セキュアなWebアプライアンスの初期設定の設定

内容

はじめに

このドキュメントでは、Secure Web Appliance(SWA)を初めて設定するために必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SWA管理。
- ネットワーキングの基本原則

Cisco では次の前提を満たす推奨しています。

- 物理または仮想SWAがインストールされている。
- SWAグラフィカルユーザインターフェイス(GUI)への管理アクセス。
- SWAコマンドラインインターフェイス(CLI)への管理アクセス。
- SWAコンソールへの管理アクセス。
- 有効なSWAライセンスまたはスマートライセンス管理ポータルへのアクセス (スマートラ

イセンスを使用している場合）

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

SWAのインストール

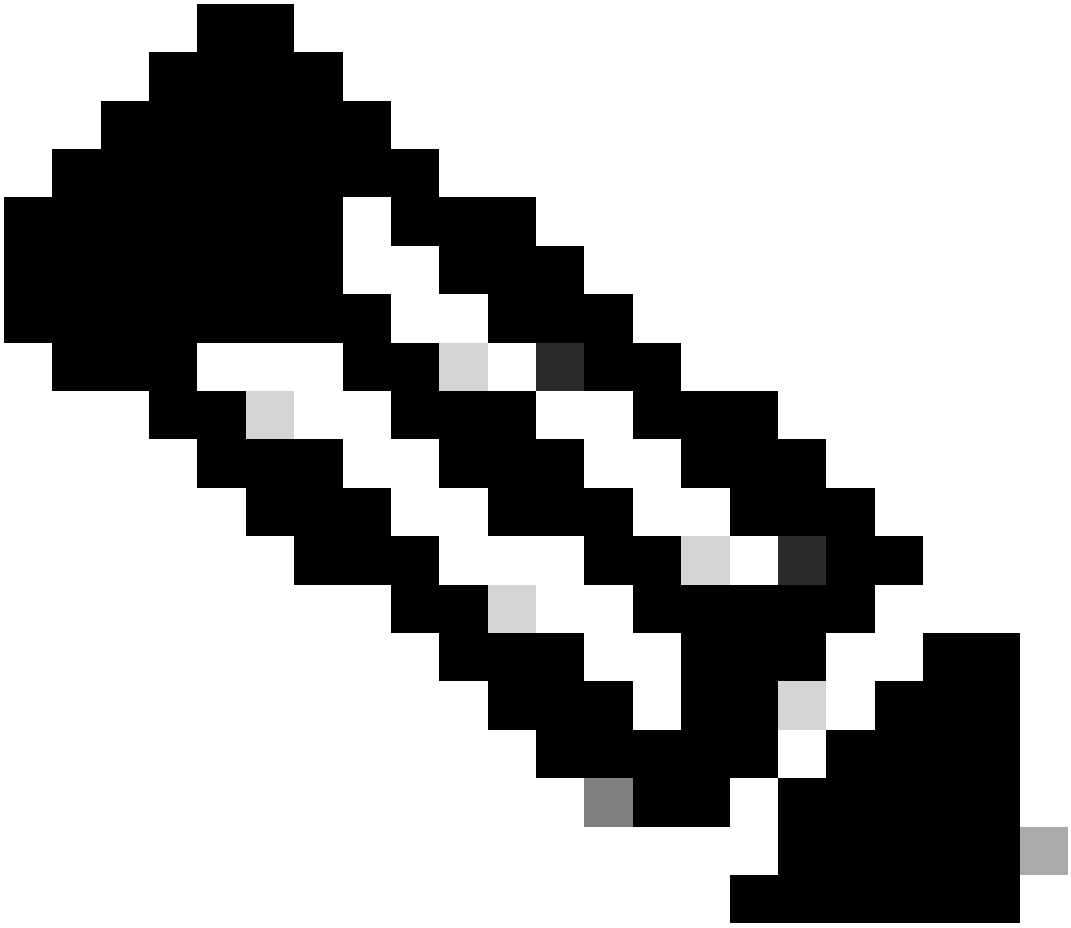
Cisco SWAは、組織のWebセキュリティと制御を強化するために設計されたフォワードプロキシソリューションです。SWAは仮想形式と物理形式の両方で使用でき、多様なニーズを満たす柔軟な導入オプションを提供します。仮想SWAは、Microsoft Hyper-V、VMware ESX、KVMなどの複数のハイパーバイザプラットフォームをサポートし、さまざまな仮想環境との互換性を確保します。物理アプライアンスをご希望のお客様には、S100、S300、S600の3種類のモデルをご用意しています。各モデルはさまざまなレベルのパフォーマンス要件やキャパシティ要件に対応できるように設計されているため、組織はそれぞれのWebセキュリティニーズに適したソリューションを見つけることができます。

仮想マシンイメージをダウンロードするには、https://software.cisco.com/download/homeにアクセスしてください。

仮想Cisco SWAのインストールは、適切なハイパーバイザプラットフォームの選択から始まる単純なプロセスです。まず、シスコのWebサイトから仮想SWAインストールファイルをダウンロードします。VMware ESXの場合は、OVAファイルを導入し、ネットワーク設定を構成し、CPU、メモリ、ストレージなどの十分なリソースを割り当てます。Microsoft Hyper-Vの場合は、ダウンロードしたVHDファイルをHyper-Vマネージャーにインポートし、それに応じて仮想マシンの設定を構成します。KVMの場合、virt-managerまたはvirshコマンドラインツールを使用して、ダウンロードしたイメージを使用する仮想マシンを定義および起動します。仮想マシンが起動して実行されたら、この記事の手順を使用して初期セットアップを行うことができます。

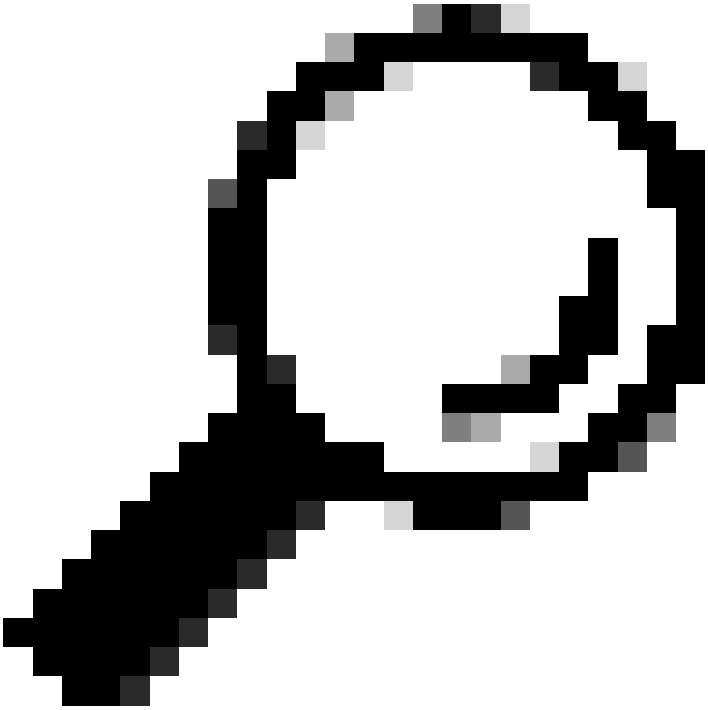
初期設定

SWAをインストールした後、初期導入のために次の手順を実行します。

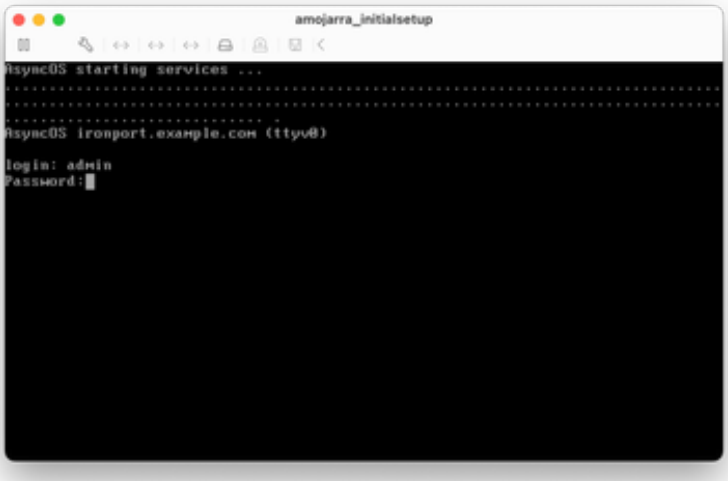


注：初期設定では、コンソール、SSH、およびGUIを使用してSWAにアクセスできる必要があります。

接続方法	段階	設定手順
コンソール	IPアドレスの設定	ステップ 1：ユーザ名とパスワードを入力して、CLIにログインします。



ヒント：デフォルトのユーザ名はadminで、デフォルトのパスワードはironportです。



イメージ：ログイン画面

ステップ 2：ifconfigを実行します。

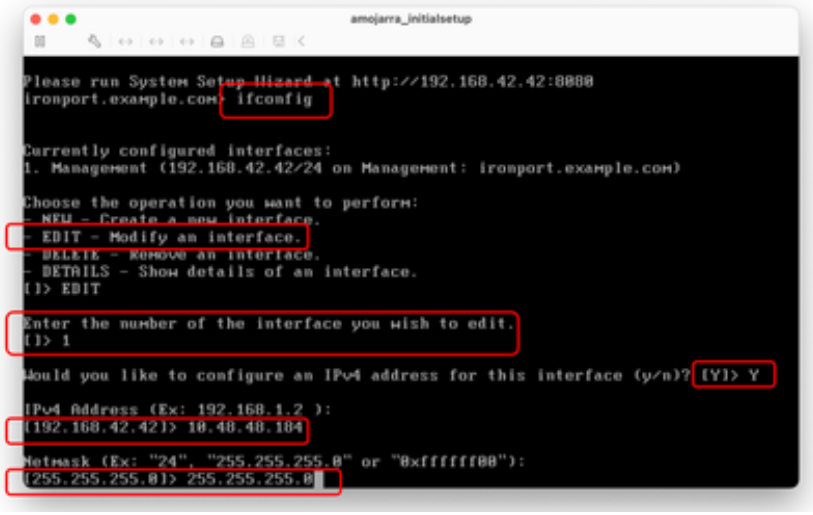
ステップ 3：[Edit] を選択します。

ステップ 4：管理インターフェイスに関連付けられている番号を入力します。

ステップ 5：デフォルトのIPv4アドレスを編集するには、Yを選択します。

手順 6：IPアドレス

手順 7：サブネットマスクを入力します。



イメージ：管理インターフェイスのIPアドレスの編集

ステップ 8：IPv6を設定する場合は、「Would you like to Configure IPv6?」という質問に対してYと入力します。これをデフォルト(No)のままにして、Enterキーを押します。

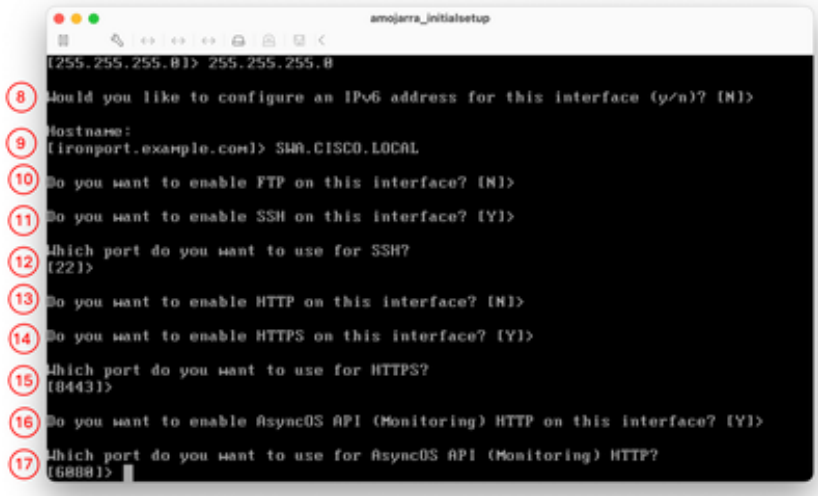
ステップ 9：ホスト名として完全修飾ドメイン名(FQDN)を入力します。

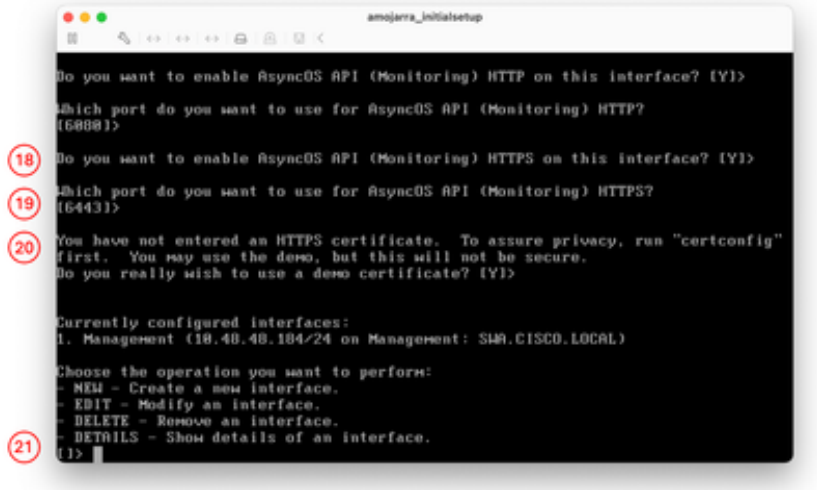
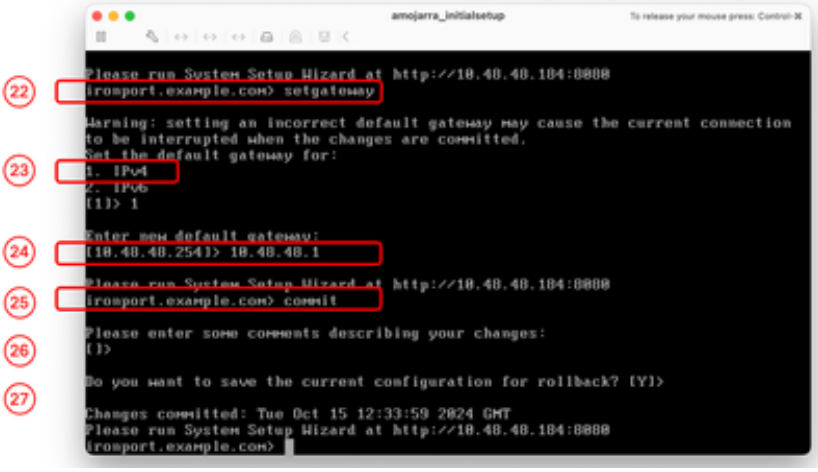
ステップ 10：ファイル転送プロトコル(FTP)による管理インターフェイスへのアクセスを有効にするには、Yを選択するか、Enterキーを押します。

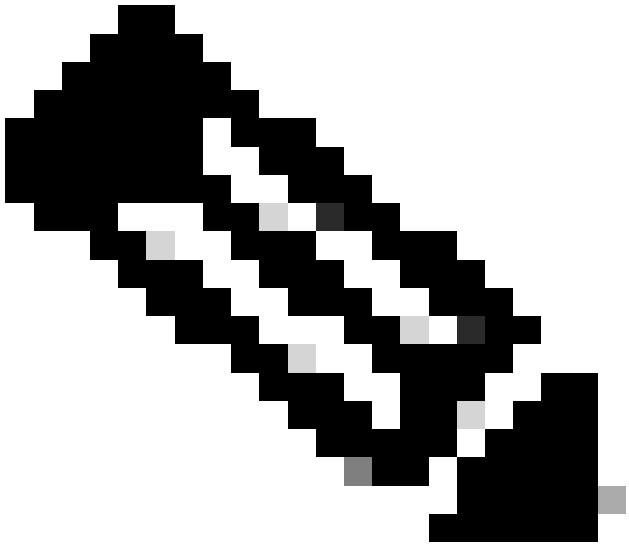
ステップ 11Secure Shell(SSH)はデフォルトで有効に設定されています。SSHを有効にすることをお勧めします。Yを入力して続行します。

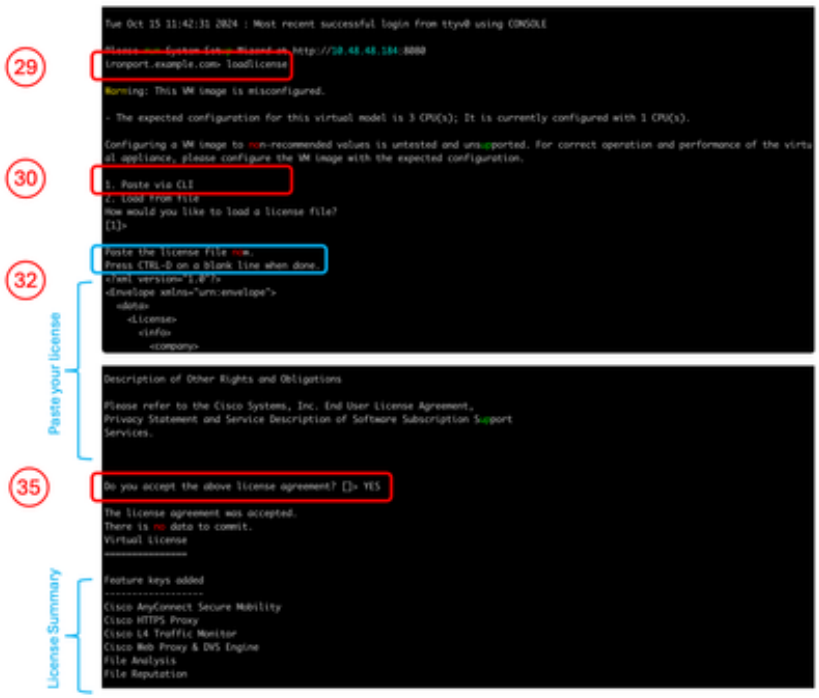
ステップ12:（オプション）デフォルトのSSHポートをTCP 22から任意のポート番号に変更できます（ただし、ポートの競合がない場合に限ります）。Enterキーを押して、デフォルトポート(TCP/22)を使用します。

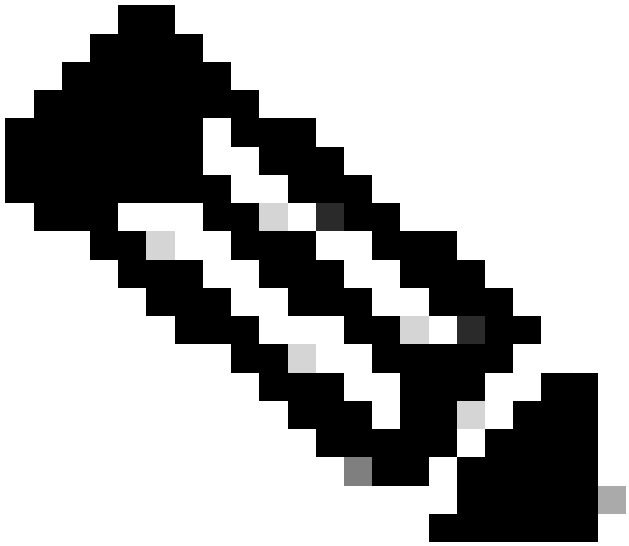
ステップ 13管理インターフェイスにハイパーテキスト転送プロトコル(HTTP)でアクセスする場合は、Yを入力して、HTTPアクセスのポート番号を設定します。それ以外の場合は、Nを選択して、Hypertext Transfer Protocol Secure（HTTPS；ハイパーテキスト転送プロトコル）だけが管理インターフェイスにアクセスできるようにします。

		ステップ 14：Yと入力してEnterキーを押し、管理インターフェイスへのHTTPSアクセスを有効にします。 ステップ 15：ポートの競合がない限り、デフォルトのHTTPSポート番号を8443から任意のポート番号に変更できます。デフォルトのポート(TCP/8443)を使用するには、Enterキーを押します。 ステップ 16： アプリケーションプログラミングインターフェイス(API)はデフォルトでEnableに設定されています。APIを使用していない場合は、Nを入力してEnterキーを押すことによりAPIを無効にできます。 ステップ 17：APIを有効にすると、ポートの競合がない限り、デフォルトのAPIポート番号を6080から任意のポート番号に変更できます。デフォルトのポート(TCP/6080)を使用するには、Enterキーを押します。  イメージ：管理インターフェイスサービスの設定 ステップ 18：AsyncOS API（モニタリング）はSWAの新しいGUIです。新しいユーザインターフェイスレポートを使用する場合は、このオプションをY（デフォルト）に設定します。それ以外の場合は、Nを入力してステップ20に進みます ステップ 19： ポートの競合がない限り、デフォルトの新規GUI HTTPSポート番号を6443から任意のポート番号に変更できます。デフォルトのポート(TCP/6443)を使用するには、Enterキーを押します。 ステップ 20：SWA管理インターフェイスは、シスコデモ証明書を使用します。Yを入力してデモ用証明書を受け入れます。初期設定後にGUI証明書を変更できます。 ステップ 21：Enterキーを押して、ifconfigウィザードを

		終了します。  イメージ：新しいGUI TCPの設定
	デフォルト ゲートウェイの設定	ステップ 22：setgatewayを実行します。 ステップ 23：管理インターフェイスがIPv4で設定されている場合はIPv4を選択し、それ以外の場合はIPv6を選択します。 ステップ 24：デフォルトゲートウェイのIPアドレスを入力します。 ステップ 25：commitを実行して、変更を保存します。 ステップ26:（オプション）保存する変更に関するメモを追加できます ステップ27:（オプション）変更を適用する前に、SWAで設定をバックアップできます。  イメージ：デフォルトゲートウェイの設定

SSH	従来のライセンスのインポート	 注：スマートライセンスを使用している場合は、ステップ36に進んでください。 ステップ 28： SSH経由でSWAに接続します。 ステップ 29：loadlicenseの実行 ステップ 30：Paste via CLIを選択します。 ステップ 31： テキストエディタでライセンスファイルを開き、その内容をすべてコピーします ステップ 32：ライセンスをSSHシェルに貼り付けます。 ステップ 33：Enterキーを押して、新しい行に移動します。 ステップ 34：Controlキーを押しながらDキーを押します。 ステップ 35：使用許諾契約書を読み、YESと入力して条件に同意します。

		 イメージ – 従来のライセンスのインポート ステップ 58 に進みます。
GUI	DNSサーバの設定	ステップ 37： GUIにログインします(デフォルトはHTTPS://<SWA FQDN or IP Address>:8443)。 ステップ 38：Networkに移動し、DNSを選択します。 ステップ 39：[Edit Settings] をクリックします。 ステップ40:「プライマリDNSサーバ」セクションで、「使用するDNSサーバ」を選択します。 ステップ 41：プライオリティを0に設定し、DNSサーバのIPアドレスを入力します。



注：Add Rowを選択すると、複数のDNSサーバを追加できます。

ステップ 42：[Submit] をクリックします。

ステップ 43：変更を保存します。

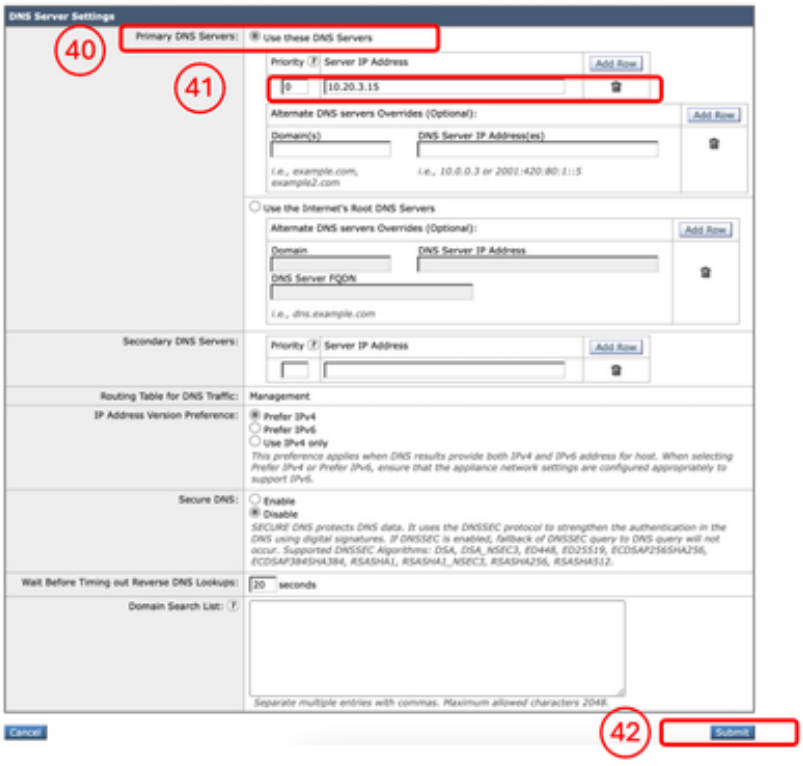
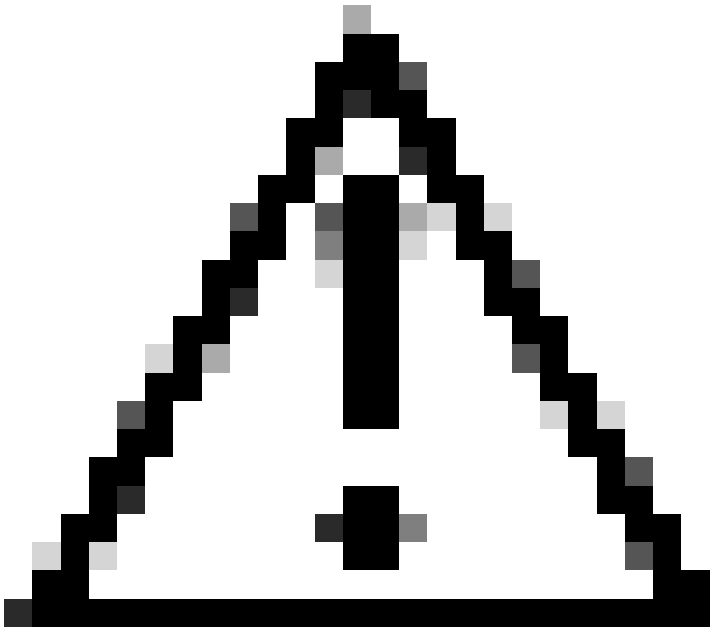
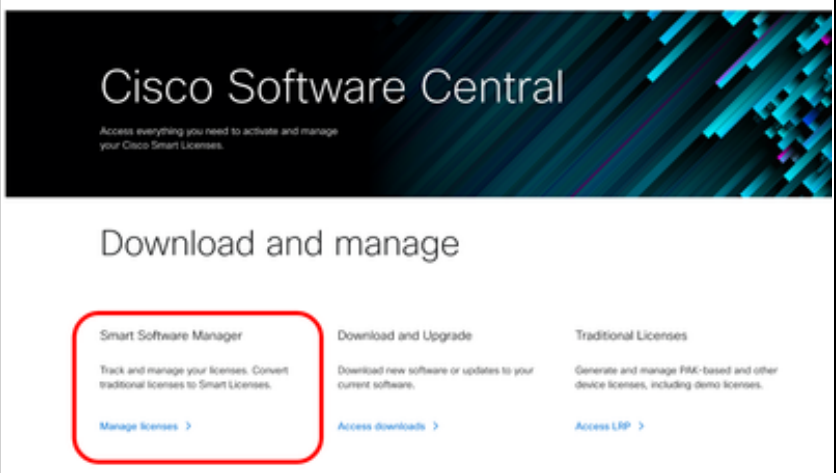


図 – DNSサーバの設定

	スマートライセンスの設定	ステップ 44：GUIで、System AdministrationからSmart Software Licensingを選択します。 ステップ 45： EnableSmart Software Licensingを選択します。  注意：アプライアンスでスマートライセンス機能を有効にした後で、スマートライセンスからクラシックライセンスにロールバックすることはできません。 ステップ 46： OKをクリックしてスマートライセンスの設定を続行します。 ステップ 47：変更を保存します。 ステップ 48： SWAを登録するためのトークンを取得するには、Cisco Software Central(https://software.cisco.com/#)にログインします ステップ 49：Manage Licensesをクリックします。



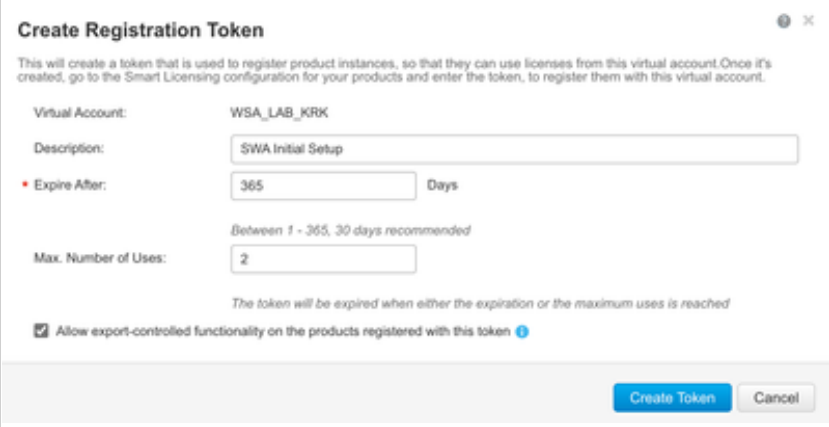
イメージ：Cisco Smart License Management

ステップ 50：Smart Software Licensingで、Inventoryを選択します。

ステップ 51：Generalタブで、New Tokenを作成するか、利用可能なトークンを使用します。

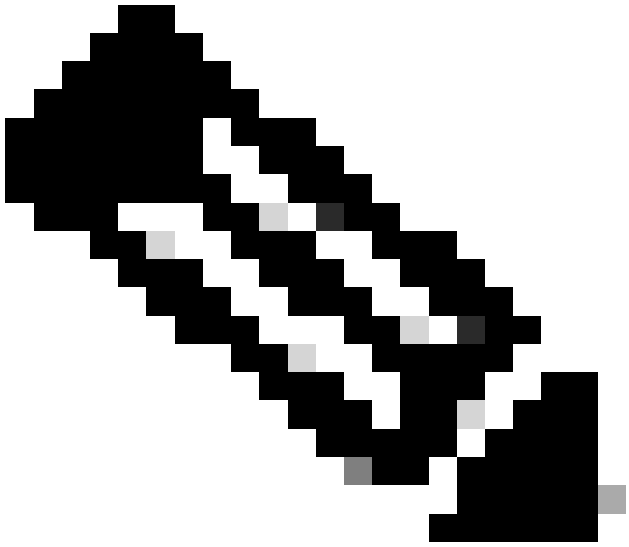
イメージ：スマートソフトウェアライセンスのインベントリページ

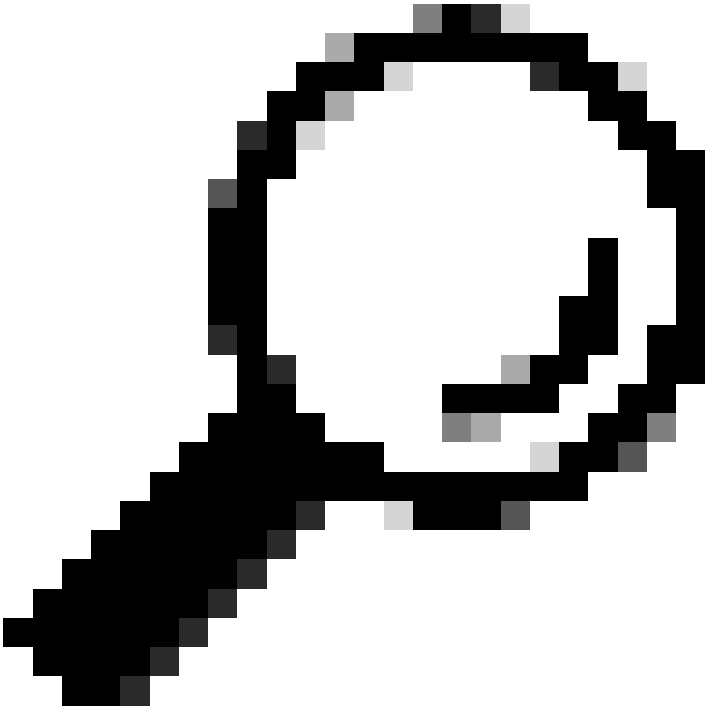
ステップ 52：必要な情報を入力し、トークンの作成を入力します。



イメージ：トークンの生成

ステップ 53：新しく追加したトークンの前にある青いア

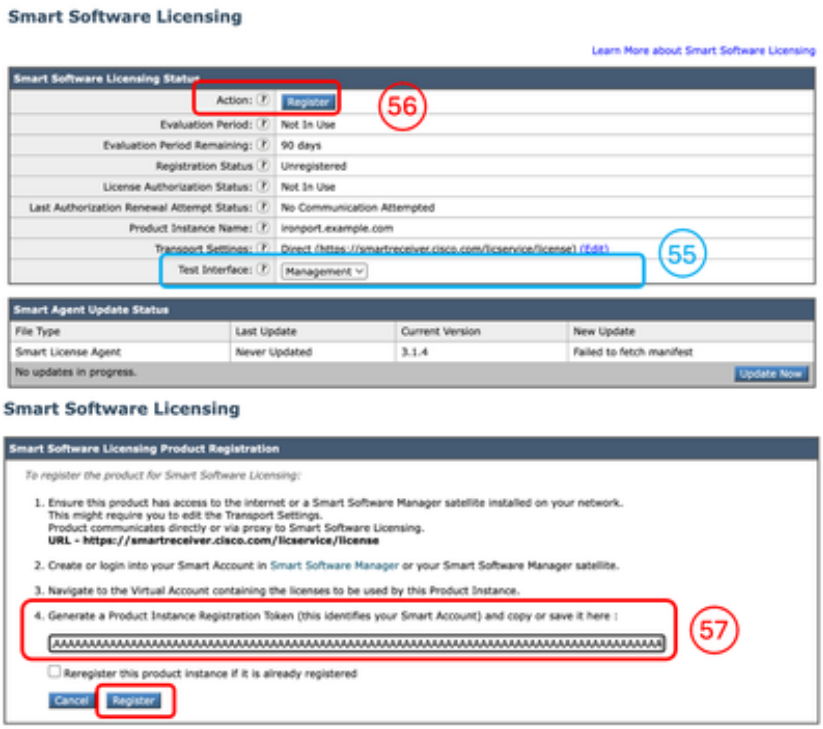
		イコンをクリックして、その内容をコピーします。  イメージ：トークンのコピー ステップ 54： SWA GUIで、System Administrationに移動し、Smart Software Licensingを選択します。
		 注：すでにSmart Software Licensingページが表示されている場合は、ページを更新してください。
		ステップ55: (オプション) SWAが管理インターフェイスからインターネットにアクセスできない場合は、テストインターフェイスを、インターネットへのアクセスが許可されているインターフェイスに変更できます。

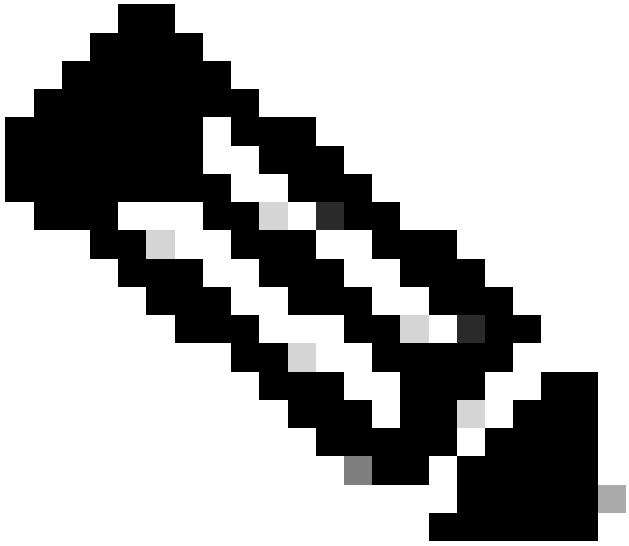
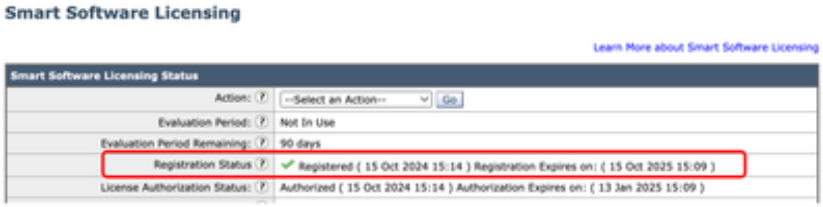


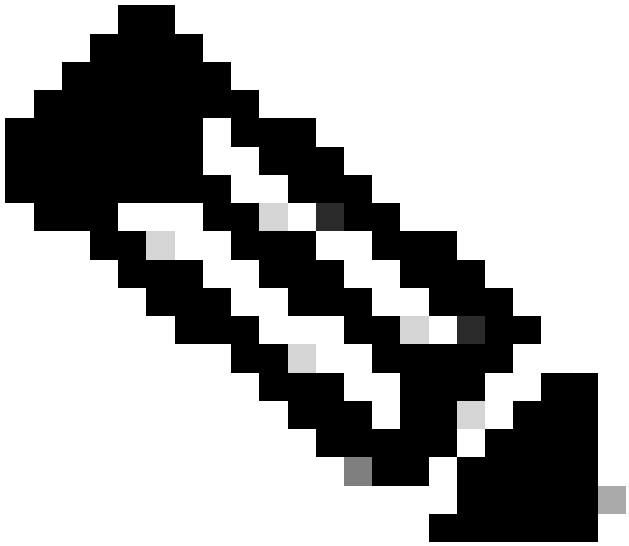
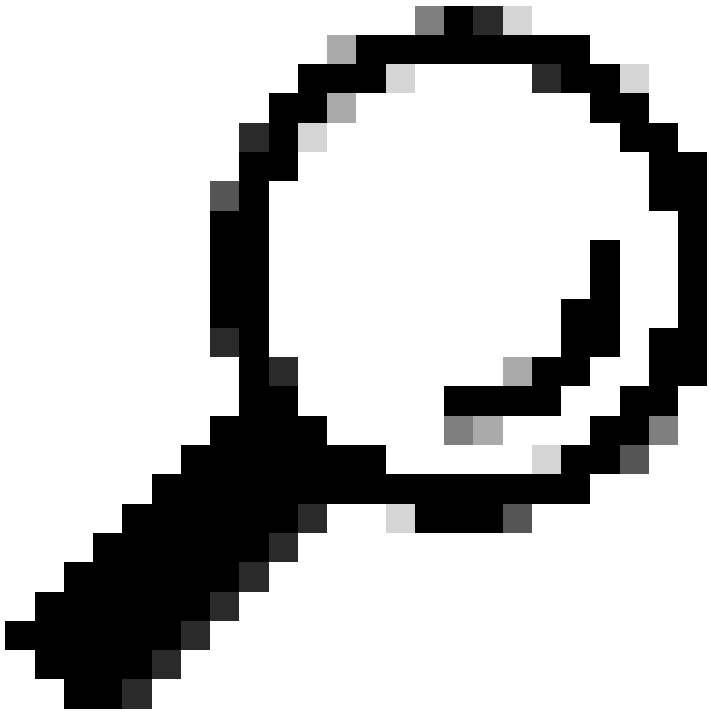
ヒント：複数のインターフェイスの設定とルーティングテーブルの詳細については、この記事の「ネットワーク設定」の項を参照してください。

ステップ 56：[Register] をクリックします。

ステップ 57：Tokenを貼り付け、Registerをクリックします。



		イメージ：スマートライセンスへのSWAの登録  注：登録を確認するには、数分待ってからSWAのスマートライセンスページを更新し、登録ステータスを確認します。  イメージ：スマートライセンスの登録ステータス
	システムセットアップウィザード	ステップ 58： SWA GUIで、System Administrationに移動し、System Setup Wizardを選択します。 ステップ 59：このライセンス契約の条項を読んで同意する。 ステップ 60：Begin Setupをクリックします。 ステップ 61：選択 標準」 Appliance Mode of Operationセクションで確認できます。 ステップ 62：Default System Hostnameを入力します。

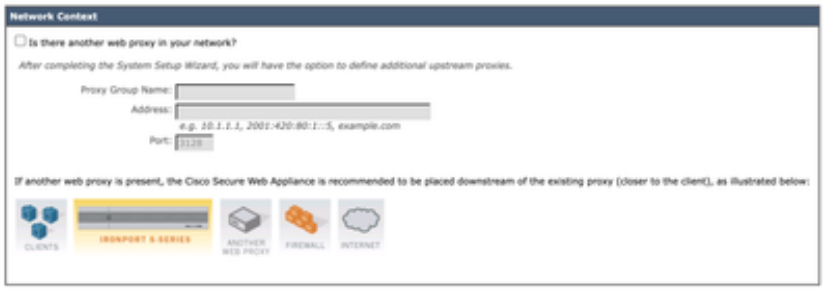
		 注：ステップ9で作成した以前のホスト名は管理インターフェイスに関連するもので、SWAに関連するものではありません。
		ステップ 63：DNSサーバのIPアドレスを入力します。 ステップ64:ネットワークタイムプロトコル(NTP)サーバを設定できます。
		 ヒント:NTPサーバで認証が必要な場合は、キーパ

ラメータを設定できます。

ステップ 65：SWAに適用するタイムゾーンを選択して、Nextをクリックします。

イメージ – システムセットアップウィザード – システム設定

ステップ66:（オプション）ネットワークでアップストリームプロキシを使用している場合は、ネットワークコンテキストページで設定するか、デフォルトのままにしてNextをクリックします。

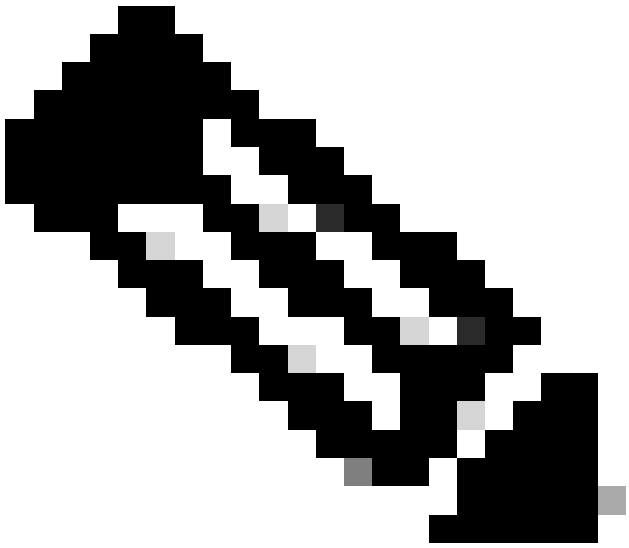
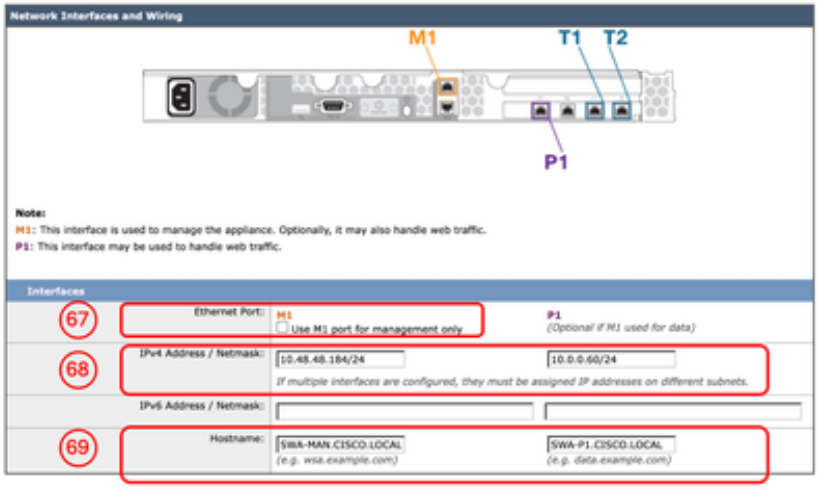


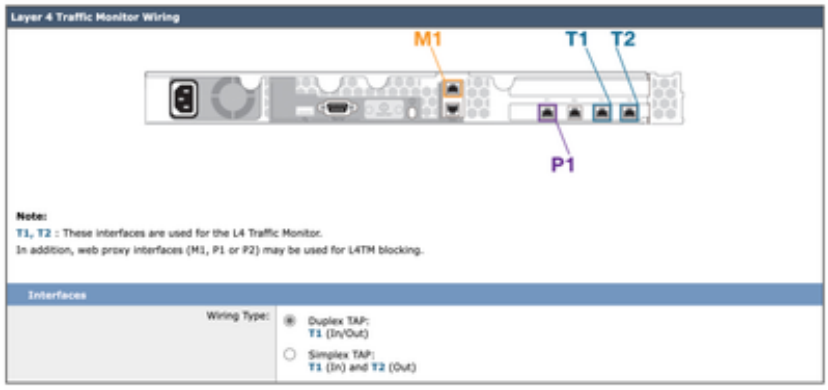
イメージ – システムセットアップウィザード – アップストリームプロキシ設定

ステップ67:（オプション）管理インターフェイストラフィックをデータインターフェイス（P1およびP2インターフェイス）トラフィックから分離する必要がある場合は、「管理のみにM1ポートを使用する」を選択します。

ステップ68:（オプション）ネットワークインターフェイスのIPアドレスは、「IPv4アドレス/ネットマスク」セクションまたは「IPv6アドレス/ネットマスク」セクションで追加または変更できます。

ステップ69:（オプション）ネットワークインターフェイスのホスト名を追加または変更し、Nextをクリックでき

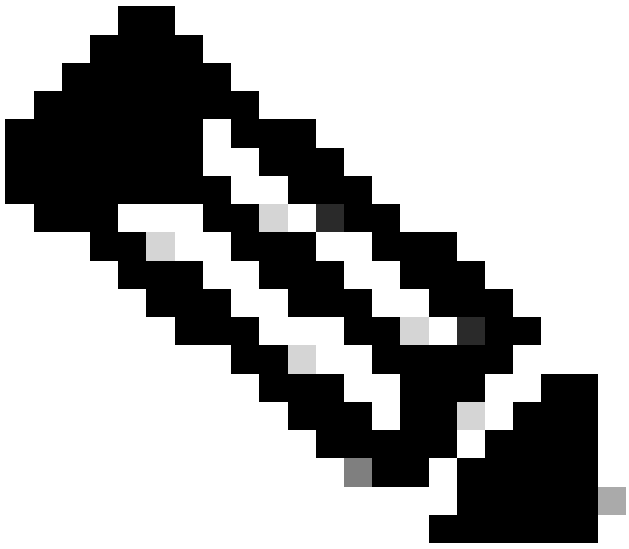
		ます。  注:P1ポートは、システムセットアップウィザードを使用して有効にし、設定できます。P2インターフェイスを有効にするには、システムセットアップウィザードを完了した後で行う必要があります。  イメージ – システムセットアップウィザード – ネットワークインターフェイスの設定 ステップ70:（オプション）レイヤ4トラフィックモニタ(L4TM)を設定する予定の場合は、デュプレックス設定を設定するか、デフォルトのままにしてNextをクリックします。



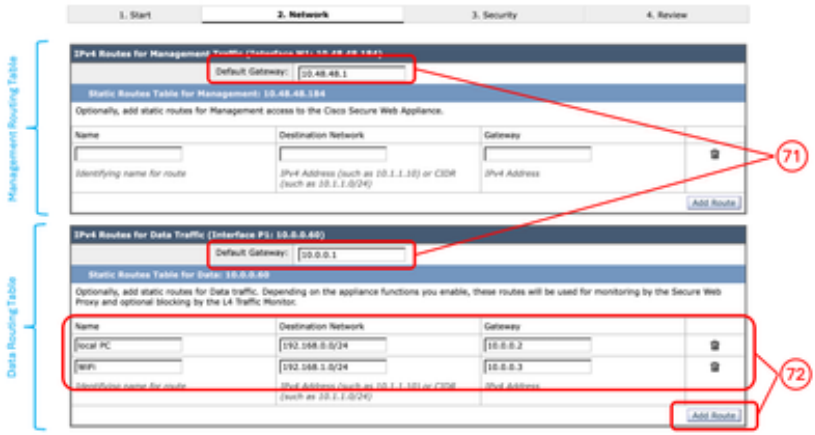
イメージ – システムセットアップウィザード – レイヤ4トラフィックモニタの設定

手順71: (オプション) IPv4ルートの管理ページで、デフォルトゲートウェイを変更できます

ステップ72: (オプション) スタティックルートを作成するためにルートを追加できます。

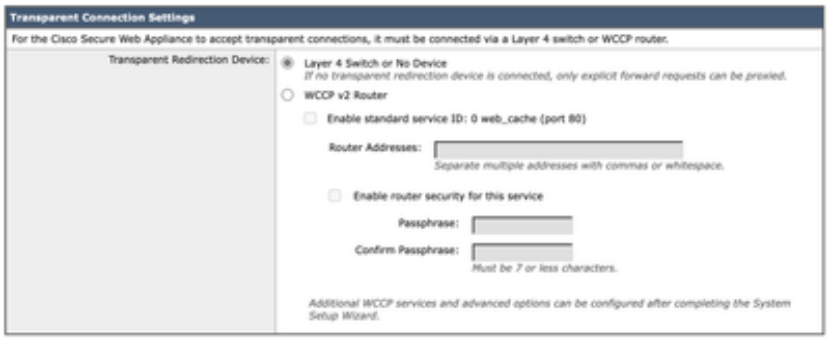


注：ステップ67で「管理のみにM1ポートを使用する」を選択した場合、管理インターフェイス (P1とP2) とデータインターフェイス (P1とP2) 用に2つの別個のルーティングテーブルが存在することになります。



イメージ – システムセットアップウィザード – ルートの追加

ステップ73:（オプション）Web Cache Communication Protocol(WCCP)を使用して透過型プロキシ導入を設定する場合は、WCCPを設定するか、デフォルトのレイヤ4スイッチをNo Device（デフォルト）のままにして、Nextをクリックします。



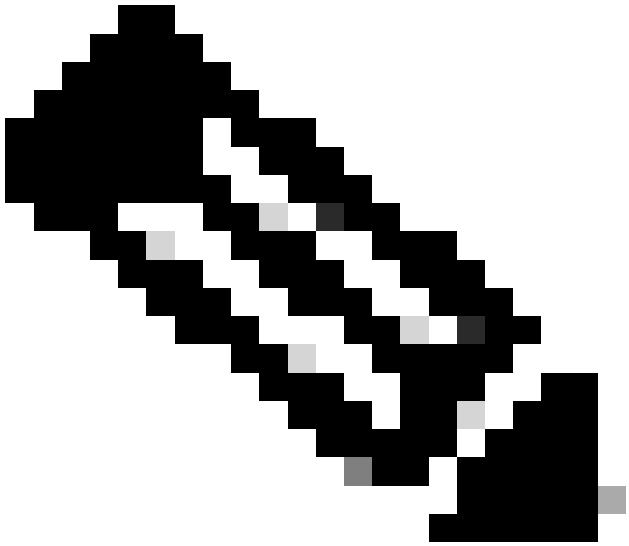
イメージ – システムセットアップウィザード – プロキシ配置の構成

ステップ 74：管理者アカウントの新しいパスワードを設定します。

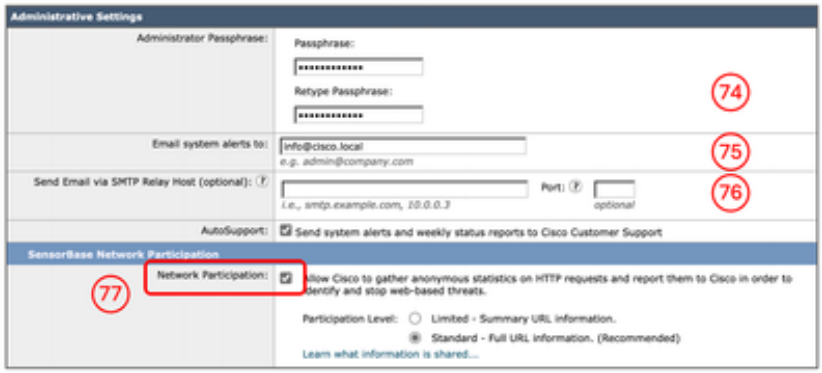
ステップ 75：システムアラートを受信する電子メールアドレスを入力します。

ステップ76:（オプション）シンプルメール転送プロトコル(SMTP)リレーホスト情報を指定します。それ以外の場合は空白のままにします 内部リレーホストが定義されていない場合、SMTPはMXレコードのDNSルックアップを使用します。

ステップ77:（オプション）Cisco SensorBaseネットワークへの参加を無効にする場合は、Network Participationチェックボックスのチェックを外します。デフォルトのままにする場合は、Nextをクリックします。

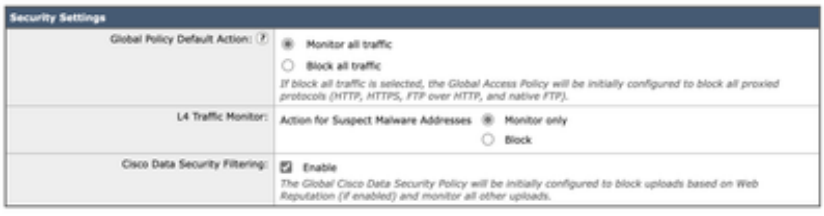


注：Cisco SensorBaseネットワークに参加することは、シスコがデータを収集し、その情報をSensorBase脅威管理データベースと共有することを意味します。



イメージ – システムセットアップウィザード – 管理設定

ステップ78: (オプション) グローバルポリシー、L4TM、およびCisco Data Security Filteringのデフォルトのアクションを変更するか、デフォルトのままにしてNextをクリックします。



イメージ – システムセットアップウィザード – セキュリティ設定

		ステップ 79：設定を確認します。変更が必要な場合は、Previousボタンをクリックして前のページに戻るか、Install This Configurationをクリックします。

ネットワーク設定

ネットワークインターフェイスを設定するには、CLIとGUIの両方を使用できます。

	コマンド/パス	アクション
CLIからのネットワークインターフェイスカードの設定	CLI > ifconfig	新規：インターフェイスがifconfig出力にリストされていないが、仮想マシンまたは物理アプライアンスに存在する場合は、このコマンドを使用してリストにインターフェイスを表示できます。 Edit：このアクションは、IPアドレス、サブネットマスク、インターフェイスホスト名、またはその他の関連パラメータを編集することです。 Details：インターフェイスの詳細（MACアドレス、メディアタイプ、デュプレックスモードなど）を表示します。 Delete：インターフェイスをifconfigリストから削除します。以前にIPアドレスが割り当てられている場合、このリストからIPアドレスを削除します。
GUIからのネットワークインターフェイスカードの設定	GUI >ネットワーク>インターフェイス	インターフェイスのIPアドレスとホスト名を編集できます。 ポート番号を有効、無効、または変更するには、 FTP、SSH、HTTPアクセス、HTTPSアクセスなどのアプライアンス管理サービス。

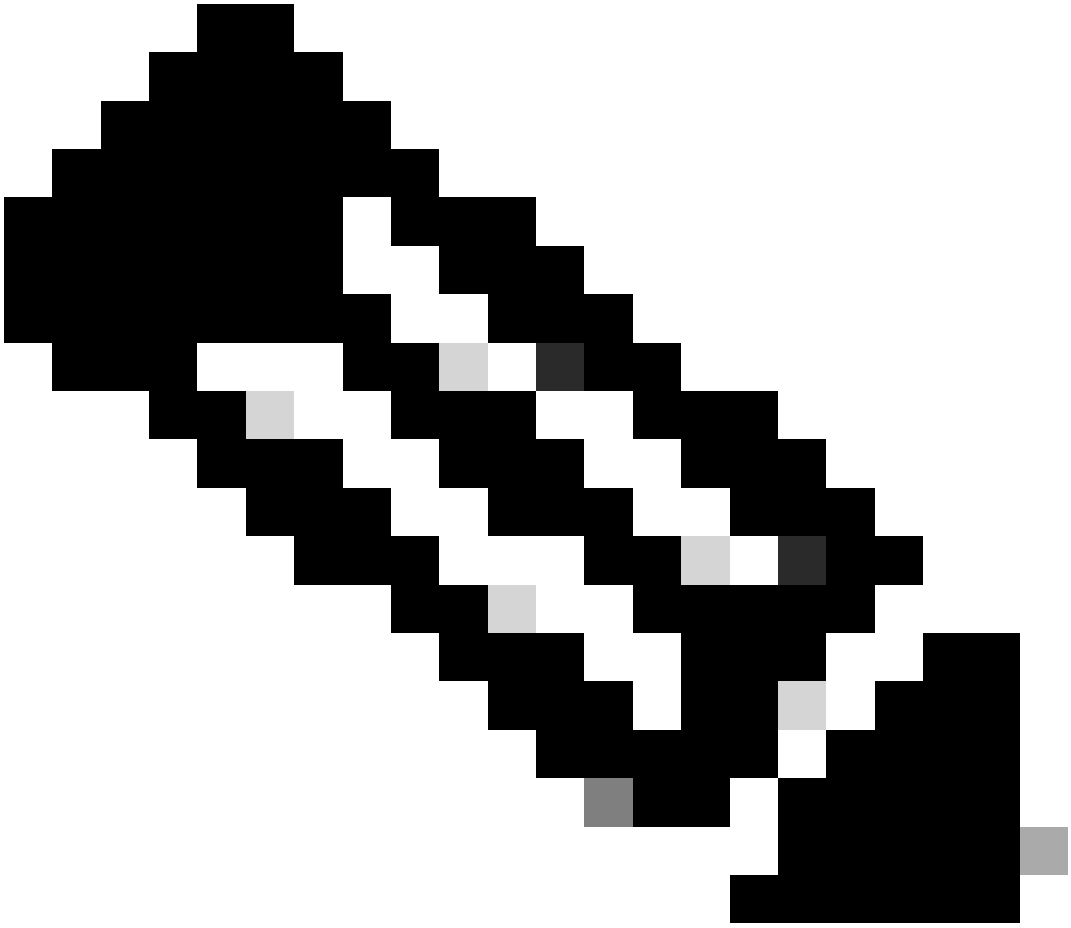
ルーティング テーブル

ルートは、ネットワークトラフィックの送信先を決定するために不可欠です。SWAは次のタイプのトラフィックを処理します。

- データトラフィック：これには、インターネットを閲覧しているエンドユーザからWebプロキシによって処理されたトラフィックが含まれます。
- 管理トラフィック：これには、Webインターフェイス経由でアプライアンスを管理することによって生成されるトラフィックと、SWAのアップグレード、コンポーネントの更新、DNS、認証、その他の関連タスクなどの管理サービス用のトラフィックが含まれます。

デフォルトでは、どちらのタイプのトラフィックも、設定されたすべてのネットワークインターフェイスに対して定義されたルートを使用します。ただし、ルーティングを分離するオプションがあるため、管理トラフィックは専用の管理ルーティングテーブルを使用し、データトラフィックは別個のデータルーティングテーブルを使用します。

管理トラフィック	データ トラフィック
WebUI SSH SNMP ドメインコントローラによる認証(設定可能) Syslog FTPプッシュ DNS(設定可能) アップデート/アップグレード/機能キー(設定可能)	HTTPプロキシ HTTPSプロキシ FTPプロキシ WCCPネゴシエーション 外部DLPサーバによるICAP要求 DNS(設定可能) アップデート/アップグレード/機能キー(設定可能) ドメインコントローラを使用した認証(設定可能)



注:[管理のみにM1ポートを使用する]オプションを選択すると、データルーティングテーブルと呼ばれる追加のルーティングテーブルがSWAに追加されます。このルーティングテーブルには、設定可能なデフォルトゲートウェイが1つだけあります。追加のルーティングパスは手動で設定する必要があります。

関連情報

- AsyncOS 15.2 for Cisco Secure Web Applianceユーザガイド
- Cisco Secure Email & Web仮想アプライアンスインストールガイド
- Secure Web ApplianceでのカスタムURLカテゴリの設定：シスコ
- セキュアなWebアプライアンスのベストプラクティスの使用
- セキュアWebアプライアンス用のファイアウォールの設定
- セキュアWebアプライアンスでの復号化証明書の設定

- SWAでのSNMPの設定およびトラブルシューティング
- Microsoftサーバを使用したセキュアWebアプライアンスでのSCPプッシュログの設定
- SWAで特定のYouTubeチャネル/ビデオを有効にし、YouTubeの残りをブロックする
- Secure Web ApplianceのHTTPSアクセスログ形式について
- セキュアなWebアプライアンスのログへのアクセス
- セキュアWebアプライアンスでの認証のバイパス
- Secure Web Applianceでのトラフィックのブロック
- Secure Web ApplianceでのMicrosoft Updatesトラフィックのバイパス

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。