステム設定に対する完全なアクセス権を許可します。ただし、`upgradecheck` および `upgradeinstall` CLI コマンドは、システム定義の「admin」アカウントからのみ発行できます。
オペレータ（Operator）	ユーザー アカウントを作成、編集、および削除できません。オペレータ グループでは、以下の CLI コマンドの使用も制限されます。 • `resetconfig` • `upgradecheck` • `upgradeinstall` オペレータ グループでは、システム セットアップ ウィザードの使用も制限されます。
オペレータ（読み取り専用）（Read-Only Operator）	このロールのユーザー アカウントは、 • 設定情報を表示できます。 • 機能の設定方法を確認するために変更を行って送信はできますが、コミットはできません。 • キャッシュをクリアしたり、ファイルを保存するなどのアプライアンスへの他の変更を加えることはできません。 • ファイル システム、FTP、または SCP にアクセスできません。
ゲスト（Guest）	ゲスト グループのユーザーは、レポートやトラッキングなど、システムのステータス情報の参照のみを実行できます。

ステップ 6 パスフレーズを入力するか、または作成します。

ステップ 7 変更を送信し、保存します。

ユーザーアカウントを削除する

Procedure

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] を選択します。

ステップ 2 プロンプトが表示されたら、一覧表示されているユーザー名に対応するゴミ箱アイコンをクリックして確認します。

ステップ 3 変更を送信し、保存します。

ユーザー アカウントの編集

Procedure

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] を選択します。

ステップ 2 ユーザー名をクリックします。

ステップ 3 必要に応じて、[ユーザーの編集（Edit User）] ページでユーザーに変更を加えます。

ステップ 4 変更を送信し、保存します。

パスフレーズの変更

現在ログインしているアカウントのパスフレーズを変更するには、ウィンドウの右上で、[オプション（Options）] > [パスフレーズの変更（Change Passphrase）] を選択します。

他のアカウントの場合は、[ローカルユーザー設定（Local User Settings）] ページで、アカウントを編集してパスフレーズを変更します。

関連項目

- ユーザー アカウントの編集, on page 44
- 管理ユーザーのパスフレーズ要件の設定 , on page 48

制限的なユーザ アカウントとパスフレーズの設定値の構成

ユーザー アカウントとパスフレーズの制限を定義して、組織全体にパスフレーズ ポリシーを強制的に適用することができます。ユーザー アカウントとパスフレーズ制限は、Cisco アプライアンスに定義されたローカル ユーザーに適用されます。次の設定値を設定できます。

- **ユーザ アカウントのロック。**ユーザのアカウントがロックアウトされる失敗ログインの試行回数を定義できます。ユーザーログイン試行回数は 1 ～ 60 の範囲で設定できます。デフォルト値は 5 です。
- **パスフレーズ存続期間のルール。**ログイン後にユーザがパスフレーズの変更を要求されるまでの、パスフレーズの存続期間を定義できます。
- **パスフレーズのルール。**任意指定の文字や必須の文字など、ユーザが選択できるパスフレーズの種類を定義できます。

（注） AsyncOS バージョン 14.0 以降では、パスフレーズルールはデフォルトで有効になります。ただし、**パスフレーズルールで拒否する 3 文字以上の反復文字または連続文字**、および**パスフレーズルールで拒否する単語のリスト**は例外です。

- **パスフレーズの強度。**管理ユーザーが新しいパスフレーズを入力するときに、パスフレーズ強度インジケータを表示できます。

  詳細については、「管理ユーザーのパスフレーズ要件の設定」を参照してください。

ユーザ アカウントとパスフレーズの制限は、[システム管理（System Administration）] > [ユーザ（Users）] ページの [ローカル ユーザ アカウントとパスフレーズの設定（Local User Account & Passphrase Settings）] セクションで定義します。

RADIUS ユーザー認証

Secure Web Applianceは RADIUS ディレクトリ サービスを使用して、HTTP、HTTPS、SSH、および FTP によりアプライアンスにログインするユーザを認証します。PAP または CHAP 認証を使用して、認証のために複数の外部サーバーと連携するように、アプライアンスを設定できます。外部ユーザのグループを Secure Web Applianceのさまざまなユーザ ロール タイプにマッピングできます。

RADIUS 認証のイベントのシーケンス

外部認証がイネーブルになっている場合にユーザが Secure Web Applianceにログインすると、アプライアンスは以下を実行します。

1. ユーザーがシステム定義の「admin」アカウントであるかどうかを確認します。
2. 「admin」アカウントでない場合は、まず、設定されている外部サーバーをチェックし、ユーザーがそのサーバーで定義されているかどうかを確認します。
3. 最初の外部サーバーに接続できない場合、アプライアンスはリスト内の次の外部サーバーをチェックします。
4. アプライアンスが外部サーバに接続できない場合、アプライアンスは Secure Web Appliance で定義されたローカル ユーザとしてユーザを認証しようとします。
5. そのユーザーが外部サーバーまたはアプライアンスに存在しない場合、またはユーザーが間違ったパスフレーズを入力した場合は、アプライアンスへのアクセスが拒否されます。

RADIUS を使用した外部認証の有効化

Procedure

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] ページで、[外部認証を有効にする（Enable External Authentication）] をクリックします。

ステップ 2 認証タイプとして [RADIUS] を選択します。

ステップ 3 RADIUS サーバーのホスト名、ポート番号、共有シークレット パスフレーズを入力します。デフォルトのポートは 1812 です。

ステップ 4 タイムアウトまでにアプライアンスがサーバーからの応答を待つ時間を秒単位で入力します。

ステップ 5 RADIUS サーバーが使用する認証プロトコルを選択します。

ステップ 6 （任意）[行を追加（Add Row）] をクリックして別の RADIUS サーバーを追加します。各 RADIUS サーバーについて、**1 ～ 5** のステップを繰り返します。

Note
最大 10 個の RADIUS サーバーを追加できます。

ステップ 7 再認証のために再び RADIUS サーバーに接続するまでに、AsyncOS が外部認証クレデンシャルを保存する秒数を [外部認証キャッシュ タイムアウト（External Authentication Cache Timeout）] フィールドに入力します。デフォルトは 0 です。

Note
RADIUS サーバーがワンタイム パスフレーズ（トークンから作成されたパスフレーズなど）を使用している場合は、ゼロ（0）を入力します。値をゼロに設定すると、AsyncOS は、現在のセッション中に認証のために RADIUS サーバーに再アクセスしません。

ステップ 8 グループ マッピングを設定します。すべての外部認証されたユーザー全員を管理者ロールにマッピングするか、異なるアプライアンス ユーザー ロール タイプにマッピングするかを選択します。

設定	説明
外部認証されたユーザを複数のローカル ロールにマッピング。	RADIUS CLASS 属性で定義されたグループ名を入力し、アプライアンス ロール タイプを選択します。[行の追加（Add Row）] をクリックして、さらにロール マッピングを追加できます。 AsyncOS は、RADIUS CLASS 属性に基づいて、RADIUS ユーザをアプライアンス ロールに割り当てます。CLASS 属性の要件： • 最小 3文字 • 最大 253 文字 • コロン、カンマ、または改行文字なし • 各 RADIUS ユーザに対し 1 つ以上のマップ済み CLASS 属性（この設定を使用する場合、AsyncOS は、マップ済み CLASS 属性のない RADIUS ユーザへのアクセスを拒否します）。 複数の CLASS 属性のある RADIUS ユーザの場合、AsyncOS は最も制限されたロールを割り当てます。たとえば、Operator ロールにマッピングされている CLASS 属性と、Read-Only Operator ロールにマッピングされている CLASS 属性の 2 つが RADIUS ユーザにある場合、AsyncOS は、Operator ロールよりも制限された Read-Only Operator ロールに RADIUS ユーザを割り当てます。 以下のアプライアンス ロールは、最も制限が厳しいものから順番に並んでいます。 • 管理者（Administrator） • オペレータ（Operator） • Read-Only Operator • ゲスト（Guest）
外部認証されたすべてのユーザを管理ロールにマップします。	AsyncOS は すべての RADIUS ユーザーを Administrator ロールに割り当てます。

ステップ 9 変更を送信し、保存します。

What to do next

関連項目

- 外部認証
- ローカル ユーザー アカウントの追加, on page 42。

ユーザー プリファレンスの定義

レポートの表示形式などのプリファレンス設定は、各ユーザーごとに保存され、ユーザーがどのクライアントマシンからアプライアンスにログインするかに関係なく同じ設定が適用されます。

Procedure

ステップ 1 [オプション（Options）] > [環境設定（Preferences）] を選択します。

ステップ 2 [ユーザー設定（User Preferences）] ページで、[設定を編集（Edit Preferences）] をクリックします。

ステップ 3 必要に応じて、プリファレンスを設定します。

プリファレンス設定	説明
言語の表示（Language Display）	Web インターフェイスおよび CLI で使用する言語の Web 用 AsyncOS。
ランディング ページ（Landing Page）	ユーザーがアプライアンスにログインするときに表示されるページ。
表示されるレポート時間範囲（Reporting Time Range Displayed）（デフォルト）	[レポート（Reporting）] タブでレポートに対して表示するデフォルトの時間範囲。
表示するレポート行の数（Number of Reporting Rows Displayed）	デフォルトで各レポートに表示されるデータの行数。

ステップ 4 変更を送信し、保存します。

管理者の設定

管理ユーザーのパスフレーズ要件の設定

アプライアンスでローカル定義された管理ユーザーのパスフレーズ要件を設定するには、以下の手順を実行します。

Procedure

ステップ 1 [システム管理（System Administration）] > [ユーザー（Users）] を選択します。

ステップ 2 [パスフレーズの設定（Passphrase Settings）] セクションで、[設定を編集（Edit Settings）] をクリックします。

ステップ 3 以下のオプションから選択します。

オプション	説明
パスフレーズで許可しない単語の一覧（List of words to disallow in passphrases）	1 行ごとに各禁止単語を記入した .txt ファイルを作成し、そのファイルを選択してアップロードします。後続のアップロードによって以前のアップロードが上書きされます。
パスフレーズの強度（Passphrase Strength）	管理ユーザーが新しいパスフレーズを入力するときに、パスフレーズ強度インジケータを表示できます。 この設定によって強固なパスフレーズが作成されるわけではありません。この設定は、入力したパスフレーズの推測されやすさを示すだけです。 インジケータを表示する対象ロールを選択します。次に、選択したロールごとにゼロより大きい数字を入力します。数値が大きいほど、強固なパスフレーズとして登録されるパスフレーズの実現が困難になります。この設定には最大値がありませんが、非常に大きな数値を指定するとパスフレーズの作成が非常に困難になります。 さまざまな値を試すことで、最も要件を満たす数値を確認してください。 パスフレーズの強度は対数目盛で測定されます。評価は、トラブルシューティング トピックの NIST SP 800-63 で定義されている米国立標準技術研究所のエントロピーのルールに基づいています。 一般的に、強固なパスフレーズは以下のような特徴を備えています。 • 長い。 • 大文字、小文字、数字、および特殊文字を含む。 • あらゆる言語の辞書にある語を含まない。 これらの特徴を備えたパスフレーズを適用するには、このページの他の設定を使用します。

ステップ 4 変更を送信し、保存します。

アプライアンスの割り当てに対するセキュリティ設定の追加

CLI コマンド `adminaccessconfig` を使用すると、管理者がアプライアンスにログインする際のアクセス要件をさらに厳格にするように Secure Web Applianceを設定できます。

コマンド	説明
adminaccessconfig > banner	管理者がログインを試みるときに指定したテキストが表示されるようにアプライアンスを設定します。Web UI、CLI、FTP などの任意のインターフェイスを使用して管理者がアプライアンスにアクセスすると、カスタムのログイン バナーが表示されます。 CLI プロンプトに貼り付けるか、 Secure Web Appliance上のテキスト ファイルからコピーすることによって、カスタム テキストをロードできます。ファイルからテキストをアップロードするには、まず FTP を使用してアプライアンスの configuration ディレクトリにファイルを転送します。
adminaccessconfig > welcome	これは、管理者がログインに成功したときに表示されるポストログインバナーです。このテキストは、ログインの adminaccessconfig > banner テキストと同じ方法でアプライアンスの設定に追加されます。
adminaccessconfig > ipaccess	管理者が Secure Web Applianceにアクセスするときの接続元の IP アドレスを制御します。管理者は、任意のマシンまたは指定した一覧内の IP アドレスを持つマシンからアプライアンスにアクセスできます。 アクセスを許可リストに制限する場合は、IP アドレス、サブネット、または CIDR アドレスを指定できます。デフォルトでは、アプライアンスにアクセスできるアドレスを一覧表示すると、現在のマシンの IP アドレスが許可リストの最初のアドレスとして一覧表示されます。許可リストから現在のマシンの IP アドレスは削除できません。この情報は、Web UI を使用して表示することもできます。ユーザー ネットワーク アクセス, on page 51を参照してください。
adminaccessconfig > csrf	悪意のある要求、またはなりすました要求を識別して、これから保護するために使用される、Web UI のクロスサイト要求偽造保護機能を有効/無効にします。最大のセキュリティを確保するには、CSRF 保護をイネーブルにすることを推奨します。
adminaccessconfig > hostheader	HTTP 要求でホスト ヘッダーを使用するよう設定します。 デフォルトでは、Web UI は、HTTP 要求内で Web クライアントから送信されたホスト ヘッダーを使用して応答します。セキュリティを高めるために、アプライアンス固有のホスト名、つまりアプライアンスに設定された名前（wsa_04.local など）のみを使用して応答するように Web UI を設定することができます。

コマンド	説明
`adminaccessconfig > timeout`	非アクティビティのタイムアウト間隔、つまりユーザーがログアウトするまでに非アクティブでいられる期間（分数）を指定します。5 ～ 1440 分（24 時間）の値を指定できます。デフォルト値は 30 分です。この情報は、Web UI を使用して表示することもできます。ユーザー ネットワーク アクセス, on page 51を参照してください。
`adminaccessconfig > how-tos`	特定の設定タスク実行をサポートするウォークスルーを有効にします。
`adminaccessconfig > strictssl`	管理者がより強力な SSL 暗号（56 ビット暗号化以上）を使用してポート 8443 の Web インターフェイスにログインできるように、アプライアンスを設定します。 より強力な SSL 暗号を必要とするようにアプライアンスを設定すると、その変更は HTTPS を使用して管理の目的でアプライアンスにアクセスする管理者にのみ適用されます。HTTPS を使用して Web プロキシに接続されている他のネットワーク トラフィックには適用されません。
`adminaccessconfig > loginhistory`	ログイン履歴を保持する日数を設定します。
`adminaccessconfig > maxsessions`	同時ログイン セッションの最大数を設定します（CLI および Web インターフェイス）。

ユーザー ネットワーク アクセス

AsyncOS が、アプライアンスから非アクティブなユーザーをログアウトするまでの時間を指定できます。また、許可するユーザー接続のタイプを指定することもできます。

セッション タイムアウトは、管理者を含め、Web UI または CLI にログインしているすべてのユーザーに適用されます。AsyncOS がログアウトしたユーザーは、アプライアンスのログイン ページにリダイレクトされます。

（注） このタイムアウトの値を設定するには、CLI `adminaccessconfig > timeout` を使用することもできます。

手順

ステップ 1 [システム管理（System Administration）] > [ネットワーク アクセス（Network Access）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [セッション非アクティブ タイムアウト（Session Inactivity Timeout）] フィールドに、ログアウトするまでに許容するユーザーの非アクティブ時間を分数で入力します。

5 ～ 1440 分（24 時間）の範囲でタイムアウト間隔を定義できます。デフォルト値は 30 分です。

ステップ 4 [ユーザー アクセス（User Access）] セクションで、ユーザーのシステム アクセスを制御します。[任意の接続を許可（Allow Any Connection）] または [特定の接続のみを許可（Only Allow Specific Connections）] のいずれかをオンにします。

[特定の接続のみを許可（Only Allow Specific Connections）] をオンにする場合、特定の接続を IP アドレス、IP 範囲、または CIDR 範囲として定義します。クライアント IP アドレスとともに、アプライアンス IP アドレスが [ユーザー アクセス（User Access）] セクションに自動的に追加されます。

ステップ 5 変更を送信し、保存します。

管理者パスフレーズのリセット

Before you begin

- admin アカウントのパスフレーズが不明な場合は、カスタマーサポートプロバイダに連絡してパスフレーズをリセットしてください。
- パスフレーズの変更は即座に有効になり、変更を送信する必要はありません。

すべての管理者レベルのユーザーは、「admin」ユーザーのパスフレーズを変更できます。

Procedure

ステップ 1 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ユーザー（Users）] を選択します。

ステップ 2 [User（ユーザー）] リストで [admin] リンクをクリックします。

ステップ 3 [パスフレーズの変更（Change Passphrase）] を選択します。

ステップ 4 新しいパスフレーズを作成するか、または入力します。

生成されたメッセージの返信アドレスの設定

レポート用に AsyncOS によって生成されたメールの返信アドレスを設定できます。

Procedure

ステップ 1 [システム管理（System Administration）] > [返信先アドレス（Return Addresses）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 表示名、ユーザー名、およびドメイン名を入力します。

ステップ 4 変更を送信し、保存します。

アラートの管理

アラートとは、Cisco Secure Web Applianceで発生しているイベントに関する情報が記載されている、電子メールによる通知のことです。これらのイベントにはマイナー（情報）からメジャー（クリティカル）までの重要度（または重大度）レベルがあり、一般的にアプライアンスの特定のコンポーネントまたは機能に関連しています。

Note アラートと通知メール通知を受信するには、アプライアンスが電子メールメッセージへの送信に使用する SMTP リレー ホストを設定する必要があります。

アラートの分類と重大度

アラートに含まれる情報は、アラートの分類と重大度によって決まります。アラート受信者に送信するアラート分類と重大度を指定できます。

アラートの分類

AsyncOS は以下のタイプのアラートを送信します。

- システム（System）
- ハードウェア（Hardware）
- アップデータ（Updater）
- Web プロキシ（Web Proxy）
- マルウェア対策（Anti-Malware）
- AMP
- L4 トラフィック モニター（L4 Traffic Monitor）
- 外部 URL カテゴリ（External URL Categories）
- ポリシーの有効期限（Policy Expiration）

アラートの重大度

アラートは、次の重大度に従って送信されます。

- クリティカル：ただちに対処する必要があります。

- 警告：今後モニターリングが必要な問題またはエラー。すぐに対処が必要な場合もあります。
- 情報：デバイスのルーティン機能で生成される情報。

アラート受信者の管理

Note システムのセットアップ時にAutoSupportをイネーブルにした場合、指定した電子メールアドレスにすべての重大度およびクラスのアラートを受信します（デフォルト）。この設定はいつでも変更できます。

アラート受信者の追加および編集

Procedure

ステップ1 [システム管理（System Administration）] > [アラート（Alerts）] を選択します。

ステップ2 [アラート受信者（Alert Recipients）] リストで受信者をクリックして編集するか、[受信者の追加（Add Recipient）] をクリックして新しい受信者を追加します。

ステップ3 受信者の電子メールアドレスを追加または編集します。複数のアドレスをカンマで区切って入力することもできます。

ステップ4 各アラートタイプごとに、受信するアラートの重大度を選択します。

ステップ5 変更を送信し、保存します。

アラート受信者の削除

Procedure

ステップ1 [システム管理（System Administration）] > [アラート（Alerts）] を選択します。

ステップ2 [アラート受信者（Alert Recipient）] のリストで、アラート受信者に対応するゴミ箱アイコンをクリックして確定します。

ステップ3 変更を保存します。

アラート設定値の設定

アラート設定はグローバルな設定であるため、すべてのアラートの動作に影響します。

Procedure

ステップ 1 [システム管理（System Administration）] > [アラート（Alerts）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 必要に応じて、アラートの設定値を設定します。

オプション	説明
アラートの送信元アドレス（From Address to Use When Sending Alerts）	アラートを送信するときに使用する RFC 2822 準拠の「Header From:」アドレス。システムのホスト名（「alert@<hostname>」）に基づいてアドレスを自動生成するオプションが用意されています。
重複アラート送信時の待ち時間（Wait Before Sending a Duplicate Alert）	重複アラートの時間間隔を指定します。2 つの設定があります。 [重複アラート初回送信時の待ち時間（秒）（Initial Number of Seconds to Wait Before Sending a Duplicate Alert）]。この値を 0 に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます（短時間に大量の電子メールを受信する可能性があります）。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。増加する秒数は、前回の待機間隔の 2 倍の値を足した秒数です。つまり、この値を 5 秒に設定すると、アラートは 5 秒後、15 秒後、35 秒後、75 秒後、155 秒後、315 秒後といった間隔で送信されます。 [重複アラート送信時の最大待ち時間（秒）（Maximum Number of Seconds to Wait Before Sending a Duplicate Alert）]。 [重複するアラート メッセージを送信する前に待機する最大の秒数（Maximum Number of Seconds to Wait Before Sending a Duplicate Alert）] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を 5 秒に設定し、最大値を 60 秒に設定すると、アラートは 5 秒、15 秒、35 秒、60 秒、120 秒などの間隔で送信されます。

Note
AsyncOS 12.0 以降、Cisco AutoSupport オプションはアラート設定から削除されています。AutoSupport 機能は **alertconfig** CLI を使用してのみ有効または無効にできます。

ステップ 4 変更を送信し、保存します。

アラート リスト

以下の項では、分類別にアラートを一覧表示します。各項の表には、アラート名（内部で使用される descriptor）、アラートの実際のテキスト、説明、重大度（クリティカル、情報、または警告）およびメッセージのテキストに含まれるパラメータ（存在する場合）が含まれています。

ハードウェア アラート

以下の表は、AsyncOS で生成されるさまざまなハードウェア アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
A RAID-event has occurred: $error	警告（Warning）	**$error**：RAID エラーのテキスト。

システム アラート

以下の表は、AsyncOS で生成されるさまざまなシステム アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
Startup script $name exited with error: $message	クリティカル（Critical）。	**$name**：スクリプトの名前。 **$message**：エラー メッセージ テキスト。
System halt failed: $exit_status: $output',	クリティカル（Critical）。	**$exit_status**：コマンドの終了コード。 **$output**：コマンドからの出力。
System reboot failed: $exit_status: $output	クリティカル（Critical）。	**$exit_status**：コマンドの終了コード。 **$output**：コマンドからの出力。
Process $name listed $dependency as a dependency, but it does not exist.	クリティカル（Critical）。	**$name**：プロセスの名前。 **$dependency**：一覧表示されている依存性の名前。
Process $name listed $dependency as a dependency, but $dependency is not a wait_init process.	クリティカル（Critical）。	**$name**：プロセスの名前。 **$dependency**：一覧表示されている依存性の名前。
Process $name listed itself as a dependency.	クリティカル（Critical）。	**$name**：プロセスの名前。

メッセージ	アラートの重大度	パラメータ
Process $name listed $dependency as a dependency multiple times.	クリティカル（Critical）。	**$name**：プロセスの名前。 **$dependency**：一覧表示されている依存性の名前。
Dependency cycle detected: $cycle.	クリティカル（Critical）。	**$cycle**：サイクルに関係するプロセス名のリスト。
An error occurred while attempting to share statistical data through the Network Participation feature. Please forward this tracking information to your support provider: Error: $error.	警告（Warning）。	**$error**：例外に関連付けられたエラー メッセージ。
There is an error with “$name”.	クリティカル（Critical）。	**$name**：コア ファイルを生成したプロセスの名前。
An application fault occurred: “$error”	クリティカル（Critical）。	**$error**：エラーのテキスト（通常はトレースバック）。
Appliance: $appliance, User: $username, Source IP: $ip, Event: Account locked due to X failed login attempts. User $username is locked after X consecutive login failures. Last login attempt was from $ip.	情報（Information）。	**$appliance**：特定の Secure Web Applianceの ID。 **$username**：特定のユーザー アカウントの ID。 **$ip**：ログインが試行された IP アドレス。
Tech support: Service tunnel has been enabled, port $port	情報（Information）。	**$port**：サービス トンネルに使用されるポート番号。
Tech support: Service tunnel has been disabled.	情報（Information）。	適用なし

メッセージ	アラートの重大度	パラメータ
• The host at $ip has been added to the blocked list because of an SSH DOS attack. • The host at $ip has been permanently added to the ssh allowed list. • The host at $ip has been removed from the blocked list.	警告（Warning）。	**$ip**：ログインが試行されたIPアドレス。 **説明**： SSHを介してアプライアンスへの接続を試みているが、有効なクレデンシャルを提示しないIPアドレスは、2分以内に11回以上試行に失敗した場合、SSHのブロックリストに追加されます。 同じIPアドレスからユーザが正常にログインすると、そのIPアドレスは許可リストに追加されます。 許可リストのアドレスは、それらがブロックリストに含まれていてもアクセスが許可されます。 エントリは約1日後にブロックリストから自動的に削除されます。

Note システムアラートには、機能キーアラート、ロギングアラート、レポートアラートが含まれます。これらのアラートは、システムアラートの一部として設定した後に受信します。

機能キー アラート

以下の表は、AsyncOSで生成されるさまざまな機能キー アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
A “$feature” key was downloaded from the key server and placed into the pending area. EULA acceptance required.	情報（Information）。	**$feature**：機能の名前。
Your “$feature” evaluation key has expired. Please contact your authorized sales representative.	警告（Warning）。	**$feature**：機能の名前。

メッセージ	アラートの重大度	パラメータ
Your “$feature” evaluation key will expire in under $days day(s). Please contact your authorized sales representative.	警告（Warning）。	**$feature**：機能の名前。 **$days**：機能キーの期限が切れるまでの日数。

ロギング アラート

以下の表は、AsyncOS で生成されるさまざまなロギング アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
$error.	情報（Information）。	**$error**：エラーのトレースバック文字列。
Log Error: Subscription $name: Log partition is full.	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。
Log Error: Push error for subscription $name: Failed to connect to $ip: $reason.	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$ip**：リモート ホストの IP アドレス。 **$reason**：接続エラーについて説明するテキスト。
Log Error: Push error for subscription $name: An FTP command failed to $ip: $reason.	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$ip**：リモート ホストの IP アドレス。 **$reason**：問題点について説明するテキスト。
Log Error: Push error for subscription $name: SCP failed to transfer to $ip:$port: $reason',	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$ip**：リモート ホストの IP アドレス。 **$port**：リモート ホストのポート番号。 **$reason**：問題点について説明するテキスト。

メッセージ	アラートの重大度	パラメータ
Log Error: 'Subscription $name: Failed to connect to $hostname ($ip): $error.	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$hostname**：Syslog サーバーのホスト名。 **$ip**：Syslog サーバーの IP アドレス。 **$error**：エラー メッセージのテキスト。
Log Error: Subscription $name: Network error while sending log data to syslog server $hostname ($ip): $error	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$hostname**：Syslog サーバーのホスト名。 **$ip**：Syslog サーバーの IP アドレス。 **$error**：エラー メッセージのテキスト。
Subscription $name: Timed out after $timeout seconds sending data to syslog server $hostname ($ip).	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$timeout**：秒単位のタイムアウト。 **$hostname**：Syslog サーバーのホスト名。 **$ip**：Syslog サーバーの IP アドレス。
Subscription $name: Syslog server $hostname ($ip) is not accepting data fast enough.	クリティカル（Critical）。	**$name**：ログ サブスクリプション名。 **$hostname**：Syslog サーバーのホスト名。 **$ip**：Syslog サーバーの IP アドレス。

メッセージ	アラートの重大度	パラメータ
Subscription $name: Oldest log file(s) were removed because log files reached the maximum number of $max_num_files. Files removed include: $files_removed.	情報（Information）。	**$name**：ログ サブスクリプション名。 **$max_num_files**：ログ サブスクリプションごとに許可されるファイルの最大数。 **$files_removed**：削除されたファイルのリスト。

レポート アラート

以下の表は、AsyncOS で生成されるさまざまなレポート アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
The reporting system is unable to maintain the rate of data being generated. Any new data generated will be lost.	クリティカル（Critical）。	適用なし
The reporting system is now able to handle new data.	情報（Information）。	適用なし
A failure occurred while building periodic report ‘$report_title’. This subscription should be examined and deleted if its configuration details are no longer valid.	クリティカル（Critical）。	**$report_title**：レポートのタイトル。
A failure occurred while emailing periodic report ‘$report_title’. This subscription has been removed from the scheduler.	クリティカル（Critical）。	**$report_title**：レポートのタイトル。
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	警告（Warning）。	**$threshold**：しきい値。

メッセージ	アラートの重大度	パラメータ
PERIODIC REPORTS: While building periodic report $report_title' the expected domain specification file could not be found at '$file_name'. No reports were sent.	クリティカル（Critical）。	**$report_title**：レポートのタイトル。 **$file_name**：ファイルの名前。
Counter group "$counter_group" does not exist.	クリティカル（Critical）。	**$counter_group**：counter_group の名前。
PERIODIC REPORTS: While building periodic report $report_title' the domain specification file '$file_name' was empty. No reports were sent.	クリティカル（Critical）。	**$report_title**：レポートのタイトル。 **$file_name**：ファイルの名前。
PERIODIC REPORTS: Errors were encountered while processing the domain specification file '$file_name' for the periodic report '$report_title'. Any line which has any reported problem had no report sent. $error_text	クリティカル（Critical）。	**$report_title**：レポートのタイトル。 **$file_name**：ファイルの名前。 **$error_text**：発生したエラーのリスト。
Processing of collected reporting data has been disabled due to lack of logging disk space. Disk usage is above $threshold percent. Recording of reporting events will soon become limited and reporting data may be lost if disk space is not freed up (by removing old logs, etc). Once disk usage drops below $threshold percent, full processing of reporting data will be restarted automatically.	警告（Warning）。	**$threshold**：しきい値。
The reporting system has encountered a critical error while opening the database. In order to prevent disruption of other services, reporting has been disabled on this machine. Please contact customer support to have reporting enabled. The error message is: $err_msg	クリティカル（Critical）。	**$err_msg**：エラー メッセージ テキスト。

アップデータ アラート

以下の表は、AsyncOS で生成されるさまざまなアップデータ アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
The $app application tried and failed $attempts times to successfully complete an update. This may be due to a network configuration issue or temporary outage.	警告（Warning）。	**$app**： Secure Web Applianceセキュリティ サービス名。 **$attempts**：試行回数。
The updater has been unable to communicate with the update server for at least $threshold.	警告（Warning）。	**$threshold:**：しきい値の時間。
Unknown error occurred: $traceback.	クリティカル（Critical）。	**$traceback**：トレースバック情報。
Certificate Revoke: OCSP validation failed for the UPDATER Server Certificate ($host:$port). Ensure the certificate is valid.	クリティカル（Critical）	**$host**：**UPDATER** サーバーのホスト名。 **$port**：**UPDATER** サーバーのポート。

マルウェア対策アラート

Advanced Malware Protection に関連するアラートについては、Advanced Malware Protection の問題に関するアラートの確実な受信を参照してください。

ポリシーの期限切れアラート

次の表は、AsyncOS で生成されるさまざまなポリシー アラートのリストです。アラートの説明と重大度が記載されています。

メッセージ	アラートの重大度	パラメータ
'$PolicyType': '$GroupName' は、有効期限の設定のため、ディセーブルにされています。	情報	**$PolicyType:** は、Web ポリシー タイプに基づくアクセス ポリシー/復号ポリシーです。 **$GroupName:** は、ポリシー グループの名前です。
'$PolicyType' : '$GroupName' は、3 日後に期限切れとなります。	情報	**$PolicyType:** は、Web ポリシー タイプに基づくアクセス ポリシー/復号ポリシーです。 **$GroupName:** は、ポリシー グループの名前です。

FIPS Compliance

Federal Information Processing Standard（FIPS）は、機密情報であるが機密扱いされていない情報を保護するために、すべての政府機関で使用される暗号化モジュールの要件を規定しています。FIPS は、連邦政府のセキュリティとデータ プライバシー要件の遵守を確実にするために役立ちます。国立標準技術研究所（NIST）によって開発された FIPS は、連邦政府の要件を満たす任意の規格がない場合に使用されます。

Secure Web Applianceは Cisco Common Cryptographic Module（C3M）を使用して FIPS モードの FIPS 140-2 準拠を実現します。デフォルトでは、FIPS モードはディセーブルです。

関連項目

- FIPS モードの問題

FIPS 証明書の要件

FIPS モードでは、 Secure Web Applianceでイネーブルになっているすべての暗号化サービスについて FIPS 準拠の証明書を使用する必要があります。これは、以下の暗号化サービスに適用されます。

- HTTPS プロキシ
- 認証
- SaaS のアイデンティティ プロバイダー
- アプライアンス管理 HTTPS サービス
- セキュア ICAP 外部 DLP 設定
- Identity Services Engine
- カスタムの信頼できるルート CA
- SSL の設定
- SSH の設定
- NTP の設定

Note FIPS モードをイネーブルにする前に、FIPS 準拠証明書を使用してアプライアンス管理 HTTPS サービスを設定する必要があります。他の暗号化サービスはイネーブルにする必要はありません。

FIPS 準拠の証明書は以下の要件を満たす必要があります。

証明書	アルゴリズム	署名アルゴリズム	注記
X509	RSA	sha1WithRSAEncryption sha256WithRSAEncryption	最適な復号パフォーマンスと十分なセキュリティを実現するために、1024 ビットのキー サイズを推奨します。ビットサイズをさらに大きくすると、セキュリティは向上しますが、復号のパフォーマンスに影響します。

FIPS 証明書の検証

FIPS モードがイネーブルの場合、アプライアンスは次の証明書チェックを実行します。

- Secure Web Applianceにアップロードされたすべての証明書は、UI によってアップロードされたのか、それとも `certconfig` CLI コマンドによってアップロードされたのかに関係なく、CC 標準に厳格に従うように検証されます。 Secure Web Applianceの信頼ストア内の適切な信頼パスが設定されていない証明書は、アップロードできません。
- 信頼できるパス検証によって証明書の署名が検証され、すべての署名者証明書に対して検証済みの `basicConstrains` および `CAFlag` のセットによって証明書/公開キーの改ざんが検証されます。
- 失効リストに対して証明書を検証するために OCSP 検証を使用できます。これは、`certconfig` CLI コマンドを使用して設定できます。

（注） 新しいサブコマンド `OCSPVALIDATION_FOR_SERVER_CERT` がメインの CLI コマンド `certconfig` の下に追加されました。新しいサブコマンドを使用すると、LDAP サーバ証明書およびアップデータサーバ証明書の OCSP 検証を有効にできます。証明書の検証が有効になっている場合、通信に関係する証明書が失効するとアラートが表示されます。

厳格な証明書検証について （70 ページ） も参照してください。

FIPS モードの有効化または無効化

Before you begin

- アプライアンス設定のバックアップ コピーを作成します（以下を参照）。 アプライアンス設定ファイルの保存, on page 3
- FIPS モードで使用される証明書で、FIPS 140-3 認定の公開キーアルゴリズムが使用されていることを確認します（FIPS 証明書の要件, on page 64を参照）。

Note

- FIPS モードを変更すると、アプライアンスが再起動されます。
- FIPS モードを無効にした場合、SSL および SSH 設定（FIPS モードが有効にされている場合は、自動的に FIPS 対応になるようにする設定）はデフォルト値にリセットされません。接続する際、厳格でない SSH/SSL 設定を使用してクライアントが接続できるようにする必要がある場合は、明示的にこれらの設定を変更する必要があります。詳細については、SSL の設定 , on page 67を参照してください。

Procedure

ステップ 1 [システム管理（System Administration）] > [FIPS モード（FIPS Mode）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [FIPS コンプライアンスの有効化（Enable FIPS Compliance）] をオンにして、FIPS コンプライアンスを有効にします。

[FIPS コンプライアンスの有効化（Enable FIPS Compliance）] をオンにすると、[重大な機密性パラメータ（CSP）の暗号化を有効にする（Enable encryption of Critical Sensitive Parameters (CSP)）] チェックボックスが有効になります。

ステップ 4 パスワード、認証情報、証明書、共有キーなどの設定データの暗号化を有効にする場合は、[重大な機密性パラメータ（CSP）の暗号化を有効にする（Enable encryption of Critical Sensitive Parameters (CSP)）] をオンにします。

ステップ 5 [送信（Submit）] をクリックします。

ステップ 6 [続行（Continue）] をクリックして、アプライアンスの再起動を許可します。

システムの日時の管理

タイム ゾーンの設定

Procedure

ステップ 1 [システム管理（System Administration）] > [タイム ゾーン（Time Zone）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 地域、国、およびタイム ゾーンを選択するか、GMT オフセットを選択します。

ステップ 4 変更を送信し、保存します。

NTP サーバーによるシステム クロックの同期

アプライアンスで手動で時間を設定するのではなく、ネットワーク タイムプロトコル（NTP）サーバーに照会して現在の日時を追跡できるように Secure Web Applianceを設定することをお勧めします。これは、特にアプライアンスが他のデバイスと統合されている場合に該当します。統合されたすべてのデバイスが同じ NTP サーバーを使用する必要があります。

Secure Web Appliance は NTPv4 をサポートします。

Procedure

ステップ 1 [システム管理（System Administration）] > [時間の設定（Time Settings）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [時刻の設定方法（Time Keeping Method）] として [NTP（Network Time Protocol）を使用（Use Network Time Protocol）] を選択します。

ステップ 4 NTP サーバの完全修飾ホスト名または IP アドレスを入力し、以下を実行します：

a) **[キー タイプ（Key Type）]** ドロップダウン リストから **[MD5]**、**[SHA-1]** または **[AES-CMAC]** を選択します。

b) 指定された NTP サーバから、対応する MD5、SHA-1、または AES-CMAC **キー番号**および**キー値**を入力します。

c) [行の追加（Add Row）] をクリックします。

Note
FIPS が有効な場合、**[キー タイプ（Key Type）]** ドロップダウン リストに MD5 暗号化方式が表示されません。これは、MD5 暗号化方式が FIPS に準拠していないために予想される動作です。

ステップ 5 （任意）NTP クエリーに使用するアプライアンスのネットワーク インターフェイス タイプ（管理またはデータのいずれか）に関連付けられている、ルーティング テーブルを選択します。これは、NTP クエリーが発信される IP アドレスになります。

Note
このオプションは、アプライアンスがデータ トラフィック用と管理トラフィック用に分割ルーティングを使用している場合にのみ変更できます。

ステップ 6 変更を送信し、保存します。

SSL の設定

セキュリティを向上させるために、いくつかのサービスで SSL v3 とさまざまなバージョンの TLS をイネーブルまたはディセーブルにできます。最善のセキュリティを実現するために、す

べてのサービスで SSL v3 をディセーブルにすることをお勧めします。デフォルトでは、すべてのバージョンの TLS がイネーブルに設定され、SSL がディセーブルに設定されます。

Note これらの機能は、`sslconfig` CLI コマンドを使用してイネーブルまたはディセーブルにすることもできます。Secure Web Appliance CLI コマンドを参照してください。

Note

- TLSv1.0 と TLSv1.1 は、プロキシ構成以外の SSL 構成ではサポートされなくなりました。AsyncOS をアップグレードする前に、TLS バージョンを TLSv1.2 以降に変更する必要があります。
- SSL 設定ページおよび CLI から、ポート 6443、アプライアンス管理 Web ユーザーインターフェイス、および NGUI の TLS バージョンと暗号をカスタマイズできるようになりました。

  CLI から暗号をカスタマイズする場合は、`sslconfig` コマンドを使用できます。
- TLS 暗号が無効になる SSL 構成を修正または変更した場合は、アプリケーションを再起動します。

Procedure

ステップ 1 [システム管理（System Administration）] > [SSL 設定（SSL Configuration）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 これらのサービスで SSL v3 と TLS v1.x をイネーブルにするには、対応するチェックボックスをオンにします。

- [アプライアンス管理 Web ユーザー インターフェイス（Appliance Management Web User Interface）]：この設定を変更すると、すべてのアクティブ ユーザーの接続が切断されます。

  Note
  - プロトコルバージョンの場合、TLSv1.2 はデフォルトで有効になっています。[TLSv1.3] チェックボックスをオンにするか、`sslconfig` コマンドを使用して、TLSv1.3 を選択できるようになりました。このコマンドの詳細については、Secure Web Appliance CLI コマンドを参照してください。プロトコルバージョンとして TLSv1.3 を選択する場合は、TLSv1.3 を使用する暗号を提供する必要があります。

- [プロキシ サービス（Proxy Services）]：セキュア クライアント用の HTTPS プロキシとクレデンシャル暗号化が含まれます。このセクションには以下も含まれています。
  - [使用する暗号（Cipher(s) to Use）]：プロキシ サービスとの通信に使用する追加の暗号スイートを入力できます。スイートの区切りにはコロン（:）を使用します。特定の暗号の使用を防止するに

は、その文字列の先頭に感嘆符（!）を追加します。たとえば `!EXP-DHE-RSA-DES-CBC-SHA` と入力します。

確認済みの TLS/SSL バージョンに適切なスイートのみを入力するようにしてください。詳細および暗号リストについては、https://www.openssl.org/docs/manmaster/man1/ciphers.htmlを参照してください。

アプライアンスは TLSv1.3 バージョンをサポートしています。暗号 `TLS_AES_256_GCM_SHA384` がデフォルトの暗号リストに追加されました。デフォルトでは、TLSv1.3 はアプライアンス上で有効になります。

AsyncOS バージョン 14.0 では、暗号 `TLS_AES_128_GCM_SHA256` および `TLS_CHACHA20_POLY1305_SHA256` がデフォルトの暗号リストに追加されます。

AsyncOS バージョン 9.0 以前のデフォルトの暗号は、`DEFAULT:+kEDH` です。

AsyncOS バージョン 9.1 ～ 11.8 のデフォルトの暗号は、次のとおりです。

```
EECDH:DSS:RSA:!NULL:!eNULL:!EXPORT:!3DES:!RC4:!RC2:!DES:!SEED:!CAMELLIA
:!SRP:!IDEA:!ECDHE-ECDSA-AES256-SHA:!ECDHE-RSA-AES256-SHA:!DHE-DSS-AES256-SHA:
!AES256-SHA:DHE-RSA-AES128-SHA
```

この場合、デフォルトの暗号は ECDHE 暗号の選択によって変わる場合があります。

AsyncOS バージョン 12.0 以降のデフォルトの暗号は、次のとおりです。

```
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
```

```
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:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

Note
新しい AsyncOS バージョンにアップグレードする際に、デフォルトの暗号スイートを更新します。暗号スイートは自動的に更新されません。以前のバージョンから AsyncOS 12.0 以降にアップグレードする場合は、暗号スイートを次のように更新することを推奨します。

```
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
```

```
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:TLS_AES_128_GCM_SHA256: TLS_CHACHA20_POLY1305_SHA256
```

- [TLS 圧縮の無効化（推奨）（Disable TLS Compression (Recommended)）]：TLS 圧縮を無効にするには、このチェックボックスをオンにします。最善のセキュリティを実現するには、この設定が推奨されます。

- [セキュア LDAP サービス（Secure LDAP Services）]：認証、外部認証、およびセキュア モビリティが含まれます。
- [セキュアICAPサービス（外部DLP）（Secure ICAP Services (External DLP)）]：アプライアンスと外部 DLP （データ漏洩防止）サーバー間の ICAP 通信の保護に使用するプロトコルを選択します。詳細については、外部 DLP サーバーの設定を参照してください。

- [サービスの更新（Update Service）]：アプライアンスと利用可能なアップデート サーバー間の通信に使用するプロトコルを選択します。サービスの更新の詳細については、AsyncOS for Web のアップグレートとアップデート, on page 76を参照してください。

Note
シスコのアップデート サーバーはSSL v3をサポートしていません。したがって、TLS 1.0以上をCiscoアップデート サービスでイネーブルにしておく必要があります。ただし、ローカル アップデート サーバーでは現在も SSL v3 を使用することができます（そのように設定されている場合）。それらのサーバーでサポートされている SSL/TLS のバージョンを確認してください。

ステップ 4 [Submit] をクリックします。

証明書の管理

アプライアンスでは、デジタル証明書を使用してさまざまな接続を確立、確認、保護します。[証明書の管理（Certificate Management）] ページでは、現在の証明書リストの表示や更新、信頼できるルート証明書の管理、およびブロックされた証明書の表示を行うことができます。

Note アプライアンスがインターネットに接続されていない場合、[証明書管理（Certificate Management）] ページのロードに時間がかかり、タイムアウトエラーが発生します。さらに、証明書をロードした後、[マニフェストを取得できませんでした（Failed to fetch manifest）] ネットワークエラーが [証明書の更新（Certificate Updates）] リストに表示されます。

関連項目

- 証明書およびキーについて, on page 71
- 証明書の更新, on page 72
- 信頼できるルート証明書の管理, on page 71
- ブロックされた証明書の表示, on page 72

厳格な証明書検証について

AsyncOS 10.5 での FIPS モード更新のリリースに伴い、提示される証明書はすべて、アップロード前にコモン クライテリア（CC）標準に準拠していることを確認するため厳格に検証されます。証明書を証明書失効リストと照合して検証するには、OCSP 検証を使用できます。

適切で有効な証明書が Secure Web Applianceにアップロードされていることと、すべての関連サーバーで円滑なSSLハンドシェイクを実行できるように、有効でセキュアな証明書がすべての関連サーバーで設定されていることを確認する必要があります。

厳格な証明書検証は、次の証明書のアップロードに適用されます。

- HTTPS プロキシ（[セキュリティサービス（Security Services）]>[HTTPSプロキシ（HTTPS Proxy）]）

- ファイル分析サーバー（[セキュリティサービス（Security Services）]>[マルウェア対策とレピュテーション（Anti-Malware and Reputation）]>[ファイル分析の詳細設定（Advanced Settings for File Analysis）]>[ファイル分析サーバー（File Analysis Server）]：[プライベートクラウドおよび認証局（Private Cloud & Certificate Authority）]：[アップロードされた認証局の使用（Use Uploaded Certificate Authority）]）
- 信頼できるルート証明書（[ネットワーク（Network）]>[証明書の管理（Certificate Management）]）
- グローバル認証の設定（[ネットワーク（Network）]>[認証（Authentication）]>[グローバル認証の設定（Global Authentication Settings）]）
- SaaS の ID プロバイダ（[ネットワーク（Network）]>[SaaS のIDプロバイダ（Identity Provider for SaaS）]）
- Identity Services Engine（[ネットワーク（Network）]>[Identity Services Engine]）
- 外部 DLP サーバー（[ネットワーク（Network）]>[外部DLPサーバー（External DLP Servers）]）
- LDAP およびセキュア LDAP（[ネットワーク（Network）]>[認証（Authentication）]>[レルム（Realm）]）

FIPS Compliance （64 ページ） も参照してください。

証明書およびキーについて

ユーザーに認証を要求するときに、ブラウザはセキュア HTTPS 接続を使用して Web プロキシに認証クレデンシャルを送信します。 Secure Web Applianceは、デフォルトで付属の「Cisco Web セキュリティ アプライアンス デモ証明書（Cisco Web Security Appliance Demo Certificate）」を使用して、クライアントとの HTTPS 接続を確立します。多くのブラウザでは、証明書が無効であるという内容の警告が表示されます。無効な証明書に関するメッセージをユーザーに表示しないようにするには、アプリケーションで自動的に認識される証明書とキーのペアをアップロードします。

関連項目

- 証明書とキーのアップロードまたは生成, on page 73
- 証明書署名要求, on page 74
- 中間証明書, on page 75

信頼できるルート証明書の管理

Secure Web Applianceには、信頼できるルート証明書のリストが付属し、これが維持されます。信頼できる証明書を持つ Web サイトでは、復号は必要ありません。

信頼できる証明書のリストに証明書を追加し、機能的に証明書を削除すると、信頼できる証明書のリストを管理できます。 Secure Web Applianceでは、プライマリリストから証明書は削除

されませんが、ユーザーが証明書の信頼を無効化できます。これで、信頼できるリストから証明書が機能的に削除されます。

信頼できるルート証明書を追加、上書き、ダウンロードするには、以下の手順を実行します。

Procedure

ステップ 1 [ネットワーク（Network）] > [証明書の管理（Certificate Management）] の順に選択します。

ステップ 2 [証明書の管理（Certificate Management）] ページの [信頼できるルート証明書の管理（Manage Trusted Root Certificates）] をクリックします。

ステップ 3 シスコ認識済みリストに記載されていない認証局の署名が付いたカスタムの信頼できるルート証明書を追加するには、以下の手順を実行します。

[インポート（Import）] をクリックし、証明書ファイルを参照して選択し、[送信（Submit）] します。

ステップ 4 1 つ以上のシスコ認識済み証明書の信頼を上書きするには、以下の手順を実行します。

a) 上書きする各エントリの [信頼を上書き（Override Trust）] チェックボックスをオンにします。

b) [送信（Submit）] をクリックします。

ステップ 5 特定の証明書のコピーをダウンロードするには、以下の手順を実行します。

a) シスコの信頼できるルート証明書リストで証明書の名前をクリックし、エントリを展開します。

b) [証明書をダウンロード（Download Certificate）] をクリックします。

証明書の更新

[更新（Updates）]セクションには、アプライアンス上のシスコの信頼できるルート証明書とブロックリストのバンドルについて、バージョン情報と最終更新情報が一覧表示されます。これらのバンドルは定期的に更新されます。

Procedure

[証明書の管理（Certificate Management）] ページで [今すぐ更新（Update Now）] をクリックし、アップデート可能なすべてのバンドルを更新します。

ブロックされた証明書の表示

シスコにより無効であると判定されてブロックされた証明書のリストを表示するには、以下の手順を実行します。

Procedure

[ブロック済み証明書を表示（View Blocked Certificates）] をクリックします。

証明書とキーのアップロードまたは生成

一部のAsyncOS機能では、接続の確立、確認、または保護のために証明書とキーが必要です。たとえば、Identity Services Engine（ISE）などの機能がこれに該当します。既存の証明書とキーをアップロードしたり、機能を設定するときに新しい証明書とキーを生成したりできます。

証明書およびキーのアップロード

アプライアンスにアップロードする証明書は、以下の要件を満たしている必要があります。

- X.509 標準を使用していること。
- 一致する秘密キーが PEM 形式で含まれていること。DER 形式はサポートされていません。

Procedure

ステップ 1 [アップロードされた証明書とキーを使用（Use Uploaded Certificate and Key）] を選択します。

ステップ 2 [証明書（Certificate] フィールドで [参照（Browse）]をクリックし、アップロードするファイルを検索します。

Note
Web プロキシは、ファイル内の最初の証明書またはキーを使用します。証明書ファイルは PEM 形式にする必要があります。DER 形式はサポートされていません。

ステップ 3 [キー（Key）] フィールドで [参照（Browse）] をクリックし、アップロードするファイルを指定します。

Note
キーの長さは 512、1024、または 2048 ビットである必要があります。秘密キー ファイルは PEM 形式でなければなりません。DER 形式はサポートされていません。

ステップ 4 キーが暗号化されている場合は、[キーは暗号化されています（Key is Encrypted）] を選択します。

ステップ 5 [ファイルのアップロード（Upload File）] をクリックします。

証明書およびキーの生成

Procedure

ステップ 1 [生成された証明書とキーを使用（Use Generated Certificate and Key）] を選択します。

ステップ 2 [新しい証明書とキーを生成（Generate New Certificate and Key）] をクリックします。

a) [証明書とキーを生成（Generate Certificate and Key）] ダイアログボックスで、必要な生成情報を入力します。

Note
[共通名（Common Name）] フィールドには、スラッシュ（/）を除く任意の ASCII 文字を入力できます。

b) [証明書とキーを生成（Generate Certificate and Key）] ダイアログボックスで、[生成（Generate）] をクリックします。

生成が完了すると、[証明書（Certificate）] セクションに、証明書の情報と 2 つのリンク（[証明書をダウンロードDownload Certificate] と [証明書署名要求のダウンロード（Download Certificate Signing Request）]）が表示されます。また、認証局（CA）から署名付き証明書を受信したときに、それをアップロードするために使用する [署名付き証明書（Signed Certificate）] オプションも表示されます。

ステップ 3 [証明書をダウンロードDownload Certificate] をクリックして、アプライアンスにアップロードする新しい証明書をダウンロードします。

ステップ 4 [証明書署名要求のダウンロード（Download Certificate Signing Request）] をクリックして、署名のために認証局（CA）に送信する新しい証明書ファイルをダウンロードします。この処理の詳細については、証明書署名要求, on page 74を参照してください。

a) CA から署名付き証明書が返送されたら、[証明書（Certificate）] フィールドの [署名付き証明書（Signed Certificate）] で [参照（Browse）] をクリックして、署名付き証明書ファイルを指定し、[ファイルのアップロード（Upload File）] をクリックしてアプライアンスにアップロードします。

b) CA のルート証明書がアプライアンスの信頼できるルート証明書リストに含まれていることを確認します。リストにない場合は追加します。詳細については、信頼できるルート証明書の管理, on page 71を参照してください。

証明書署名要求

Secure Web Applianceは、アプライアンスにアップロードされた証明書の証明書署名要求（CSR）を生成することはできません。そのため、アプライアンス用に作成された証明書を使用するには、別のシステムから署名要求を発行する必要があります。後でアプライアンスにインストールする必要があるため、このシステムから PEM 形式のキーを保存します。

最新バージョンの OpenSSL がインストールされた、任意の UNIX マシンを使用できます。CSR にアプライアンスのホスト名があることを確認してください。OpenSSL を使用した CSR の生成の詳細については、以下の場所にあるガイドラインを参照してください。

`http://www.modssl.org/docs/2.8/ssl_faq.html#ToC28`

CSR が生成されたら、認証局（CA）に送信します。CA は、証明書を PEM 形式で返します。

初めて証明書を取得する場合は、インターネットで「certificate authority services SSL server certificates（SSL サーバー証明書を提供している認証局）」を検索して、環境のニーズに最も適したサービスを選択します。サービスの手順に従って、SSL 証明書を取得します。

Note 独自の証明書を生成して署名することもできます。そのためのツールは`http://www.openssl.org`の無料のソフトウェア OpenSSL に含まれています。

中間証明書

ルート認証局(CA)の証明書検証に加えて、AsyncOS では、中間証明書の検証の使用もサポートされます。中間証明書とは信頼できるルート認証局によって発行された証明書であり、追加の証明書を作成するために使用されます。これは、信頼の連鎖を作成します。たとえば、信頼できるルート認証局によって証明書を発行する権利が与えられた example.com によって証明書が発行されたとします。example.com によって発行された証明書は、example.com の秘密キーおよび信頼できるルート認証局の秘密キーと照合して検証する必要があります。

サーバーは、SSL ハンドシェイクで「証明書チェーン」を送信し、クライアント（ブラウザなど。この場合は HTTPS プロキシである Secure Web Appliance）がサーバーを認証できるようにします。通常、サーバー証明書は中間証明書により署名され、中間証明書は信頼できるルート証明書により署名され、ハンドシェイク中にサーバー証明書と全体の証明書チェーンがクライアントに表示されます。通常、ルート証明書は Secure Web Applianceの信頼できる証明書ストアに存在するため、証明書チェーンの検証は成功します。

ただし、サーバーでエンドポイントエンティティ証明書が変更された場合、新しいチェーンに必要な更新が実行されません。その結果、サーバーは SSL ハンドシェイク中にサーバー証明書のみを表示し、 Secure Web Appliance プロキシは中間証明書が存在しないため証明書チェーンを検証できません。

以前のソリューションでは、 Secure Web Appliance管理者が手動で介入し、信頼できる証明書ストアに必要な中間証明書をアップロードしていました。現在は、CLI コマンド `advancedproxyconfig > HTTPS > Do you want to enable automatic discovery and download of missing Intermediate Certificates?` を使用して、「中間証明書の検出」を有効にできます。これは、 Secure Web Applianceがこれらの状況で手動手順を排除しようとするために使用するプロセスです。

中間証明書の検出では、「AIA 追跡」という方法を使用します。この方法では、信頼できない証明書が存在する場合、 Secure Web Applianceはその証明書に「Authority Information Access」という拡張情報があるか検証します。この拡張情報には、オプションの CA 発行者の URI フィールドが含まれています。このフィールドには、問題のサーバー証明書の署名に使用される発行者証明書を照会することができます。これが使用可能になると、 Secure Web Applianceはルートの CA 証明書が取得されるまで発行者の証明書を再帰的に取得し、チェーンを再度検証しようとします。

AsyncOS for Web のアップグレードとアップデート

シスコでは、AsyncOS for Web とそのコンポーネント向けに、アップグレード（新しいソフトウェア バージョン）とアップデート（現在のソフトウェア バージョンの変更）を定期的にリリースしています。

Note TLSv1.0 と TLSv1.1 は、プロキシ構成以外の SSL 構成ではサポートされなくなりました。AsyncOS をアップグレードする前に、TLS バージョンを TLSv1.2 以降に変更する必要があります。

AsyncOS for Web をアップグレードするためのベスト プラクティス

- アップグレードを開始する前に、[システム管理（System Administration）] > [設定ファイル（Configuration File）] ページまたは saveconfig コマンドを使用して、 Secure Web Appliance から XML コンフィギュレーション ファイルを保存します。
- PAC ファイルやカスタマイズしたエンドユーザー通知ページなど、アプライアンスに格納されている他のファイルを保存します。
- アップグレード時には、さまざまなプロンプトで長い時間作業を中断しないでください。TCP セッションがダウンロード中にタイムアウトしてしまった場合、アップグレードが失敗する可能性があります。
- アップグレードが完了したら、XML ファイルに設定情報を保存します。

関連項目

- アプライアンス設定の保存、ロード、およびリセット, on page 2

AsyncOS およびセキュリティ サービス コンポーネントのアップグレードとアップデート

アップグレードのダウンロードとインストール

始める前に

アプライアンスのコンフィギュレーション ファイルを保存します（アプライアンス設定の保存、ロード、およびリセット （2 ページ）を参照）。

（注） AsyncOS を Cisco サーバーからではなくローカル サーバーから 1 回の操作でダウンロードとアップグレードする場合は、アップグレードはダウンロード中に即座に実行されます。アップグレード プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレードプロセスを終了できます。

（注） アップグレードの実行中、セキュア認証の証明書が FIPS 準拠でない場合は、アプライアンスがアップグレードされる最新パスのデフォルトの証明書で置き換えられます。これは、お客様がアップグレードの前にデフォルトの証明書を使用した場合にのみ起こります。

1 回の操作でダウンロードとインストールを行うか、またはバックグラウンドでダウンロードし後でインストールできます。

varstore ファイルに保存されている設定値に ASCII 以外の文字が含まれていると、アップグレードが失敗します。

手順

ステップ 1 [システム管理（System Administration）] > [システム アップグレード（System Upgrade）] を選択します。

ステップ 2 [アップグレードオプション（Upgrade Options）] をクリックします。

アップグレード オプションとアップグレード イメージを選択します。

設定	説明
アップグレード オプションの選択	• [ダウンロードとインストール（Download and install）] : 1 回の操作でアップグレードをダウンロードしてインストールします。 すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。 • [ダウンロードのみ（Download only）] : アップグレードインストーラをダウンロードしますが、インストールは行いません。 すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。インストーラはサービスを中断することなく、バックグラウンドでダウンロードします。 ダウンロードが完了すると、[インストール（Install）] ボタンが表示されます。このボタンをクリックして、ダウンロードしたアップグレードをインストールします。
	[アップグレード サーバーで使用可能なアップグレード イメージファイルのリスト（List of available upgrade images files at upgrade server）] から、ダウンロードするアップグレードイメージを選択するか、ダウンロードしてインストールしたアップグレード イメージを選択します。

設定	説明
アップグレードの準備	• 現在の設定のバックアップ コピーをアプライアンス上の **configuration** ディレクトリに保存するには、[アップグレードする前に、現在の設定を configuration ディレクトリに保存（Save the current configuration to the configuration directory before upgrading）] をオンにします。 • [現在の設定を保存（Save current configuration）] オプションがオンになっている場合、[設定ファイル内のパスワードを隠す（Mask passwords in the configuration file）] をオンにしてバックアップ コピー内の現在のすべての構成パフワードをマスクすることができます。ただし、パスワードがマスクされた構成ファイルは、[設定をロード（Load Configuration）] コマンドでも、CLI **loadconfig** コマンドでもロードすることができません。 FIPS モードが有効にされている場合、[設定ファイル内のパスワードを暗号化する（Encrypt passphrases in the Configuration Files）] をオンにすることができます。これらのファイルは、リロードすることができます。 • [現在の設定を保存（Save current configuration）] オプションがオンになっている場合、[ファイルをメールで送信（Email file to）] フィールドに 1 つ以上の電子メールアドレスを入力できます。入力した各アドレスに、バックアップ設定ファイルのコピーが電子メールで送信されます。カンマで複数のアドレスを区切ります。

ステップ 3 [続行（Proceed）] をクリックします。

インストール中の場合、次に従います。

a) プロセス中のプロンプトに応答できるようにしてください。
b) 完了を求めるプロンプトで、[今すぐ再起動（Reboot Now）] をクリックします。
c) 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。

アップグレードの問題を修正するためにアプライアンスの電源を再投入する必要があると思われる場合は、再起動後 20 分以上が経過してから再投入してください。

バックグラウンド ダウンロードのキャンセルまたは削除ステータスの表示

手順

ステップ 1 [システム管理（System Administration）] > [システム アップグレード（System Upgrade）] を選択します。
ステップ 2 [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 次のオプションを選択します。

目的	操作手順
ダウンロード ステータスの表示	ページの中央を確認してください。 進行中のダウンロードおよびダウンロードが完了してインストールされるのを待っているものがない場合は、ダウンロードのステータス情報は表示されません。
ダウンロードのキャンセル	ページの中央にある、[ダウンロードをキャンセル（Cancel Download）] ボタンをクリックします。 このオプションは、ダウンロード進行中にのみ表示されます。
ダウンロードされたインストーラの削除	ページの中央にある、[ファイルを削除（Delete File）] ボタンをクリックします。 このオプションは、インストーラがダウンロードされている場合にのみ表示されます。

ステップ 4 （オプション）アップグレード ログを確認します。

次のタスク

関連項目

- ローカルおよびリモート アップデート サーバ （80 ページ）

自動および手動によるアップデート/アップグレードのクエリー

AsyncOS は、新しい AsyncOS アップグレードを除く、すべてのセキュリティ サービス コンポーネントへの新しいアップデートがないか、定期的にアップデート サーバに問い合わせます。AsyncOS をアップグレードするには、AsyncOS が使用可能なアップグレードを問い合わせるよう、手動で要求する必要があります。AsyncOS が使用可能なセキュリティ サービス アップデートを問い合わせるよう、手動で要求することもできます。詳細については、以前のバージョンの AsyncOS for Web への復元, on page 85を参照してください。

AsyncOS がアップデートまたはアップグレードのアップデート サーバを照会する場合は、以下の手順を実行します。

1. アップデート サーバに問い合わせます。

   シスコでは、アップデート サーバに以下のソースを使用できます。

   - **Cisco アップデート サーバ。**詳細については、Cisco アップデート サーバからのアップデートとアップグレード, on page 81を参照してください。
   - **ローカル サーバ。**詳細については、ローカル サーバからのアップグレード, on page 82を参照してください。

2. 入手可能なアップデートまたはAsyncOSのアップグレードバージョンを一覧表示するXMLファイルを受信します。この XML ファイルは「マニフェスト」と呼ばれます。

3. アップデートまたはアップグレード イメージ ファイルをダウンロードします。

セキュリティ サービスのコンポーネントの手動による更新

デフォルトでは、各セキュリティ サービス コンポーネントは、Cisco アップデート サーバからデータベース テーブルに定期的にアップデートを受信します。ただし、手動でデータベース テーブルを更新できます。

Note 一部のアップデートは、機能に関連する GUI ページからオンデマンドで利用できます。

Tip アップデータ ログ ファイルのアップデート アクティビティの記録を表示してください。[システム管理（System Administration）] > [ログ サブスクリプション（Log Subscriptions）] ページのアップデータ ログ ファイルに登録します。

Note 処理中のアップデートは中断できません。すべての処理中のアップデートは、新しい変更が適用される前に完了する必要があります。

Procedure

ステップ 1 **[システム管理（System Administration）] > [アップグレードとアップデートの設定（Upgrade and Update Settings）]** を選択します。

ステップ 2 **[更新設定を編集（Edit Update Settings）]** をクリックします。

ステップ 3 アップデート ファイルの場所を指定します。

ステップ 4 [セキュリティ サービス（Security Services）] タブにあるコンポーネント ページの [今すぐ更新（Update Now）] 機能キーを使用してアップデートを開始します。たとえば、[セキュリティ サービス（Security Services）] > [Web レピュテーション フィルタ（Web Reputation Filters）] ページです。

更新プロセス中、CLI および Web アプリケーション インターフェイスは、応答が遅くなったり、使用できなくなったりする場合があります。

ローカルおよびリモート アップデート サーバ

デフォルトでは、AsyncOS は、アップデート イメージとアップグレード イメージおよびマニフェスト XML ファイルについて、Cisco アップデート サーバに問い合わせます。ただし、アップグレード イメージ、アップデート イメージおよびマニフェスト ファイルをダウンロードする場所を選択できます。以下の理由から、イメージ ファイルまたはマニフェスト ファイルにローカル アップデート サーバを使用します。

- **同時にアップグレードするアプライアンスが複数あります。**ネットワーク内の Web サーバにアップグレードイメージをダウンロードして、ネットワーク内のすべてのアプライアンスに使用できます。
- **ファイアウォールの設定には、Cisco アップデート サーバのスタティック IP アドレスが必要です。**Cisco アップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。詳細については、Cisco アップデート サーバのスタティック アドレスの設定, on page 81を参照してください。

Note ローカル アップデート サーバはセキュリティ サービスのアップデートを自動的に受信しません。AsyncOS のアップグレードのみを受信します。AsyncOS のアップグレードにローカルアップデート サーバを使用した後は、アップデートとアップグレードの設定を変更して、再び Cisco アップデート サーバを使用するようにします。これにより、セキュリティ サービスが再び自動的にアップデートされるようになります。

Cisco アップデート サーバからのアップデートとアップグレード

Secure Web Applianceは、Cisco アップデート サーバに直接接続して、アップグレード イメージとセキュリティ サービス アップデートをダウンロードできます。各アプライアンスは、個別にアップデートとアップグレードをダウンロードします。

Cisco アップデート サーバのスタティック アドレスの設定

Cisco アップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、アップデートおよび AsyncOS アップグレードに対して静的な参照先を設定する必要がある場合があります。

Procedure

ステップ 1 シスコ カスタマー サポートに問い合わせて、スタティック URL アドレスを取得します。

ステップ 2 [システム管理（System Administration）] > [アップグレードとアップデートの設定（Upgrade and Update Settings）] ページの順に進み、[更新設定を編集（Edit Update Settings）] をクリックします。

ステップ 3 [アップデート設定を編集（Edit Update Settings）] ページの [アップデートサーバ（イメージ）（Update Servers (images)）] セクションで、[ローカルアップデートサーバ（Local Update Servers）] を選択し、ステップ 1 で取得したスタティック URL アドレスを入力します。

ステップ 4 [アップデート サーバ（リスト）（Update Servers (list)）] セクションで Cisco アップデート サーバが選択されていることを確認します。

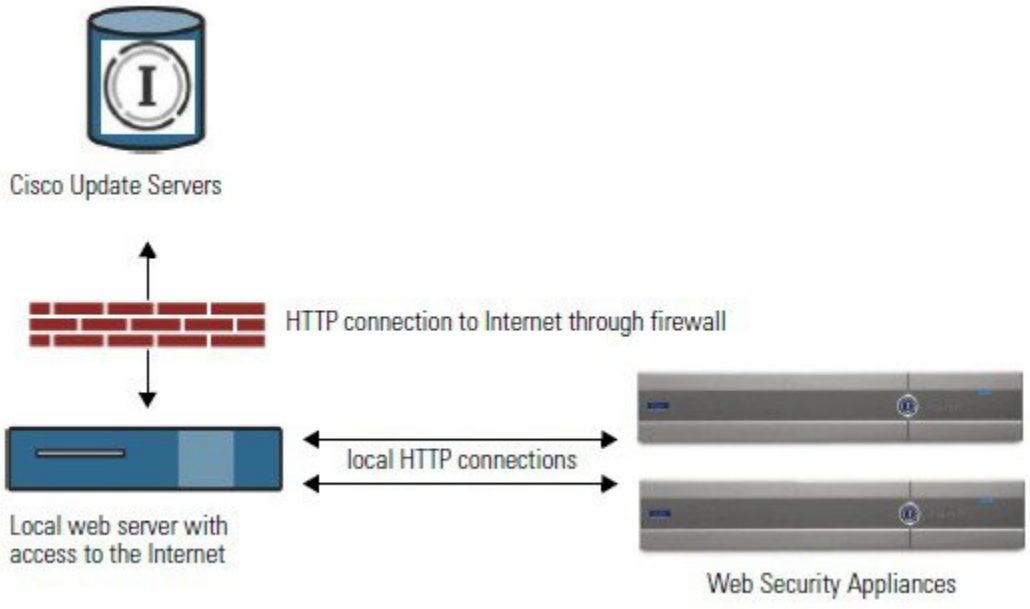
ステップ 5 変更を送信し、保存します。

ローカル サーバからのアップグレード

Secure Web Applianceは、Cisco アップデート サーバからアップグレードを直接取得する代わりに、ネットワーク内のサーバから AsyncOS のアップグレードをダウンロードできます。この機能を使用すると、シスコから1回だけアップグレードイメージをダウンロードして、ネットワーク内のすべての Secure Web Applianceでそれを使用することができます。

次の図に、 Secure Web Applianceでローカルサーバーからアップグレードイメージをダウンロードする方法を示します。

Figure 1: ローカル サーバからのアップグレード



ローカル アップグレード サーバーのハードウェアおよびソフトウェア要件

AsyncOS アップグレードファイルのダウンロードでは、Web ブラウザを備えた内部ネットワークにシステムを構築する必要があり、Cisco アップデート サーバーへのインターネット アクセスが必要になります。

Note このアドレスへの HTTP アクセスを許可するファイアウォール設定値を設定する必要がある場合、特定の IP アドレスではなく DNS 名を使用して設定する必要があります。

AsyncOS アップグレード ファイルのホスティングでは、内部ネットワーク上のサーバーは、以下の機能を持つ Microsoft IIS（Internet Information Services）などの Web サーバーまたは Apache のオープン ソース サーバーを持つ必要があります。

- 24 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
- ディレクトリの参照ができること

- 匿名（認証なし）または基本（「簡易」）認証用に設定されている
- 各 AsyncOS アップデート イメージ用に最低 350 MB 以上の空きディスク領域が存在すること

ローカル サーバーからのアップグレードの設定

Note アップグレードの完了後にセキュリティ サービス コンポーネントが引き続き自動更新されるように、アップデートとアップグレードの設定を変更して、Cisco アップデート サーバー（ダイナミックまたはスタティック アドレスを使用）を使用することを推奨します。

Procedure

ステップ 1 アップグレード ファイルを取得および供給するようにローカル サーバーを設定します。

ステップ 2 アップグレード zip ファイルをダウンロードします。

ローカル サーバー上のブラウザを使用して、http://updates.ironport.com/fetch_manifest.html にアクセスしてアップグレード イメージの zip ファイルをダウンロードします。イメージをダウンロードするには、シリアル番号（物理アプライアンス用）または VLN（仮想アプライアンス用）およびアプライアンスのバージョン番号を入力します。利用可能なアップグレードのリストが表示されます。ダウンロードするアップグレード バージョンをクリックします。

ステップ 3 ディレクトリ構造を変更せずにローカル サーバーのルート ディレクトリにある ZIP ファイルを解凍します。

ステップ 4 [システム管理（System Administration）] > [アップグレードとアップデートの設定（Upgrade and Update Settings）] ページまたは **updateconfig** コマンドを使用して、ローカル サーバーを使用するようにアプライアンスを設定します。

ステップ 5 [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、[使用可能なアップグレード（Available Upgrades）] をクリックするか、**upgrade** コマンドを実行します。

ローカルとリモートにおけるアップグレード方法の相違

以下の相違点は、Cisco アップデート サーバーからではなく、ローカル サーバーから AsyncOS をアップグレードする場合に該当します。

- ダウンロード中に、アップグレードによるインストールがすぐに実行されます。
- アップグレード プロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Control を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

アップグレードおよびサービス アップデートの設定

Secure Web Applianceがセキュリティ サービス アップデートやAsyncOS for Web のアップグレードをダウンロードする方法を設定できます。たとえば、ファイルをダウンロードするときに使用するネットワーク インターフェイスを選択したり、アップデート間隔を設定したり、自動アップデートをディセーブルにしたりできます。

Procedure

ステップ 1 **[システム管理（System Administration）] > [アップグレードとアップデートの設定（Upgrade and Update Settings）]** を選択します。

ステップ 2 **[更新設定を編集（Edit Update Settings）]** をクリックします。

ステップ 3 以下の情報を参考にして、設定値を設定します。

設定	説明
自動更新	セキュリティ コンポーネントの自動アップデートをイネーブルにするかどうかを選択します。自動更新を選択する場合、時間間隔を入力します。デフォルトはイネーブルで、更新間隔は 5 分です。
アップグレードの通知（Upgrade Notifications）	AsyncOS への新規のアップグレードが入手可能である場合に、Web インターフェイスの上部に通知を表示するかどうかを選択します。アプライアンスは、管理者に対してのみこの通知を表示します。 詳細については、AsyncOS for Web のアップグレードとアップデート, on page 76を参照してください。
アップデート サーバ（リスト）（Update Servers (list)）	利用可能なアップグレードとアップデートのリスト（マニフェスト XML ファイル）を、Cisco アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。 ローカル アップデート サーバを選択した場合、サーバのファイル名およびポート番号を含む、リストのマニフェスト XML ファイルの完全なパスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合は、有効なユーザ名とパスフレーズも入力できます。
アップデート サーバ（イメージ）（Update Servers (images)）	アップグレード イメージやアップデート イメージを、Cisco アップデート サーバまたはローカル Web サーバのどちらからダウンロードするかを選択します。 ローカル アップデート サーバを選択した場合は、サーバのベース URL とポート番号を入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合は、有効なユーザ名とパスフレーズも入力できます。
着信サービス一覧（Routing Table）	アップデート サーバに接続するときに、どのネットワーク インターフェイスのルーティング テーブルを使用するかを選択します。

設定	説明
プロキシ サーバ（Proxy Server）（オプション）	アップストリーム プロキシ サーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスフレーズをここに入力します。

ステップ 4 変更を送信し、保存します。

What to do next

関連項目

- ローカルおよびリモート アップデート サーバ, on page 80
- 自動および手動によるアップデート/アップグレードのクエリー, on page 79
- AsyncOS およびセキュリティ サービス コンポーネントのアップグレードとアップデート, on page 76

以前のバージョンの AsyncOS for Web への復元

Web 用 AsyncOS には、緊急時に Web 用オペレーティング システム AsyncOS を以前の認定済みのビルドに戻す機能があります。

Note バージョン 7.5 よりも前の Web 用 AsyncOS のバージョンには戻せません。

仮想アプライアンスの AsyncOS を復元した場合のライセンスへの影響

AsyncOS 8.0 に復元した場合、アプライアンスがセキュリティ機能なしで Web トランザクションを処理する 180 日の猶予期間はありません。ライセンスの有効期限は影響を受けません。

復元プロセスでのコンフィギュレーション ファイルの使用

バージョン7.5で有効であり、それ以降のバージョンにアップグレードする場合、アップグレード プロセスは Secure Web Applianceのファイルに現在のシステム設定を自動的に保存します（ただし、バックアップとして、コンフィギュレーション ファイルをローカル マシンに手動で保存することを推奨します）。これによって、以前のバージョンに復元した後、AsyncOS for Web が以前のリリースに関連するコンフィギュレーション ファイルをロードできます。ただし、復元を実行すると、管理インターフェイスに現在のネットワーク設定を使用します。

SMA によって管理されるアプライアンスの AsyncOS の復元

Secure Web Applianceから Web 用 AsyncOS に復元することができます。ただし Secure Web Applianceがセキュリティ管理アプライアンスで管理されている場合は、以下のルールとガイドラインを考慮してください。

- 中央集中型レポーティングを Secure Web Applianceでイネーブルにすると、Web 用 AsyncOS は復帰を開始する前にセキュリティ管理アプライアンスへのレポートデータの転送を終了します。セキュリティ管理アプライアンスへのファイルの転送に40秒以上かかる場合は、Web 用 AsyncOS がファイルの転送をこのまま待機するように促すか、すべてのファイルを転送せずに復帰を続けます。
- 復元後、適切なプライマリ構成に Secure Web Applianceを関連付ける必要があります。それ以外の場合、セキュリティ管理アプライアンスから Secure Web Applianceに設定をプッシュすると失敗する可能性があります。

以前のバージョンへの Web 用の AsyncOS の復元

Caution Secure Web Applianceのオペレーティング システムの復元は非常に破壊的な操作であり、すべての設定ログとデータベースが削除されます。さらに、アプライアンスが再設定されるまで、復元によって Web トラフィック処理が中断されます。初期の Secure Web Appliance設定に応じて、この操作がネットワークの設定を破壊する場合があります。このような場合、復元の実行後にアプライアンスへの物理的なローカル アクセスが必要になります。

Caution Cisco Secure Web Appliance のオペレーティングシステムをスマートライセンスが有効になっている以前のバージョンに復元する場合、スマートライセンスの設定は保持されません。以前の AsyncOS バージョンに正常に復元したら、スマートライセンスを有効にして CSSM ポータルに登録する必要があります。スマート ソフトウェア ライセンシングをアクティブ化したときに [特定/永久ライセンスの予約（Specific/Permanent License Reservation）] オプションを選択した場合は、操作の復元の前にアプライアンスで使用されているライセンスを解放し、CSSM ポータルからアプライアンスを登録解除することをお勧めします。復元操作の前にライセンスを解放しなかった場合、またはアプライアンスを登録解除しなかった場合は、シスコサポートに連絡してサポートを受けることができます。

Note URL カテゴリ セットのアップデートが利用可能な場合は、AsyncOS の復元後にそれらが適用されます。

Before you begin

- Cisco Quality Assurance に問い合わせて、目的とする復元が実行可能かどうかを確認してください。（BS：これは、元のトピックの「使用可能なバージョン」セクションの要約です。これが正確かどうか質問済みです。）
- Secure Web Applianceから別のマシンに以下の情報をバックアップします。
  - システム コンフィギュレーション ファイル（パスフレーズをマスクしない状態）。
  - 保持するログ ファイル。

- 保持するレポート。
- アプライアンスに保存されるカスタマイズされたエンド ユーザー通知ページ。
- アプライアンス上に格納されている PAC ファイル。

Procedure

ステップ 1 バージョンを戻すアプライアンスの CLI にログインします。

Note
次のステップで `revert` コマンドの実行するときに、いくつかの警告プロンプトが発行されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元に向けた準備手順が完了するまで、復元プロセスを開始しないてください。

ステップ 2 `revert` コマンドを入力します。

ステップ 3 復元で続行するアプライアンスを 2 回確認します。

ステップ 4 戻る利用可能なバージョンの 1 つを選択します。

アプライアンスが 2 回リブートします。

Note
復元プロセスは時間のかかる処理です。復元が完了して、アプライアンスへのコンソール アクセスが再び利用可能になるまでには、15 ～ 20 分かかります。

アプライアンスは、選択された Web バージョンの AsyncOS を使用して稼働します。Web ブラウザから Web インターフェイスにアクセスできます。

SNMP を使用したシステムの状態のモニタリング

AsyncOS オペレーティング システムは、SNMP（シンプル ネットワーク管理プロトコル）を使用したシステム ステータスのモニターリングをサポートしています。（SNMP の詳細については、RFC 1065、1066、および 1067 を参照してください）。

以下の点に注意してください。

- SNMP は、デフォルトで**オフ**になります。
- SNMP SET 動作（コンフィギュレーション）は実装されません。
- AsyncOS は SNMPv1、v2、および v3 をサポートしています。SNMPv3 の詳細については、RFC 2571-2575 を参照してください。
- SNMPv3 をイネーブルにする場合、メッセージ認証と暗号化は必須です。認証のパスフレーズと暗号は異なっていなければなりません。暗号化アルゴリズムには AES（推奨）または DES を指定できます。認証アルゴリズムには SHA-1（推奨）または MD5 を指定でき

ます。次に snmpconfig コマンドを実行するときは、コマンドにこのパスフレーズが「記憶」されています。

- 15.0 より前の AsyncOS リリースの場合：

  SNMPv3 ユーザー名は v3get です。

```
> snmpwalk -v 3 -l AuthNoPriv -u v3get -a MD5 serv.example.com
```

- AsyncOS リリース 15.0 以降の場合：

  デフォルトの SNMPv3 ユーザー名は v3get です。管理者は、他のユーザー名を選択できます。

```
> snmpwalk -v 3 -l AuthNoPriv -u <username> -a MD5 serv.example.com
```

- SNMPv1 または SNMPv2 のみを使用する場合は、コミュニティ ストリングを設定する必要があります。コミュニティ ストリングは、`public` にデフォルト設定されません。
- SNMPv1 および SNMPv2 の場合、どのネットワークからの SNMP GET 要求を受け入れるかを指定する必要があります。
- トラップを使用するには、SNMP マネージャ（AsyncOS には含まれていません）が実行中であり、その IP アドレスがトラップ ターゲットとして入力されている必要があります（ホスト名を使用できますが、その場合、トラップは DNS が動作しているときに限り機能します）。

MIB ファイル

MIB ファイルは http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html から入手できます。

各 MIB ファイルの最新バージョンを使用します。

以下の複数の MIB ファイルがあります。

- syncoswebsecurityappliance-mib.txt： Secure Web Appliance用のエンタープライズ MIB の SNMPv2 互換の説明。
- ASYNCOS-MAIL-MIB.txt：電子メール セキュリティ アプライアンス用のエンタープライズ MIB の SNMPv2 互換の説明。
- IRONPORT-SMI.txt：この「管理情報構造」ファイルは、asyncoswebsecurityappliance-mib の役割を定義します。

このリリースには、RFC 1213 および 1907 に規定されている MIB-II の読み取り専用のサブセットが実装されています。

SNMP を使用してアプライアンスで CPU 使用率をモニターリングする方法については、https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118415-technote-wsa-00.html を参照してください。

SNMP モニターリングのイネーブル化と設定

アプライアンスのシステム ステータス情報を収集するように SNMP を設定するには、コマンドライン インターフェイス（CLI）で snmpconfig コマンドを使用します。インターフェイスの値を選択し、設定し終えると、アプライアンスは SNMPv3 GET 要求に応答します。

SNMP モニターリングを使用する場合、以下の点に注意してください。

- これらのバージョン 3 要求には、一致するパスフレーズが含まれている必要があります。
- デフォルトでは、バージョン 1 および 2 要求は拒否されます。
- イネーブルにする場合は、バージョン 1 および 2 要求に一致するコミュニティ ストリングが含まれている必要があります。

ハードウェア オブジェクト

Intelligent Platform Management Interface Specification（IPMI）準拠のハードウェア センサーによって、温度、ファン スピード、電源モジュール ステータスなどの情報が報告されます。

モニターリング可能なハードウェア関連のオブジェクト（ファンの数や動作温度範囲など）を決定するには、アプライアンス モデルのハードウェア ガイドを参照してください。

関連項目

- ドキュメント セット

SNMP トラップ

SNMP には、1 つまたは複数の条件が合致したときにトラップ（または通知）を送信して管理アプリケーションに知らせる機能が備わっています。トラップとは、トラップを送信するシステムのコンポーネントに関するデータを含むネットワーク パケットです。トラップは、SNMP エージェント（この場合は Cisco Secure Web Appliance）で、ある条件が満たされた場合に生成されます。条件が満たされると、SNMP エージェントは SNMP パケットを形成し、SNMP 管理コンソール ソフトウェアが稼働するホストに送信します。

インターフェイスに対して SNMP をイネーブルにするときに、SNMP トラップを設定（特定のトラップをイネーブル化またはディセーブル化）できます。

複数のトラップ ターゲットの指定方法：トラップ ターゲットの入力を求められたときに、カンマで区切った IP アドレスを 10 個まで入力できます。

関連項目

- SNMP の connectivityFailure トラップについて , on page 89

SNMP の connectivityFailure トラップについて

connectivityFailure トラップは、インターネットへのアプライアンスの接続をモニターするために使用されます。これは、5～7 秒ごとに 1 つの外部サーバーに接続して HTTP GET 要求を送信する試みにより実行されます。デフォルトでは、モニターされる URL はポート 80 上の `downloads.ironport.com` です。

モニターする URL またはポートを変更するには、snmpconfig コマンドを実行し、connecivityFailure トラップをイネーブルにします（すでにイネーブルになっている場合も実行します）。URL を変更するプロンプトが表示されます。

Tip connectivityFailure トラップをシミュレートするために、dnsconfig CLI コマンドを使用して、未使用の DNS サーバーを入力することができます。downloads.ironport.com の検索は失敗し、5～7秒ごとにトラップが送信されます。テストが完了したら、DNS サーバを使用中のサーバーに戻してください。

CLI の例：snmpconfig

```
Do you want to enable SNMP? [Y]>

Please choose an IP interface for SNMP requests.
1. Management (10.10.192.43/24 on Management: wsa033.cs1)
[1]>

Which port shall the SNMP daemon listen on?
[161]>

Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]>

Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]>

Enter the SNMPv3 username or press return to leave it unchanged.
[v3get]>

.
.
.
```

Web トラフィック タップ（Web Traffic Tap）

開始する前に：Web トラフィック タップ機能を有効にすると、アプライアンスがタップ インターフェイスにメッセージをコピーするための追加の CPU サイクルとメモリが必要になり、アプライアンスのトランザクション処理容量（1 秒あたりのリクエスト）が低下することになります。

（注） Web トラフィック タップ機能によるパフォーマンスの影響を低減するには、適切な Web トラフィック タップ ポリシーを設定し、タップされるトラフィックの量を減らします。

この機能は、Amazon Web Services（AWS）ではサポートされません。

Web トラフィックタップ機能により、アプライアンスをパススルーする HTTP および HTTPS の Web トラフィックがタップ可能になり、リアル タイム データ トラフィックとともに Secure Web Appliance インターフェイスにインラインでコピーすることができます。タップされたトラフィックデータを送信する Secure Web Appliance インターフェイスを選択することができます。タップされたトラフィックに HTTPS のデータが含まれている場合、タップ インターフェイスに送信する前に、アプライアンスによって復号ポリシーに基づいて復号されます。復号ポリシーを参照してください。

選択されたタップインターフェイスは、分析、調査、およびアーカイブのため、外部のセキュリティ デバイスに直接接続する必要があります。または、専用の VLAN 上の L2 スイッチに接続します。

（注） タップインターフェイスにミラーリングされたトラフィックは、イーサネット層経由でブロードキャストされ、IP ルーティングに対応していません。したがって、L2 スイッチに接続する場合は、専用の VLAN が必要です。

この機能では、Web トラフィック タップ ポリシーを設定することもできます。お客様によって定義されたこれらのポリシー フィルタに基づき、アプライアンスは外部のセキュリティ デバイスで使用可能な Web トラフィックをミラーリングします。Web トラフィック タップ機能により、HTTPS トラフィックへの可視性が実現します。

タッピングという用語は、直接接続されたクライアントとサーバー間で発生した場合、完全な TCP（Transmission Control Protocol）ストリームの再構築を指します。

仮想 Secure Web Applianceでは、Web トラフィックタップ機能がサポートされます。

（注） SSL トラフィックの検査アクションは、企業ポリシーのガイドランおよび/または国の法令に従う必要が生じる場合があります。シスコはどのような法的義務も負わず、そのような法的要件またはポリシー要件に従って Secure Web Applianceの Web トラフィックタップ機能を使用することには、使用者が単独で責任を負います。

アプライアンスを使用して Web トラフィックにタップするには、次の手順を実行する必要があります。

1. Web トラフィック タップ機能の有効化
2. Web トラフィック タップ ポリシーの設定

関連項目

- Web トラフィック タップの有効化 （92 ページ）
- Web トラフィック タップ ポリシーの設定 （93 ページ）

Web トラフィック タップの有効化

始める前に

Web トラフィック タップ機能はデフォルトでは無効になっています。Web トラフィック タップ ポリシーを定義する前に、[Web セキュリティ マネージャ（Web Security Manager）] > [Web トラフィック タップ ポリシー（Web Traffic Tap Policies）] を使用して、Web トラフィック タップ機能を有効にする必要があります。

（注） HTTPS トランザクションをタップするには、復号ポリシーを定義する必要があります。復号ポリシーを参照してください。

手順

ステップ 1 [ネットワーク（Network）] > [Web トラフィック タップ（Web Traffic Tap）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [Web トラフィック タップの編集（Edit Web Traffic Tap）] ページで、[有効（Enable）] チェックボックスをオンにし、Web トラフィック タップ機能を有効にします。

（注）
Web トラフィック タップ機能を無効にするには、[有効化（Enable）] チェックボックスをオフにします。Web トラフィック タップ機能を無効にすると、Web トラフィック タップ ポリシーの表示や編集ができません。ポリシーの表示や編集を行うには、機能を再び有効にする必要があります。

ステップ 4 [タップインターフェイス（Tap Interface）] ドロップダウンリストから、タップされたトラフィックデータを送信する Secure Web Applianceインターフェイスを選択します。インターフェイスのオプションは、P1、P2、T1、T2 です。インターフェイスについての詳細は、アプライアンスの接続を参照してください。

（注）
選択されたタップインターフェイスは、分析、調査、およびアーカイブのため、外部のセキュリティデバイスに直接接続する必要があります。または、専用の VLAN 上の L2 スイッチに接続します。選択されたタップ インターフェイスは接続され、ステータスがアクティブである必要があります。そうでない場合は、タップされたトラフィックのミラーリングは失敗します。

ステップ 5 [送信（Submit）] をクリックし、変更をコミットします。

Web トラフィック タップ ポリシーの設定

手順

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [Web トラフィック タップ ポリシー（Web Traffic Tap Policies）] を選択します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ポリシーの作成の手順に従い、新しい Web トラフィック タップ ポリシーを追加します。

（注）
タッピング設定なしのグローバル トラフィック タップ ポリシーは、[Web トラフィック タップ ポリシー（Web Traffic Tap Policies）] ページで、デフォルトで使用できます（[Web セキュリティ マネージャ（Web Security Manager）] > [Web トラフィック タップ ポリシー（Web Traffic Tap Policies）]）。

ステップ 3 [ポリシー メンバの定義（Policy Member Definition）] 領域の [詳細設定（Advanced）] セクションを展開して、以下の Web トラフィック タップ用の追加のグループ メンバーシップを追加します。

- プロトコル：HTTP または HTTPS プロトコルのいずれか、またはその両方を選択して、Web トラフィック タップ ポリシーを作成します。

  （注）
  HTTPS トラフィックをタップするには、一致する複合ポリシーを定義する必要があります（[Web セキュリティ マネージャ（Web Security Manager）] > [複合化ポリシー（Decryption Policies）]）。

  Web トラフィック タップ ポリシーは、ネイティブの FTP と SOCKS プロトコルをサポートしていません。

- サブネット（Subnets）
- URL カテゴリ：必要に応じて、URL フィルタリング カテゴリ用に [タップする（Tap）] または [タップしない（No Tap）] を設定します。未分類の URL でトラフィック タップを設定するには、未分類の URL のドロップダウン リストから [タップする（Tap）] を選択して、[送信（Submit（送信）] をクリックします。
- ユーザー エージェント（User Agents）

追加のグループ メンバーシップの条件の定義について詳細を確認するには、ポリシーの作成を参照してください。

（注）
タップするトラフィックは、Web トラフィック タップ ポリシーで定義されたすべてのフィルタ条件を満たしている必要があります。

[Web セキュリティ マネージャ（Web Security Manager）] > [Web トラフィック タップ ポリシー（Web Traffic Tap Policies）] を使用して、URL フィルタリングの表から URL カテゴリを追加することもできます。

（注）

すでに [詳細設定（Advanced）] セクションに URL のカテゴリが追加されている場合、URL フィルタリングの表ではそれらのカテゴリのみが表示されます（[Web セキュリティ マネージャ（Web Security Manager）] > [Web トラフィック タップ ポリシー（Web Traffic Tap Policies）]）。

Web トラフィック タップ ポリシーの順序について詳しくは、ポリシーの順序を参照してください。

HTTP 2.0 プロトコルの設定

Cisco AsyncOS 14.0 バージョンは、TLS を介した Web リクエストおよび応答向けに HTTP 2.0 をサポートします。

TLS を介した Web リクエストおよび応答用の HTTP 2.0。HTTP 2.0 サポートには、TLS 1.2 以降のバージョンでのみ使用可能な TLS ALPN ベースのネゴシエーションが必要です。

このリリースでは、HTTPS 2.0 は次の機能ではサポートされていません。

- Web トラフィック タップ（Web Traffic Tap）
- 外部 DLP（External DLP）
- 全体の帯域幅とアプリケーションの帯域幅

（注） デフォルトでは HTTP 2.0 機能が無効になっているため、CLI コマンド HTTP 2 を使用して機能を有効にします。

HTTP 2.0 機能では、次をサポートします。

- 最大 4,096 の同時セッションと 128 の同時ストリーム
- ALPN にあるすべての HTTP プロトコルとアドバタイズされた ALPN にある最大 7 つのプロトコル。
- 最大サイズが 16k のヘッダー。

（注） 2.0 の明示的なプロキシに対応する CONNECT も HTTP 1.1 で開始します

HTTP 2.0 設定を有効または無効にするために、新しい CLI コマンド `HTTP2` が導入されました。「Secure Web Appliance CLI コマンド」を参照してください。

アプライアンスの Web ユーザインターフェイスを使用して HTTP 2.0 を有効または無効にしたり、ドメインを制限したりすることはできません。HTTP 2.0 設定は、Cisco Secure Email and Web Manager（シスコのコンテンツセキュリティ管理アプライアンス）ではサポートされていません。

- URL が HTTP 2 例外リストとパススルー URL カテゴリの両方で失敗した場合、HTTP 2 がパススルーよりも優先されます。
- ALPN ログは、パススルー URL カテゴリに対して一貫性がありません。

Cisco クラウド Web セキュリティ プロキシへのアプライアンスの接続

この章で説明する内容は、次のとおりです。

クラウド コネクタ モードで機能を設定および使用する方法

クラウドコネクタのサブセットに含まれる機能の使用方法は、注記した点を除き、標準モードと同じです。詳細については、操作モードの比較を参照してください。

このトピックは本書のさまざまな個所と関連し、標準モードとクラウド Web セキュリティコネクタモードの両方に共通する Secure Web Appliance の主要機能の一部は、それらの個所に記載されています。クラウドへのディレクトリ グループの送信に関する情報およびクラウド コネクタの設定情報を除き、関連情報は本書の他の個所に記載されています。

このトピックには、標準モードでは適用できないクラウド Web セキュリティコネクタの設定に関する情報が含まれています。

本書には、Cisco クラウド Web セキュリティ製品に関する情報は記載されていません。Cisco クラウド Web セキュリティのドキュメントは、http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html [英語] から入手できます。

クラウド コネクタ モードでの展開

アプライアンスの初期設定時に、クラウド コネクタ モードと標準モードのどちらで展開するかを選択します。必要なライセンスを所有している場合は、現在展開されているアプライアンスでシステム セットアップ ウィザードを標準モードで実行し、これをクラウド コネクタ モードで再展開することもできます。システム セットアップ ウィザードを実行すると、既存の設定は上書きされ、既存のすべてのデータが削除されます。

アプライアンスの展開は標準モードとクラウド セキュリティ モードのどちらにおいても同様ですが、オンサイト Web プロキシ サービスおよびレイヤ 4 トラフィック モニター サービスは、クラウド Web セキュリティ コネクタ モードでは使用できません。

クラウド Web セキュリティ コネクタは、明示的な転送モードまたは透過モードで展開できます。

初期設定後にクラウド コネクタの設定を変更するには、[ネットワーク（Network）] > [クラウド コネクタ（Cloud Connector）] を選択します。

関連項目

- 接続、インストール、設定

クラウド コネクタの設定

Before you begin

「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有効化」を参照してください。

Procedure

ステップ 1 Secure Web Applianceの Web インターフェイスにアクセスします。

インターネット ブラウザに Secure Web Applianceの IPv4 アドレスを入力します。

初めてシステム セットアップ ウィザードを実行するときは、以下のデフォルトの IPv4 アドレスを使用します。

```
https://192.168.42.42:8443
```

または

```
http://192.168.42.42:8080
```

ここで、`192.168.42.42` はデフォルトの IPv4 アドレス、`8080` は、HTTP のデフォルトの管理ポート設定、`8443` は HTTPS のデフォルトの管理ポートです。

ステップ 2 [システム管理（System Administration）] > [システム セットアップ ウィザード（System Setup Wizard）] を選択します。

ステップ 3 ライセンス契約の条項に同意します。

ステップ 4 [セットアップの開始（Begin Setup）] をクリックします。

ステップ 5 システム設定項目を設定します。

設定	説明
デフォルト システム ホスト名（Default System Hostname）	Secure Web Applianceの完全修飾ホスト名。
DNS サーバー（DNS Server(s)）	ドメイン名サービス ルックアップ用のインターネット ルート DNS サーバー。 DNS の設定も参照してください。
NTP サーバー（NTP Server）	システム クロックと同期させるサーバー。デフォルトは time.ironport.com です。
タイム ゾーン	アプライアンス上にタイム ゾーンを設定して、メッセージ ヘッダーおよびログ ファイルのタイムスタンプが正確に表示されるようにします。

ステップ 6 アプライアンス モードの [クラウド Web セキュリティ コネクタ（Cloud Web Security Connector）] を選択します。

ステップ 7 クラウド コネクタの設定項目を設定します。

設定	説明
クラウド Web セキュリティ プロキシ サーバー（Cloud Web Security Proxy Servers）	クラウド プロキシ サーバー（CPS）のアドレス（例：proxy1743.scansafe.net）。
失敗のハンドリング（Failure Handling）	AsyncOS がクラウド Web セキュリティ プロキシへの接続に失敗した場合、インターネットに [直接接続（Connect directly）] するか、[要求をドロップ（Drop requests）] します。
Cloud Web Security 認証スキーム（Cloud Web Security Authorization Scheme）	トランザクションを認証する方式： • Secure Web Applianceの一般向け IPv4 アドレス • 各トランザクションに含まれている認証キー。Cisco Cloud Web Security Portal 内で認証キーを生成できます。

ステップ 8 ネットワーク インターフェイスおよび配線を設定します。

設定	説明
イーサネット ポート（Ethernet Port）	M1 インターフェイスを管理トラフィック専用として設定する場合は、データ トラフィック用の P1 インターフェイスを設定する必要があります。ただし、管理トラフィックとデータ トラフィックの両方をM1インターフェイスとして使用する場合でも、P1 インターフェイスを設定できます。
IPアドレス（IP Address）	Secure Web Applianceを管理するために使用する IPv4 アドレス。
ネットワーク マスク（Network Mask）	このネットワーク インターフェイス上の Secure Web Applianceを管理する際に使用するネットワークマスク。
ホスト名（Hostname）	このネットワーク インターフェイス上の Secure Web Applianceを管理する際に使用するホスト名。

ステップ 9 管理およびデータ トラフィックのルートを設定します。

設定	説明
デフォルト ゲートウェイ（Default Gateway）	管理インターフェイスやデータ インターフェイスを通過するトラフィックに使用するデフォルトのゲートウェイの IPv4 アドレス。
名前（Name）	スタティック ルートの識別に使用する名前。
内部ネットワーク（Internal Network）	このルートのネットワーク上の宛先の IPv4 アドレス。
内部ゲートウェイ（Internal Gateway）	このルートのゲートウェイの IPv4 アドレス。ルート ゲートウェイは、それが設定されている管理インターフェイスまたはデータ インターフェイスと同じサブネット上に存在する必要があります。

ステップ 10 透過的接続の設定項目を設定します。

Note
デフォルトでは、クラウド コネクタはトランスペアレント モードで展開され、レイヤ4 スイッチまたは WCCP バージョン 2 ルータと接続する必要があります。

設定	説明
レイヤ 4 スイッチ（Layer-4 Switch） または デバイスなし（No Device）	• Secure Web Applianceはレイヤ 4 スイッチに接続されます。 または • 明示的な転送モードでクラウド コネクタを展開します。

設定	説明
WCCP v2 ルータ（WCCP v2 Router）	Secure Web Applianceは WCCP バージョン 2 対応ルータに接続されます。 注：パスフレーズは任意であり、7 文字以内の文字を含めることができます。

ステップ 11 管理設定項目を設定します。

設定	説明
管理者パスフレーズ（Administrator Passphrase）	Secure Web Applianceにアクセスするためのパスフレーズ。パスフレーズは 6 文字以上にする必要があります。
システム アラート メールの送信先（Email system alerts to）	アプライアンスによって送信されるアラートの宛先メール アドレス。
SMTP リレー ホスト経由で電子メールを送信（Send Email via SMTP Relay Host）	（任意）AsyncOS がシステムによって生成された電子メール メッセージの送信に使用する SMTP リレー ホストのホスト名またはアドレス。 デフォルトの SMTP リレー ホストは、MX レコードにリストされているメール サーバーです。 デフォルトのポート番号は 25 です。
オートサポート（AutoSupport）	アプライアンスは、シスコ カスタマー サポートにシステム アラートと毎週のステータス レポートを送信できます。

ステップ 12 レビューしてインストールします。

a) インストールを確認します。
b) 前に戻って変更する場合は、[前へ（Previous）] をクリックします。
c) 入力した情報を使って続行する場合は、[この設定をインストール（Install This Configuration）] をクリックします。

What to do next

関連項目

- セキュア データの漏洩防止, on page 101
- ネットワーク インターフェイス
- TCP/IP トラフィック ルートの設定
- トランスペアレント リダイレクションの設定
- アラートの管理, on page 53

- SMTP リレー ホストの設定

クラウドのディレクトリ グループの使用による Web アクセスの制御

Cisco クラウド Web セキュリティを使用して、ディレクトリ グループに基づいてアクセスを制御できます。Cisco クラウド Web セキュリティへのトラフィックがクラウドコネクタモードの Secure Web Applianceを介してルーティングされている場合、Cisco クラウド Web セキュリティは、グループベースのクラウドポリシーを適用できるように、クラウドコネクタからトランザクションと共にディレクトリグループ情報を受け取る必要があります。

Before you begin

Secure Web Applianceの設定に認証レルムを追加します。

Procedure

ステップ 1 [ネットワーク（Network）] > [クラウドコネクタ（Cloud Connector）] に移動します。

ステップ 2 [クラウドポリシーディレクトリ グループ（Cloud Policy Directory Groups）] 領域で、[グループの編集（Edit Groups）] をクリックします。

ステップ 3 Cisco クラウド Web セキュリティ内で作成したクラウド ポリシーの対象となる [ユーザー グループ（User Groups）] と [マシン グループ（Machine Groups）] を選択します。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [完了（Done）] をクリックして、変更を確定します。

What to do next

関連情報

- 認証レルム

クラウド プロキシ サーバーのバイパス

クラウド ルーティング ポリシーを使用すると、以下の特性に基づいて、Web トラフィックを Cisco クラウド Web セキュリティ プロキシにルーティングしたり、インターネットに直接ルーティングできたりします。

- 識別プロファイル
- プロキシ ポート（Proxy Port）
- Subnet
- URL カテゴリ
- ユーザー エージェント

クラウドコネクタ モードでクラウドルーティング ポリシーを作成するプロセスは、標準モードを使用してルーティング ポリシーを作成するプロセスと同じです。

関連項目

- ポリシーの作成

クラウド コネクタ モードでの FTP および HTTPS の部分的サポート

クラウドコネクタモードの Secure Web Applianceでは、FTP および HTTPS が完全にはサポートされていません。

FTP

FTP はクラウド コネクタではサポートされません。アプライアンスがクラウド コネクタ用に設定されている場合、AsyncOS はネイティブ FTP トラフィックをドロップします。

FTP over HTTP はクラウド コネクタ モードでサポートされます。

HTTPS

クラウド コネクタは復号をサポートしていません。復号せずに HTTPS トラフィックを渡します。

クラウド コネクタは復号をサポートしていないため、通常、AsyncOS は HTTPS トラフィックのクライアント ヘッダー情報にアクセスできません。したがって、通常、AsyncOS は暗号化されたヘッダー情報に依存するルーティング ポリシーを適用できません。これは、透過的 HTTPS トランザクションでよくあることです。たとえば、透過的 HTTPS トランザクションの場合、AsyncOS は HTTPS クライアント ヘッダー内のポート番号にアクセスできないため、ポート番号に基づいてルーティングポリシーを照合できません。この場合、AsyncOS はデフォルトのルーティング ポリシーを使用します。

明示的な HTTPS トランザクションの場合は 2 つの例外があります。AsyncOS は、明示的 HTTPS トランザクションの以下の情報にアクセスできます。

- URL
- 宛先ポート番号

明示的 HTTPS トランザクションの場合は、URL またはポート番号に基づいてルーティング ポリシーを照合できます。

セキュア データの漏洩防止

[ネットワーク（Network）] > [外部 DLP サーバー（External DLP Servers）] で、クラウド コネクタを外部のデータ漏洩防止サーバーと統合できます。

関連項目

- 機密データの漏洩防止

グループ名、ユーザー名、IP アドレスの表示

設定したグループ名、ユーザー名、IP アドレスを表示するには、whoami.scansafe.net にアクセスします。

クラウド コネクタ ログへの登録

クラウド コネクタ ログには、認証されたユーザーやグループ、クラウド ヘッダー、認証キーなど、クラウド コネクタの問題のトラブルシューティングに役立つ情報が含まれています。

Procedure

ステップ 1 [システム管理（System Administration）] > [ログ サブスクリプション（Log Subsctiptions）] に移動します。
ステップ 2 [ログタイプ（Log Type）] メニューから [クラウドコネクタログ（Cloud Connector Logs）] を選択します
ステップ 3 [ログ名（Log Name）] フィールドに名前を入力します。
ステップ 4 ログ レベルを設定します。
ステップ 5 変更を [実行（Submit）] して [確定する（Commit）] します。

What to do next

関連項目

- ログによるシステム アクティビティのモニター

クラウド Web セキュリティ コネクタの使用による識別プロファイルと認証

クラウド Web セキュリティ コネクタは、基本認証および NTLM をサポートしています。また、特定の宛先に対して認証をバイパスできます。

クラウド コネクタ モードで Active Directory レルムを使用すると、トランザクション要求を特定のマシンから発信された要求として識別できます。マシン ID サービスは標準モードでは使用できません。

2 つの例外を除き、認証は Secure Web Appliance全体で同様に機能します。標準構成であるかクラウドコネクタ構成であるかは問いません。次に例外を示します。

- マシン ID サービスは標準モードでは使用できません。

- アプライアンスがクラウド コネクタ モードに設定されている場合、AsyncOS は Kerberos をサポートしません。

Note ユーザー エージェントまたは宛先 URL に基づく識別プロファイルは、HTTPS トラフィックに対応していません。

関連項目

- ポリシーの適用に対するマシンの識別, on page 103
- 未認証ユーザーのゲスト アクセス, on page 104
- ポリシーの適用に対するエンドユーザーの分類
- エンドユーザー クレデンシャルの取得の概要

ポリシーの適用に対するマシンの識別

マシン ID サービスを有効にすると、AsyncOS は、認証済みユーザーや IP アドレスなどの識別子ではなく、トランザクション要求を実行したマシンに基づいてポリシーを適用できるようになります。AsyncOS は NetBIOS を使用してマシン ID を取得します。

Note マシン ID サービスは Active Directory レルムを介してのみ使用できることに注意してください。Active Directory レルムが設定されていない場合、このサービスはディセーブルになります。

Procedure

ステップ 1 [ネットワーク（Network）] > [マシンIDサービス（Machine ID Service）] を選択します。

ステップ 2 [設定の有効化と編集（Enable and Edit Settings）] をクリックします。

ステップ 3 マシン ID の設定項目を設定します。

設定	説明
マシン ID の NetBIOS の有効化（Enable NetBIOS for Machine Identification）	マシン ID サービスをイネーブルにする場合に選択します。
レルム	トランザクション要求を開始しているマシンの識別に使用する Active Directory レルム。
失敗のハンドリング（Failure Handling）	AsyncOS がマシンを識別できない場合に、トランザクションをドロップするか、ポリシーの照合を続行するかを指定します。

ステップ 4 変更を [実行（Submit）] して [確定する（Commit）] します。

未認証ユーザーのゲスト アクセス

クラウドコネクタモードで、未認証ユーザーにゲストアクセスを提供するように Secure Web Applianceが設定されている場合、AsyncOS は __GUEST_GROUP__ グループにゲストユーザーを割り当て、その情報を Cisco クラウド Web セキュリティに送信します。未認証ユーザーにゲスト アクセスを提供するには、ID を使用します。これらのゲスト ユーザーを制御するには、Cisco クラウド Web セキュリティ ポリシーを使用します。

関連項目

- 認証失敗後のゲスト アクセスの許可

Web 要求の代行受信

この章で説明する内容は、次のとおりです。

Web 要求の代行受信の概要

Secure Web Applianceは、ネットワーク上のクライアントまたは他のデバイスから転送された要求を代行受信します。

アプライアンスは他のネットワーク デバイスと連携してトラフィックを代行受信します。そのようなデバイスとして、一般的なスイッチ、トランスペアレント リダイレクション デバイス、ネットワーク タップ、およびその他のプロキシサーバーまたは Secure Web Applianceなどがあげられます。

Web 要求の代行受信のためのタスク

手順	タスク	関連項目および手順へのリンク
ステップ 1	ベスト プラクティスを検討します。	• Web 要求の代行受信のベスト プラクティス, on page 106
ステップ 2	（任意）以下のネットワーク関連のフォローアップ タスクを実行します。 • アップストリーム プロキシを接続および設定する。 • ネットワーク インターフェイス ポリシーを設定する。 • 透過リダイレクション デバイスを設定する。 • TCP/IP ルートを設定する。 • VLAN の設定。	• アップストリーム プロキシ • ネットワーク インターフェイス • トランスペアレント リダイレクションの設定 • TCP/IP トラフィック ルートの設定 • VLAN の使用によるインターフェイス能力の向上
ステップ 3	（任意）次の Web プロキシのフォローアップ タスクを実行する。 • 転送モードまたは透過モードで動作するように Web プロキシを設定する。 • 代行受信するプロトコル タイプに追加のサービスが必要かどうかを決定。 • IP スプーフィングの設定。 • Web プロキシ キャッシュの管理。 • カスタム Web 要求ヘッダーの使用。 • 一部の要求に対してプロキシをバイパス。	• Web 要求を代行受信するための Web プロキシ オプション, on page 106 • Web プロキシの設定, on page 107 • Web 要求を代行受信するための Web プロキシ オプション, on page 106 • Web プロキシ キャッシュ, on page 111 • Web プロキシの IP スプーフィング, on page 114 • Web プロキシのバイパス, on page 117
ステップ 4	以下のクライアント タスクを実行します。 • クライアントが Web プロキシに要求をリダイレクトする方法を決定。 • クライアントとクライアント リソースの設定。	• Web 要求をリダイレクトするためのクライアント オプション, on page 124 • クライアント アプリケーションによる PAC ファイルの使用, on page 125
ステップ 5	（任意）FTP プロキシを有効化して設定します。	• FTP プロキシ サービス, on page 128

Web 要求の代行受信のベスト プラクティス

- 必要なプロキシ サービスのみをイネーブルにします。
- Secure Web Applianceで定義されているすべての WCCP サービスに対して、同じ転送方式とリターン方式（L2 または GRE）を使用します。これによって、プロキシ バイパス リストが確実に機能します。
- ユーザーが企業ネットワークの外部から PAC ファイルにアクセスできないことを確認します。これによって、モバイル ワーカーは、企業ネットワーク上にいるときは Web プロキシを使用し、それ以外の場合は Web サーバーに直接接続できます。
- 信頼できるダウンストリーム プロキシまたはロードバランサからの X-Forwarded-For ヘッダーのみが Web プロキシで許可されるようにします。
- 当初は明示的な転送だけを使用していた場合でも、Webプロキシをデフォルトの透過モードのままにしておきます。透過モードでは、明示的な転送要求も許可されます。

Web 要求を代行受信するための Web プロキシ オプション

単独では、Web プロキシは HTTP（FTP over HTTP を含む）および HTTPS を使用する Web 要求を代行受信できます。プロトコル管理を向上させるために、さらに次のプロキシモジュールを利用できます。

- **FTP プロキシ。**FTP プロキシを使用すると、（HTTP でエンコードされた FTP トラフィックだけでなく）ネイティブ FTP トラフィックを代行受信できます。
- **HTTPS プロキシ。**HTTPS プロキシは HTTPS トラフィックの復号をサポートしているので、Webプロキシは、暗号化されていないHTTPS要求をコンテンツ分析のためにポリシーに渡すことができます。

Note 透過モードでは、HTTPS プロキシがイネーブルでない場合、Web プロキシは透過的にリダイレクトされたすべてのHTTPS要求をドロップします。透過的にリダイレクトされたHTTPS要求がドロップされた場合、その要求のログ エントリは作成されません。

- **SOCKS プロキシ。**SOCKS プロキシを使用すると、SOCKS トラフィックを代行受信できます。

これらの追加のプロキシのそれぞれが機能するには、Web プロキシが必要です。Web プロキシをディセーブルにすると、これらをイネーブルにできません。

Note Webプロキシはデフォルトでイネーブルになります。デフォルトでは、他のプロキシはすべてディセーブルになります。

関連項目

• FTP プロキシ サービス, on page 128
• SOCKS プロキシ サービス, on page 131

Web プロキシの設定

Before you begin

Web プロキシをイネーブルにします。

Procedure

ステップ 1 [セキュリティサービス（Security Services）] > [Webプロキシ（Web Proxy）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 必要に応じて基本的な Web プロキシ設定項目を設定します。

プロパティ	説明
プロキシを設定するHTTPポート（HTTP Ports to Proxy）	Web プロキシが HTTP 接続をリッスンするポート
キャッシング（Caching）	Web プロキシによるキャッシングをイネーブルにするかディセーブルにするかを指定します。 Web プロキシは、パフォーマンスを向上させるためにデータをキャッシュします。
プロキシ モード（Proxy Mode）	• [透過（Transparent）]（推奨）：Web プロキシがインターネット ターゲットを指定できるようにします。このモードでは、Web プロキシは、透過的または明示的に転送された Web 要求を代行受信できます。 • [転送（Forward）]：クライアント ブラウザがインターネット ターゲットを指定できるようにします。Webプロキシを使用するように各Webブラウザを個々に設定する必要があります。このモードでは、Web プロキシは明示的に転送された Web 要求のみを代行受信できます。

プロパティ	説明
IP スプーフィング接続タイプ	[プロキシモード（Proxy Mode）] に [透過的（Transparent）] を選択した場合は、IP スプーフィング接続タイプのいずれかを選択します。 • [透過的な接続に対してのみ（For Transparent Connections Only）]：透過接続の場合にのみ、IP スプーフィングを設定します。 • [すべての接続に対して（For All connections）]：透過的な接続と明示的な接続に IP スプーフィングを設定します。 [プロキシモード（Proxy Mode）] に [転送（Forward）] を選択した場合は、[IP スプーフィング接続タイプ（IP Spoofing Connection Type）] は常に [明示的（Explicit）] になります。 **Note** 選択した IP スプーフィング接続タイプは、ネイティブ FTP、HTTP、および HTTPS のすべてのプロトコルに適用されます。 ルーティングポリシーに IP スプーフィングプロファイルを追加するには、次を参照してください。 ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加

ステップ 4 必要に応じて Web プロキシの詳細設定を完了します。

プロパティ	説明
永続的接続のタイムアウト（Persistent Connection Timeout）	トランザクションが完了し、その他のアクティビティが検出されなかった後に、Web プロキシがクライアントまたはサーバーとの接続を開いたままにしておく最大時間（秒単位）。 • **[クライアント側（Client side）]**。クライアントとの接続のタイムアウト値。 • **[サーバー側（Server side）]**。サーバーとの接続のタイムアウト値。 これらの値を大きくすると、接続が開いたままになっている時間が延長され、接続の開閉に費やされるオーバーヘッドが低減します。ただし、永続的な同時接続の数が最大数に達した場合に Web Proxy が新しい接続を開く機能も低下します。 接続を確立して SSL ハンドシェイクを実行した後、クライアント要求がプロキシに送信されない場合、プロキシは永続的な接続タイムアウトを待ってから、クライアントとの接続を停止します。 シスコは、デフォルト値を維持することを推奨します。
使用中接続タイムアウト（In-Use Connection Timeout）	現在のトランザクションが完了していないときに、Web プロキシがアイドル状態のクライアントまたはサーバーからのデータをさらに待機する最大時間（秒単位）。 • **[クライアント側（Client side）]**。クライアントとの接続のタイムアウト値。 • **[サーバー側（Server side）]**。サーバーとの接続のタイムアウト値。

プロパティ	説明
同時永続的接続（サーバー最大数）（Simultaneous Persistent Connections (Server Maximum Number)）	Webプロキシサーバーがサーバーに対して開いたままにする接続（ソケット）の最大数。
クライアントあたりの最大接続数	クライアントによって開始される同時接続数を、設定した値に制限します。接続数が設定した制限値を超えると、接続がドロップされ、管理者にアラートが送信されます。 **Note** デフォルトでは、[クライアントあたりの最大接続数（Maximum Connections Per Client）] は無効になっています。 制限値を設定するには、[クライアントあたりの最大接続数（Maximum Connections Per Client）] チェックボックスをオンにして、次の手順を実行します。 • [接続（Connections）]：許可される同時接続数を入力します。 • [除外対象のダウンストリームプロキシまたはロードバランサ（Exempted Downstream Proxy or Load Balancer）]：ダウンストリームプロキシ、ロードバランサ、またはその他のクライアントIPアドレスのIPアドレスを入力します（サブネットまたはホスト名を設定することはできません）。Webプロキシには、この除外リストに含まれる IP アドレスの同時接続の制限が適用されません。

プロパティ	説明
ヘッダーの生成（Generate Headers）	要求に関する情報をエンコードするヘッダーを生成して追加します。 • **X-Forwarded-For** ヘッダーは、HTTP 要求を発信したクライアントの IP アドレスをエンコードします。 **Note** • ヘッダーの転送をオン/オフするには、`advancedproxyconfig` CLI コマンドの Miscellaneous オプション「HTTP X-Forwarded-Forヘッダーを通過させますか?（Do you want to pass HTTP X-Forwarded-For headers?）」を使用します。 • 明示的な転送アップストリーム プロキシを使用して、プロキシ認証によりユーザー認証やアクセス制御を管理するには、これらのヘッダーを転送する必要があります。 • 透過的 HTTPS 要求の場合、アプライアンスは XFF ヘッダーを復号できません。明示的要求の場合、アプライアンスは接続要求で受信される XFF ヘッダーを使用し、SSL トンネル内の XFF を復号しないため、X-Forwarded-For によるクライアント IP アドレスの識別が HTTPS 透過的要求に適用されることはありません。 • **Request Side VIA** ヘッダーは、クライアントからサーバーへの要求が通過するプロキシをエンコードします。 • **Response Side VIA** ヘッダーは、サーバーからクライアントへの要求が通過するプロキシをエンコードします。
Received ヘッダーの使用（Use Received Headers）	アップストリーム プロキシとして展開された Web プロキシが、ダウンストリーム プロキシから送信された X-Forwarded-For ヘッダーを使用してクライアントを識別できるようにします。Web プロキシは、リストに含まれていない送信元からの X-Forwarded-For ヘッダーの IP アドレスを受け入れません。 これをイネーブルにする場合は、ダウンストリーム プロキシまたはロード バランサの IP アドレスが必要です（サブネットやホスト名は入力できません）。
範囲要求の転送（Range Request Forwarding）	範囲要求の転送をイネーブルまたはディセーブルにするには、[範囲要求の転送の有効化（Enable Range Request Forwarding）] チェックボックスを使用します。詳細については、Web アプリケーションへのアクセスの管理を参照してください。

ステップ 5 変更を送信し、保存します。

What to do next

- Web プロキシ キャッシュ, on page 111
- トランスペアレント リダイレクションの設定

Web プロキシ キャッシュ

Webプロキシは、パフォーマンスを向上させるためにデータをキャッシュします。AsyncOSには「セーフ」から「アグレッシブ」の範囲の定義済みキャッシュ モードがあり、またカスタマイズしたキャッシングも使用できます。キャッシュ対象から特定のURLを除外することもできます。これを行うには、そのURLをキャッシュから削除するか、無視するようにキャッシュを設定します。

Web プロキシ キャッシュのクリア

Procedure

ステップ 1 [セキュリティサービス（Security Services）] > [Webプロキシ（Web Proxy）] を選択します。

ステップ 2 [キャッシュを消去（Clear Cache）] をクリックしてアクションを確定します。

Web プロキシ キャッシュからの URL の削除

Procedure

ステップ 1 CLI にアクセスします。

ステップ 2 `webcache> evict` コマンドを使用して、必要なキャッシング エリアにアクセスします。

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> evict
Enter the URL to be removed from the cache.
[]>
```

ステップ 3 Enter the URL to be removed from the cache.

Note
URL にプロトコルが含まれていない場合は、URL に `http://` が追加されます（たとえば、`www.cisco.com` は `http://www.cisco.com` となります）。

Web プロキシによってキャッシュしないドメインまたは URL の指定

Procedure

ステップ 1 CLI にアクセスします。

ステップ 2 webcache -> ignore コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> webcache
Choose the operation you want to perform:
- EVICT - Remove URL from the cache
- DESCRIBE - Describe URL cache status
- IGNORE - Configure domains and URLs never to be cached
[]> ignore
Choose the operation you want to perform:
- DOMAINS - Manage domains
- URLS - Manage urls
[]>
```

ステップ 3 管理するアドレス タイプを入力します（DOMAINS または URLS）。

```
[]> urls
Manage url entries:
Choose the operation you want to perform:
- DELETE - Delete entries
- ADD - Add new entries
- LIST - List entries
[]>
```

ステップ 4 **add** と入力して新しいエントリを追加します。

```
[]> add
Enter new url values; one on each line; an empty line to finish
[]>
```

ステップ 5 以下の例のように、1 行に 1 つずつ、ドメインまたは URL を入力します。

```
Enter new url values; one on each line; an empty line to finish
[]> www.example1.com
Enter new url values; one on each line; an empty line to finish
[]>
```

ドメインまたは URL を指定する際に、特定の正規表現（regex）文字を含めることができます。DOMAINS オプションでは、前にピリオドを付けることで、キャッシュ対象からドメインとそのサブドメイン全体を除外できます。たとえば、google.com ではなく、.google.com と入力すると、www.google.com、docs.google.com などを除外することができます。

URLS オプションでは、正規表現文字の全一式を使用できます。正規表現の使用方法については、正規表現を参照してください。

ステップ 6 値の入力を終了するには、メイン コマンドライン インターフェイスに戻るまで Enter キーを押します。

ステップ 7 変更を保存します。

Web プロキシのキャッシュ モードの選択

Procedure

ステップ 1 CLI にアクセスします。

ステップ 2 `advancedproxyconfig -> caching` コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> caching
Enter values for the caching options:
The following predefined choices exist for configuring advanced caching
options:
1. Safe Mode
2. Optimized Mode
3. Aggressive Mode
4. Customized Mode
Please select from one of the above choices:
[2]>
```

ステップ 3 必要な Web プロキシ キャッシュ設定に対応する番号を入力します。

入力	モード	説明
1	セーフ	他のモードと比較して、キャッシングが最も少なく、RFC #2616 には最大限準拠します。
2	最適化	キャッシングと RFC #2616 への準拠が適度です。セーフ モードと比較した場合、Last-Modified ヘッダーが存在するときにキャッシング時間が指定されていない場合に、最適化モードでは Web プロキシがオブジェクトをキャッシュします。Web プロキシは、ネガティブ応答をキャッシュします。
3	アグレッシブ	キャッシングが最も多く、RFC #2616 への準拠は最小限です。最適化モードと比較した場合、アグレッシブ モードでは、認証済みコンテンツ、ETag の不一致、および Last-Modified ヘッダーのないコンテンツがキャッシュされます。Web プロキシは非キャッシュ パラメータを無視します。
4	カスタマイズド モード	各パラメータを個々に設定します。

ステップ 4 オプション 4（カスタマイズ モード）を選択した場合は、各カスタム設定の値を入力します（または、デフォルト値のままにします）。

ステップ 5 メイン コマンド インターフェイスに戻るまで、Enter キーを押します。

ステップ 6 変更を保存します。

What to do next

関連項目

- Web プロキシ キャッシュ, on page 111。

Web プロキシの IP スプーフィング

デフォルトでは、Webプロキシは要求を転送する際に、自身のアドレスに合わせて要求の送信元 IP アドレスを変更します。これによってセキュリティは強化されますが、IP スプーフィングを実装してこの動作を変更し、 Secure Web Applianceからではなく、要求がクライアント IP やその他のルーティング可能なカスタム IP アドレスから発信されたように見せることができます。Web プロキシ IP スプーフィングを設定するには、カスタム IP アドレスの IP スプーフィングプロファイルを作成し、それらをルーティングポリシーに追加します。

IP スプーフィングは、透過的または明示的に転送されたトラフィックに対して機能します。Webプロキシが透過モードで展開されている場合は、透過的にリダイレクトされた接続のみ、またはすべての接続（透過的にリダイレクトされた接続と明示的に転送された接続）に対して（IP スプーフィング接続タイプを設定できる）ことができます。明示的に転送された接続で IP スプーフィングを使用する場合は、リターンパケットを Secure Web Applianceにルーティングする適切なネットワークデバイスがあることを確認してください。

IP スプーフィングがイネーブルで、アプライアンスが WCCP ルータに接続されている場合は、2 つの WCCP サービス（送信元ポートに基づくサービスと宛先ポートに基づくサービス）を設定する必要があります。

IP スプーフィングプロファイルには、HTTPS トラフィックが透過的にリダイレクトされる場合の制限があります。URL カテゴリ基準を使用しているルーティング ポリシーによる HTTPS サイトへのアクセス を参照してください。

関連項目

- IP スプーフィングプロファイルの作成, on page 114
- Web プロキシの設定, on page 107
- WCCP サービスの設定

IP スプーフィングプロファイルの作成

Before you begin

Web プロキシ設定でプロキシモードと IP スプーフィング接続タイプが選択されていることを確認します。詳細については、Web プロキシの設定, on page 107を参照してください。

Procedure

ステップ 1 [Web Security Manager] > [IP スプーフィングプロファイル（IP Spoofing Profiles）] を選択します。

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 IP スプーフィングプロファイルの名前を入力します。
ステップ 4 スプーフィングプロファイル名に割り当てる IP アドレスを入力します。
ステップ 5 変更を送信し、保存します。

What to do next

IP スプーフィングプロファイルをルーティングポリシーに追加します。詳細については、「ルーティングポリシーへのルーティング先と IP スプーフィングプロファイルの追加」を参照してください。

Related Topics

IP スプーフィングプロファイルの編集 （115 ページ）
IP スプーフィングプロファイルの削除 （115 ページ）

IP スプーフィングプロファイルの編集

Note IP スプーフィングプロファイルを更新すると、そのプロファイルに関連付けられているすべてのルーティングポリシーでそのプロファイルが更新されます。

Procedure

ステップ 1 [Web Security Manager] > [IP スプーフィングプロファイル（IP Spoofing Profiles）] を選択します。
ステップ 2 編集する IP スプーフィングプロファイル名のリンクをクリックします。
ステップ 3 プロファイルの詳細を変更します。
ステップ 4 変更を送信し、保存します。

IP スプーフィングプロファイルの削除

Procedure

ステップ 1 [Web Security Manager] > [IP スプーフィングプロファイル（IP Spoofing Profiles）] を選択します。
ステップ 2 削除する IP スプーフィングプロファイルに対応するゴミ箱アイコンをクリックします。

Note
削除しようとしている IP スプーフィングプロファイルが 1 つ以上のルーティングポリシーに割り当てられている場合は、アプライアンスによって警告が表示されます。この場合は、影響を受けるすべてのルーティングポリシーに割り当てる別の IP スプーフィングプロファイルを選択します。

ステップ 3 変更を送信し、保存します。

Web プロキシのカスタム ヘッダー

特定の発信トランザクションにカスタムヘッダーを追加することにより、宛先サーバーによる特別な処理を要求できます。たとえば、YouTube for Schools と関係がある場合、カスタム ヘッダーを使用して、YouTube.com へのトランザクション要求を自身のネットワークから発信された、特別な処理を必要とする要求として識別させることができます。

Web 要求へのカスタム ヘッダーの追加

Procedure

ステップ 1 CLI にアクセスします。

ステップ 2 `advancedproxyconfig -> customheaders` コマンドを使用して、必要なサブメニューにアクセスします。

```
example.com> advancedproxyconfig
Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
[]> customheaders
Currently defined custom headers:
Choose the operation you want to perform:
- DELETE - Delete entries
- NEW - Add new entries
- EDIT - Edit entries
[]>
```

ステップ 3 次のように、必要なサブコマンドを入力します。

オプション	説明
[削除（Delete）]	指定するカスタム ヘッダーを削除します。コマンドで返されたリストのヘッダーに関連付けられている番号を使用して削除するヘッダーを指定します。

オプション	説明

[新規（New）]	指定するドメインの使用に提供するヘッダーを作成します。
	ヘッダーの例：
	X-YouTube-Edu-Filter: ABCD1234567890abcdef
	（この場合の値は、YouTube で提供される固有キーです）。
	ドメインの例：
	youtube.com
	カスタムヘッダーの最大長は 16k で、CR または LF を除く任意の値を含めることができます。
	カスタムヘッダーの例：
	`Choose the operation you want to perform:`
	`- DELETE -  Delete entries`
	`- NEW -  Add new entries`
	`- EDIT -  Edit entries`
	`[]> new`
	`Please enter the custom HTTP header (in the form field: value):`
	`[]>`
	`[:characters colon(:) and double quotes(") are not allowed]`

[編集（Edit）]	既存のヘッダーを指定したヘッダーと置き換えます。コマンドで返されたリストのヘッダーに関連付けられている番号を使用して削除するヘッダーを指定します。

ステップ 4 メイン コマンド インターフェイスに戻るまで、Enter キーを押します。

ステップ 5 変更を保存します。

Web プロキシのバイパス

Web プロキシのバイパス（Web 要求の場合）

特定のクライアントからの透過的要求や特定の宛先への透過的要求が Web プロキシをバイパスするように、 Secure Web Applianceを設定できます。

Web プロキシをバイパスすることによって、以下のことが可能になります。

- HTTP ポートを使用しているが、適切に機能しない HTTP 非対応の（または独自の）プロトコルが、プロキシ サーバーに接続するときに干渉されないようにします。
- ネットワーク内の特定のマシンからのトラフィックが、マルウェアのテストマシンなど、ネットワーク プロキシおよび組み込みのセキュリティ保護をすべてバイパスすることを確認します。

バイパスは、Webプロキシに透過的にリダイレクトされる要求に対してのみ機能します。Webプロキシは、トランスペアレントモードでも転送モードでも、クライアントから明示的に転送されたすべての要求を処理します。

Web プロキシのバイパス設定（Web 要求の場合）

Procedure

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）]>[バイパス設定（Bypass Settings）] を選択します。

ステップ 2 [バイパス設定の編集（Edit Bypass Settings）] をクリックします。

ステップ 3 Web プロキシをバイパスするアドレスを入力します。

Note
/0 をバイパスリスト内の任意の IP のサブネットマスクとして設定すると、アプライアンスはすべての Web トラフィックをバイパスします。この場合、アプライアンスは設定を 0.0.0.0/0 として解釈します。

ステップ 4 プロキシバイパスリストに追加するカスタム URL カテゴリを選択します。

Note
[正規表現（Regular Expressions）] に Web プロキシバイパスを設定することはできません。

Note
カスタム URL カテゴリをプロキシバイパスリストに追加すると、カスタム URL カテゴリのすべての IP アドレスとドメイン名が、送信元と宛先の両方でバイパスされます。

ステップ 5 変更を送信し、保存します。

Note
IP スプーフィングが有効になっている場合、バイパスリストに含まれているドメインは明示的な要求をサポートしません。

Web プロキシのバイパス設定（アプリケーションの場合）

Procedure

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）]>[バイパス設定（Bypass Settings）] を選択します。

ステップ 2 [アプリケーションのスキップ設定を編集（Edit Application Bypass Settings）] をクリックします。

ステップ 3 スキャンをバイパスするアプリケーションを選択します。

ステップ 4 変更を送信し、保存します。

Note
- Microsoft Update ByPass 機能は、Application Discovery and Control（ADC）でのみ動作します。 アプリケーション制御機能に対して ADC が有効になっていることを確認する必要があります。

- Webex バイパス設定は、HTTPS トラフィックにのみ適用されます。ただし、HTTP トラフィックの場合、アプリケーションはアクセス ポリシーを介して使用してブロックできます。

ポリシーごとの Web プロキシ カスタム ヘッダー

HTTP リクエストのカスタムヘッダープロファイルを設定し、ヘッダー書き換えプロファイルの下に複数のヘッダーを作成できます。各プロファイルには最大 12 のヘッダーを設定できます。既存のヘッダー プロファイルを変更または削除することもできます。既存のアクセス ポリシーにヘッダー書き換えプロファイルを追加して、特定のアクセスポリシーが適用されるすべてのトランザクションにヘッダーを含めることができます。

ヘッダー書き換えプロファイル機能を使用すると、認証が成功した後、アプライアンスがユーザとグループの情報を別のアップストリームデバイスに渡すことができます。アップストリーム プロキシはユーザを認証済みと見なし、追加の認証をバイパスし、定義されたアクセス ポリシーに基づいてユーザにアクセスを提供します。

- HTTP Web リクエストのヘッダー書き換えプロファイルの作成 （119 ページ）
- ユーザー名とグループ ヘッダー形式の変更 （121 ページ）（オプション）
- アクセス ポリシーへのヘッダー プロファイルの追加 （121 ページ）

AsynOS バージョン 14.0 以降では、CLI コマンド `advancedproxyconfig-> customheader` を使用した Web プロキシ カスタム ヘッダーの作成を避けることを推奨します。

HTTP Web リクエストのヘッダー書き換えプロファイルの作成

手順

ステップ 1 [Web Security Manager] > [HTTP 書き換えプロファイル（HTTP Rewrite Profiles）] を選択します

ステップ 2 [プロファイルを追加（Add Profile）] をクリックします。

ステップ 3 作成するヘッダー書き換えプロファイルに一意の名前を割り当てます。

ステップ 4 [ヘッダー（Headers）] エリアで、次の情報を入力します。

（注）
[ヘッダー書き換えプロファイル（Header Rewrite Profiles）] には空または Null のヘッダー値を入力できます。ヘッダーを保存して、Null または値なしで送信すると、ヘッダーは発信リクエストに含まれません。たとえば、アウトバウンドサーバーへのヘッダー `Via` を非表示にする場合は、値「""」でHTTP書き換えプロファイルにヘッダー名 `Via` を追加します。

- [ヘッダー名（Header Name）]：HTTP リクエストに追加するヘッダー名を入力します。例：X-Client-IP、X-Authenticated-User、X-Authenticated-Groups など
- [ヘッダー値（Header Value）]：ヘッダー名に対応するリクエスト ヘッダーに含める値を入力します。ヘッダー変数のプレフィックス：

- `$ ReqMeta`：クライアント IP、ユーザー、グループなどの標準 HTTP ヘッダー変数を取得します。たとえば、リクエスト ヘッダーにユーザー名を含める場合、形式は `($ReqMeta[X-Authenticated-User])` です。
- `$ReqHeader`：標準の HTTP ヘッダーの値、または同じヘッダー書き換えプロファイルに定義された他のヘッダーのヘッダーの値を使用します。

  たとえば、

  ```
  Header1:32
  Header2: 44-($ReqHeader[Header1])-46
  ```

  ヘッダー `2` の値は `44-32-46` になります

- [テキスト形式（Text Format）]：エンコーディングのテキスト形式を選択します。使用可能なオプションは ASCII と UTF-8 です。
- [バイナリ エンコーディング（Binary Encoding）]：リクエスト ヘッダーにバイナリ エンコーディング（Base64）を使用するかどうかを選択します。

（注）
サーバー タイプに基づいて、送信されたリクエスト ヘッダー フィールドのサイズがサーバーの上限を超えた場合、アプライアンスはエラー メッセージを表示します。たとえば、異なるサーバー タイプは異なるヘッダー長をサポートします。

- Apache 2.0、2.2：8k
- Nginx：4k ー 8k
- IIS（バージョンによって異なります）：8K ー 16K
- Tomcat ：（バージョンによって異なります）8K

ISE を使用したユーザー識別の場合、グローバル X-authentication ヘッダー設定（X-Authenticated-User および X-Authenticated-Groups）は、プレフィックスとしてドメインおよび認証メカニズムを適用しません。

ASCII としてテキスト形式を選択した場合でも、`($ ReqMeta [HTTP_header])` 値として UTF+8 を入力できます。現在、次のヘッダーは `($ReqMeta[HTTP_header])` をサポートしています。

- X-Authenticated-User
- X-Authenticated-Groups
- X-Client-IP

ヘッダーの値が Null の場合、ヘッダーは発信リクエストに含まれません。これは、以下を実行しない場合に発生します。

- プロキシ認証を有効にします。
- アクセス ポリシー、復号ポリシー、またはルーティング ポリシーのメンバーシップ基準でグループを定義します。

ステップ 5 変更を送信し、保存します。

ユーザー名とグループ ヘッダー形式の変更

手順

ステップ 1 [Web Security Manager] > [HTTP 書き換えプロファイル（HTTP Rewrite Profiles）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 形式を変更します。

許可される形式は次のとおりです。

- ユーザー名：`$authMechanism://$domainName/$userName`、`$authMechanism:\\$domainName\$userName`、`$domainName/$userName`、`$domainName\$userName`、`$userName`
- グループ：`$authMechanism://$domainName/$groupName`、`$authMechanism:\\$domainName\$groupName`、`$domainName/$groupName`、`$domainName\$groupName`、`$groupName`

  カンマ（,）、コロン（:）、セミコロン（;）、バックスラッシュ（\）、縦棒（|）などのデリミタも変更できます。

ステップ 4 変更を送信し、保存します。

アクセス ポリシーへのヘッダー プロファイルの追加

始める前に

アクセス ポリシーの設定ポリシーの作成 を参照してください。

手順

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] を選択します。

ステップ 2 [アクセス ポリシー（Access Policies）] ページで、[HTTP 書き換えプロファイル（HTTP Rewrite Profile）] のリンクをクリックします。

新しいアクセス ポリシーを作成し、それにヘッダー書き換えプロファイルを追加することもできます。新しいアクセス ポリシーを作成するには、次を参照してください。ポリシーの作成

ステップ 3 ポリシーに追加するヘッダー書き換えプロファイルを選択します。追加すると、特定のアクセス ポリシーが適用される HTTP トランザクションにヘッダーが含まれます。

ステップ 4 変更を送信し、保存します。

アクセス ポリシーにリンクされたヘッダー書き換えプロファイルは削除できます。削除する前に、別のプロファイルを選択すると、選択したプロファイルがアクセス ポリシーに自動的に適用されます。

Web プロキシ使用規約

Secure Web Appliance を設定して、Web アクティビティのフィルタリングとモニタリングが行われていることをユーザに通知できます。アプライアンスは、ユーザーが初めてブラウザにアクセスしたときに、一定時間の経過後、エンドユーザー確認ページを表示します。エンドユーザー確認ページが表示されたら、ユーザーはリンクをクリックして、要求した元のサイトまたは他の Web サイトにアクセスする必要があります。

関連項目

- エンドユーザーへのプロキシ アクションの通知

ドメイン マップ

特定のクライアントからの透過的 HTTPS 要求や特定の宛先への透過的 HTTPS 要求が HTTPS プロキシをバイパスするように、 Secure Web Applianceを設定できます。

トラフィックがアプライアンスを通過することを必要とするアプリケーションに関して、変更や宛先サーバーの証明書チェックを行わずに、パススルーを使用することができます。

特定アプリケーションのドメインマップ

始める前に

特定のサーバーへのパススルートラフィックを必要とするデバイスに関して定義された識別ポリシーがあることを確認してください。詳細については、ユーザーおよびクライアント ソフトウェアの分類を参照してください。具体的には、次のことを行う必要があります。

- [認証/識別から除外（Exempt from authentication/identification）] をオンします。
- この識別プロファイルを適用するアドレスを指定します。IP アドレス、CIDR ブロック、およびサブネットを入力できます。

手順

ステップ 1 HTTPS プロキシを有効にします。詳細については、HTTPS プロキシのイネーブル化を参照してください。

ステップ 2 [Webセキュリティマネージャ（Web Security Manager）]>[ドメインマップ（Domain Map）] を選択します。

a) [ドメインの追加（Add Domain）] をクリックします。
b) [ドメイン名（Domain Name）] に宛先サーバーのドメイン名を入力します。
c) 既存のドメインが指定されている場合は、優先順位を選択します。

d) IP アドレスを入力します。
e) [送信（Submit）] をクリックします。

ステップ 3 [Webセキュリティマネージャ（Web Security Manager）] > [カスタムおよび外部URLカテゴリ（Custom and External URL Categories）] を選択します。

a) [Add Category] をクリックします。
b) 次の情報を入力します。

設定	説明
カテゴリ名（Category Name）	この URL カテゴリの識別子を入力します。この名前は、ポリシー グループに URL フィルタリングを設定するときに表示されます。
リスト順（List Order）	カスタム URL カテゴリのリストで、このカテゴリの順序を指定します。リスト内の最初の URL カテゴリに「1」を入力します。 URL フィルタリング エンジンでは、指定した順序でカスタム URL カテゴリに対してクライアント要求が評価されます。
カテゴリ タイプ（Category Type）	[ローカルカスタムカテゴリ（Local Custom Category）] を選択します。
詳細設定（Advanced）	このセクションに、追加のアドレスセットを指定する正規表現を入力できます。 正規表現を使用して、入力したパターンと一致する複数のアドレスを指定できます。 正規表現の使用方法については、正規表現を参照してください。

c) 変更を送信し、保存します。

ステップ 4 [Webセキュリティマネージャ（Web Security Manager）] > [復号ポリシー（Decryption Policies）] を選択します。

a) 新しい復号ポリシーを作成します。
b) 特定のアプリケーションの HTTPS トラフィックをバイパスするために作成した識別プロファイルを選択します。
c) [詳細設定（Advanced）] パネルで、[URLカテゴリ（URL Categories）] のリンクをクリックします。
d) [追加（Add）] カラムをクリックして、手順 3 で作成したカスタム URL カテゴリを追加します。
e) [完了（Done）] をクリックします。
f) [復号ポリシー（Decryption Policies）] ページで、[URLフィルタリング（URL Filtering）] のリンクをクリックします。
g) [パススルー（Pass Through）] を選択します。
h) 変更を送信し、保存します。

%(フォーマット指定子を使用してアクセスログ情報を表示することができます。詳細については、アクセス ログのカスタマイズを参照してください。

（注）

- ドメインマップ機能は HTTPS 透過モードで動作します。
- この機能は、明示モードでは動作せず、HTTP トラフィックについても動作しません。
- この機能を使用してトラフィックを許可するには、ローカルカスタムカテゴリを設定する必要があります。
- この機能を有効にすると、SNI 情報が利用できる場合でも、ドメインマップで設定されたサーバー名に従ってサーバー名の変更または割り当てが行われます。
- この機能は、ドメイン名に基づくトラフィックがドメインマップと一致し、対応するカスタムカテゴリ、復号ポリシー、パススルーアクションが設定されている場合、そのトラフィックをブロックしません。
- 認証をこのパススルー機能と併用することはできません。認証には復号が必要ですが、この場合、トラフィックは復号されません。
- UDP トラフィックはモニターされません。 Secure Web Applianceに到達しないように UDP トラフィックを設定する必要があります。代わりに、WhatsApp、Telegram などのアプリケーションのためにファイアウォールを経由してインターネットに直接アクセスする必要があります。
- WhatsApp、Telegram、および Skype は透過モードで動作します。ただし、WhatsApp などの一部のアプリケーションは、アプリケーションの制限のために、明示モードでは動作しません。

Web 要求をリダイレクトするためのクライアント オプション

クライアントから Web プロキシに明示的に要求を転送することを選択した場合は、それを実行するためのクライアントの設定方法も指定する必要があります。以下の方法から選択します。

- **明示的な設定を使用してクライアントを設定する。**Web プロキシのホスト名とポート番号を使ってクライアントを設定します。設定方法の詳細については、個々のクライアントのマニュアルを参照してください。

Note デフォルトでは、Web プロキシ ポートはポート番号 80 と 3128 を使用します。クライアントはいずれかのポートを使用できます。

- **プロキシ自動設定（PAC）ファイルを使用してクライアントを設定する。**PAC ファイルは、Web要求の送信先をクライアントに指示します。このオプションを使用すると、プロキシの詳細に対する以降の変更を一元管理できます。

PAC ファイルを使用する場合は、PAC ファイルの保存場所とクライアントがそれらを検出する方法を選択する必要があります。

関連項目

• クライアント アプリケーションによる PAC ファイルの使用, on page 125

クライアント アプリケーションによる PAC ファイルの使用

プロキシ自動設定（PAC）ファイルのパブリッシュ オプション

クライアントがアクセスできる場所に PAC ファイルをパブリッシュする必要があります。有効な場所は以下のとおりです。

- **Web サーバー**
- **Secure Web Appliance**。クライアントに対しては Web ブラウザとして表示される Secure Web Applianceに PAC ファイルを配置できます。アプライアンスには、さまざまなホスト名、ポート、ファイル名を使用している要求に対応する機能など、PAC ファイルを管理するための追加オプションもあります。
- **ローカル マシン。**クライアントのハードディスクに PAC ファイルをローカルに配置できます。これを一般的な解決方法として使用することは推奨されません。自動 PAC ファイル検出には適していませんが、テストには役立つ可能性があります。

関連項目

- Secure Web Applianceでの PAC ファイルのホスト, on page 126
- クライアント アプリケーションでの PAC ファイルの指定, on page 127

- Secure Web Applianceでの PAC ファイルのホスト, on page 126
- クライアント アプリケーションでの PAC ファイルの指定, on page 127

プロキシ自動設定（PAC）ファイルを検索するクライアント オプション

クライアントに対して PAC ファイルを使用する場合は、クライアントが PAC ファイルを検索する方法を選択する必要があります。以下の 2 つの対処法があります。

- **PAC ファイルの場所をクライアントに設定する。**この PAC ファイルを明確に差し指す URL をクライアントに設定します。
- **PAC ファイルの場所を自動的に検出するようにクライアントを設定する。**DHCP または DNS とともに WPAD プロトコルを使用して PAC ファイルを自動的に検索するようにクライアントを設定します。

PAC ファイルの自動検出

WPAD は、DHCP および DNS ルックアップを使用してブラウザが PAC ファイルの場所を判別できるようにするプロトコルです。

- **DHCP と共に WPAD を使用するには、**DHCP サーバーに PAC ファイルの場所の URL と共にオプション 252 を設定します。ただし、すべてのブラウザが DHCP をサポートしているわけではありません。

- **DNS と共に WPAD を使用するには**、PAC ファイルのホスト サーバーを指し示すように DNS レコードを設定します。

いずれかまたは両方のオプションを設定できます。WPAD は最初に DHCP を使用して PAC ファイルの検出を試み、検出できなかった場合は DNS を使って試みます。

関連項目

- クライアントでの PAC ファイルの自動検出, on page 128

Secure Web Applianceでの PAC ファイルのホスト

Procedure

ステップ 1 [セキュリティ サービス（Security Services）] > [PAC ファイル ホスティング（PAC File Hosting）] を選択します。

ステップ 2 [設定の有効化と編集（Enable and Edit Settings）] をクリックします。

ステップ 3 （任意）以下の基本設定項目を設定します。

オプション	説明
PAC サーバー ポート（PAC Server Ports）	Secure Web Applianceが PAC ファイル要求のリッスンに使用するポート。
PAC ファイルの有効期限（PAC File Expiration）	ブラウザ キャッシュで指定されている分数が経過した後に PAC ファイルを期限切れにできます。

ステップ 4 [PACファイル（PAC Files）] セクションで [参照（Browse）] をクリックし、 Secure Web Applianceにアップロードする PAC ファイルをローカルマシンから選択します。

Note
選択したファイルの名前が `default.pac` である場合は、ブラウザで場所を設定するときにファイル名を指定する必要がありません。名前が指定されていない場合、 Secure Web Applianceは `default.pac` というファイルを検索します。

ステップ 5 [アップロード（Upload）] をクリックして、ステップ 4 で選択した PAC ファイルを Secure Web Appliance にアップロードします。

ステップ 6 （任意）[PAC ファイルサービスを直接提供するホスト名（Hostnames for Serving PAC Files Directly）] セクションで、ポート番号を含まない PAC ファイル要求のホスト名と関連ファイル名を設定します。

オプション	説明
ホスト名（Hostname）	Secure Web Applianceが要求を処理する場合に、PAC ファイル要求に含める必要があるホスト名。要求にはポート番号が含まれていないため、要求は Web プロキシの HTTP ポート（ポート80）を使用して処理され、ホスト名評価から PAC ファイル要求として識別できます。

オプション	説明
プロキシ ポートを通じた「GET」要求に対するデフォルト PAC ファイル（Default PAC File for "Get/" Request through Proxy Port）	同じ行のホスト名に関連付けられる PAC ファイル名。ホスト名に対する要求は、ここで指定した PAC ファイルを返します。 アップロード済みの PAC ファイルのみを選択できます。
行を追加（Add Row）	別の行を追加して、追加のホスト名と PAC ファイル名を指定します。

ステップ 7 変更を送信し、保存します。

クライアント アプリケーションでの PAC ファイルの指定

- クライアントでの PAC ファイルの場所の手動設定, on page 127
- クライアントでの PAC ファイルの自動検出, on page 128

クライアントでの PAC ファイルの場所の手動設定

Procedure

ステップ 1 PAC ファイルを作成してパブリッシュします。

ステップ 2 ブラウザの PAC ファイル設定領域に PAC ファイルの場所を示す URL を入力します。

Secure Web Applianceが PAC ファイルをホストしている場合、有効な URL 形式は以下のようになります。

```
http://server_address[.domain][:port][/filename] | http://WSAHostname[/filename]
```

WSAHostname は、 Secure Web Applianceに PAC ファイルをホストするときに設定した [ホスト名（hostname）] の値です。ホストしていない場合、URL の形式は格納場所と（場合によっては）クライアントに応じて異なります。

What to do next

- Secure Web Applianceでの PAC ファイルのホスト, on page 126

クライアントでの PAC ファイルの自動検出

Procedure

ステップ 1 wpad.dat という名前の PAC ファイルを作成し、Web サーバーまたは Secure Web Applianceにパブリッシュします（DNS と共に WPAD を使用する場合は、Web サーバーのルートフォルダにファイルを配置する必要があります）。

ステップ 2 次の MIME タイプで .dat ファイルを設定するように Web サーバーを設定します。

```
application/x-ns-proxy-autoconfig
```

Note
Secure Web Applianceはこれを自動的に実行します。

ステップ 3 DNS ルックアップをサポートするには、「wpad」から始まる、内部的に解決可能な DNS 名を作成して（例：wpad.example.com）、wpad.dat ファイルをホストしているサーバーの IP アドレスに関連付けます。

ステップ 4 DHCP ルックアップをサポートするには、DHCP サーバーのオプション 252 に wpad.dat ファイルの場所の URL を設定します（例：「http://wpad.example.com/wpad.dat」）。URL には、IP アドレスなど、有効な任意のホスト アドレスを使用できます。特定の DNS エントリは必要ありません。

What to do next

- クライアント アプリケーションによる PAC ファイルの使用, on page 125
- Secure Web Applianceでの PAC ファイルのホスト, on page 126
- Firefox で WPAD を使用できない

FTP プロキシ サービス

- FTP プロキシ サービスの概要, on page 128
- FTP プロキシの有効化と設定, on page 129

FTP プロキシ サービスの概要

Web プロキシは、以下の 2 種類の FTP 要求を代行受信できます。

- **ネイティブ FTP。**ネイティブ FTP 要求は、専用 FTP クライアントによって生成されます（または、ブラウザで組み込みのFTPクライアントを使用して生成されます）。FTPプロキシが必要です。
- **FTP over HTTP。**ブラウザは、ネイティブ FTP を使用する代わりに、HTTP 要求内に FTP 要求をエンコードすることがあります。FTP プロキシは必要ありません。

関連項目

- FTP プロキシの有効化と設定, on page 129

- FTP 通知メッセージの設定

FTP プロキシの有効化と設定

Note FTP over HTTP 接続に適用されるプロキシ設定を設定するには、Web プロキシの設定, on page 107を参照してください。

Procedure

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

ステップ 2 [設定の有効化と編集（Enable and Edit Settings）] をクリックします（表示されるオプションが [設定の編集（Edit Settings）] だけの場合、FTP プロキシは設定済みです。）

ステップ 3 （オプション）基本的な FTP プロキシ設定項目を設定します。

プロパティ	説明
プロキシ リスニング ポート（Proxy Listening Port）	FTP プロキシが FTP 制御接続をリッスンするポート。クライアントは、（FTP サーバーに接続するためのポート（通常はポート 21 を使用）としてではなく）FTP プロキシを設定するときにこのポートを使用する必要があります。
キャッシング（Caching）	匿名ユーザーからのデータ接続をキャッシュするかどうか。 **Note** 匿名ではないユーザーからのデータはキャッシュされません。
サーバー側の IP スプーフィング（Server Side IP Spoofing）	FTP プロキシが FTP サーバーの IP アドレスをシミュレートできるようにします。これによって、IP アドレスが制御接続とデータ接続で異なる場合に、トランザクションを許可しない FTP クライアントに対応できます。
クライアント IP スプーフィング	FTP プロキシが FTP クライアントの送信元 IP アドレスを模倣できるようにします。有効にすると、FTP 要求は FTP プロキシではなく FTP クライアントから発信されたように見えます。
認証形式（Authentication Format）	FTP クライアントと通信するときに FTP プロキシが使用する認証形式を選択できるようにします。
パッシブモードのデータポート範囲（Passive Mode Data Port Range）	パッシブ モード接続で FTP プロキシとのデータ接続を確立するために FTP クライアントが使用する TCP ポートの範囲。

プロパティ	説明
アクティブモードのデータポート範囲（Active Mode Data Port Range）	アクティブ モード接続で FTP プロキシとのデータ接続を確立するために FTP サーバーが使用する TCP ポートの範囲。この設定は、ネイティブ FTP および FTP over HTTP 接続の両方に適用されます。 ポート範囲を大きくすると、同じ FTP サーバーからのさらに多くの要求に対応できます。TCP セッションの TIME-WAIT 遅延（通常数分）によって、ポートは使用された直後に、同じ FTP サーバーで再び使用できるようになりません。その結果、所定の FTP サーバーは短時間アクティブ モードで *n* 回以上 FTP プロキシに接続できません。ここでは *n* は、このフィールドに指定されたポート数です。
ウェルカム バナー（Welcome Banner）	接続時に FTP クライアントに表示されるウェルカム バナー。次から選択します。 • **[FTP サーバーメッセージを（FTP server message）]**。メッセージは宛先 FTP サーバーによって表示されます。このオプションは、Web プロキシが透過モードに設定されている場合にのみ利用でき、透過接続にのみ適用されます。 • **[カスタム メッセージ（Custom message）]**。このオプションをオンにすると、すべてのネイティブ FTP 接続に対してこのカスタム メッセージが表示されます。オフにした場合は、明示的な転送ネイティブ FTP 接続に使用されます。

ステップ 4 （オプション）FTP プロキシの詳細設定を設定します。

プロパティ	説明
制御接続のタイムアウト（Control Connection Timeouts）	現在のトランザクションが完了していない場合に、アイドル状態の FTP クライアントまたは FTP サーバーからの制御接続による通信を、FTP プロキシがさらに待機する最大時間（秒単位）。 • **[クライアント側（Client side）]**。アイドル状態の FTP クライアントとの制御接続のタイムアウト値。 • **[サーバー側（Server side）]**。アイドル状態の FTP サーバーとの制御接続のタイムアウト値。
データ接続のタイムアウト（Data Connection Timeouts）	現在のトランザクションが完了していない場合に、アイドル状態の FTP クライアントまたは FTP サーバーからのデータ接続による通信を、FTP プロキシがさらに待機する時間。 • **[クライアント側（Client side）]**。アイドル状態の FTP クライアントとのデータ接続のタイムアウト値。 • **[サーバー側（Server side）]**。アイドル状態の FTP サーバーとのデータ接続のタイムアウト値。

ステップ 5 変更を送信し、保存します。

What to do next

- FTP プロキシ サービスの概要, on page 128

SOCKS プロキシ サービス

SOCKS プロキシ サービスの概要

Secure Web Applianceには、SOCKS トラフィックを処理するための SOCKS プロキシが含まれます。SOCKSポリシーは、SOCKSトラフィックを制御するアクセスポリシーと同等です。アクセス ポリシーと同様に、識別プロファイルを使用して、各 SOCKS ポリシーによってどのトランザクションを管理するかを指定できます。SOCKS ポリシーをトランザクションに適用すると、ルーティング ポリシーによてトラフィックのルーティングを管理できます。

SOCKS プロキシでは、以下の点に注意してください。

- SOCKS プロトコルは、直接転送接続のみをサポートしています。
- SOCKSプロキシは、アップストリームプロキシをサポートしていません（アップストリーム プロキシに転送されません）。
- SOCKS プロキシは、Application Visibility and Control（AVC）、 Application Discovery and Control（ADC）、Data Loss Prevention（DLP）、およびマルウェア検出に使用されるスキャニングサービスをサポートしていません。
- SOCKS プロキシは、ポリシー追跡をサポートしていません。
- SOCKSプロキシは、SSL トラフィックを復号できません。これは、クライアントからサーバーにトンネリングします。

SOCKS トラフィックの処理のイネーブル化

Before you begin

Web プロキシをイネーブルにします。

Procedure

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

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [SOCKS プロキシを有効にする（Enable SOCKS Proxy）] を選択します。

ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

SOCKS プロキシの設定

Procedure

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

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [SOCKS プロキシを有効にする（Enable SOCKS Proxy）] を選択します。

ステップ 4 基本および高度な SOCKS プロキシ設定を設定します。

SOCKS プロキシ（SOCKS Proxy）	イネーブル。
SOCKS コントロール ポート（SOCKS Control Ports）	SOCKS 要求を受け入れるポート。デフォルトは 1080 です。
UDP リクエスト ポート（UDP Request Ports）	SOCKS サーバーがリッスンする必要がある UDP ポート。デフォルトは 16000 ～ 16100 です。
プロキシネゴシエーションタイムアウト（Proxy Negotiation Timeout）	ネゴシエーション段階で SOCKS クライアントからデータを送受信するのを待機する時間（秒単位）。デフォルトは 60 です。
UDP トンネル タイムアウト（Tunnel Timeout）	UDP トンネルを閉じる前に UDP クライアントまたはサーバーからのデータを待機する時間（秒単位）。デフォルトは 60 です。

SOCKS ポリシーの作成

Procedure

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [SOCKS ポリシー（SOCKS Policies）] を選択します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドに名前を割り当てます。

Note
各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

ステップ 4 （オプション）説明を追加します。

ステップ 5 [上記ポリシーを挿入（Insert Above Policy）] フィールドで、この SOCKS ポリシーに挿入する SOCKS ポリシーの場所を選択します。

Note
複数の SOCKS ポリシーを設定する場合、各ポリシーの論理的な順序を決定します。照合が適切に行われるように、ポリシーの順序を指定してください。

ステップ 6 [アイデンティティとユーザー（Identities and Users）] セクションで、このグループ ポリシーに適用する 1 つ以上の ID を選択します。

ステップ 7 （オプション）[詳細（Advanced）] セクションを拡張して、追加のメンバーシップ要件を定義します。

プロキシ ポート（Proxy Ports）	ブラウザに設定されたポート。 （オプション）Web プロキシへのアクセスに使用するプロキシ ポートによってポリシー グループのメンバーシップを定義します。[プロキシ ポート（Proxy Ports）] フィールドに、1 つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。 あるポート上に要求を明示的に転送するように設定されたクライアントのセットがあり、別のポート上に要求を明示的に転送するように設定された別のクライアントのセットがある場合、プロキシ ポート上でポリシー グループのメンバーシップを定義することがあります。 **Note** このポリシー グループに関連付けられている ID が この詳細設定によって ID メンバーシップを定義している場合、SOCKS ポリシー グループ レベルではこの設定項目を設定できません。
サブネット（Subnets）	（オプション）サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義します。 関連付けられた **ID** で**定義**できる**アドレス**を使用するか、または**特定のアドレス**をここに入力できます。 **Note** ポリシー グループに関連付けられている ID が、アドレスによってグループのメンバーシップを定義している場合は、このポリシー グループに、ID のアドレスのサブセットであるアドレスを入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込めます。
時間範囲（Time Range）	（オプション）時間範囲別にポリシー グループのメンバーシップを定義します。 **a.** [時間範囲（Time Range）] から時間範囲を選択します。 **b.** このポリシー グループが選択した時間範囲内または範囲外の時間に適用されるかどうかを指定します。

ステップ 8 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

What to do next

- （オプション）SOCKS ポリシーで使用するための ID を追加します。
- SOCKS トラフィックを管理する 1 つ以上の SOCKS ポリシーを追加します。

要求の代替受信に関するトラブルシューティング

- URL カテゴリが一部の FTP サイトをブロックしない
- 大規模 FTP 転送の切断
- ファイルのアップロード後に FTP サーバーにゼロ バイト ファイルが表示される
- アップストリーム プロキシ経由で FTP 要求をルーティングできない
- HTTPS および FTP over HTTP 要求が、認証を必要としないアクセス ポリシーにのみ一致する
- HTTPS 要求および FTP over HTTP 要求の場合にユーザーがグローバル ポリシーに一致

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。