# Cisco Stealthwatch

システム コンフィギュレーション ガイド v7.3

# 目次

# はじめに

## 概要

次の Cisco Stealthwatch™ Enterprise ハードウェアおよびバーチャルエディション（VE）アプライアンスを v7.3.2 の 1 つの管理対象システムに設定するには、このガイドを使用します。

- Stealthwatch Management Console（SMC）
- Stealthwatch Flow Collector
- Stealthwatch Data Node
- Stealthwatch Flow Sensor
- Stealthwatch UDP Director

Stealthwatch の詳細については、次のオンライン リソースを参照してください。

- **概要**：https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html［英語］
- **アプライアンス**：https://www.cisco.com/c/en/us/products/security/stealthwatch/datasheet-listing.html［英語］
- **リリースノート**：詳細については、リリースノートを参照してください。

## 対象読者

このガイドは、Stealthwatch 製品のインストールおよび設定を担当するネットワーク管理者とその他の担当者を対象としています。

仮想アプライアンスを設定する場合は、VMware または KVM の基本的な知識があることを前提としています。

専門家によるインストールを希望する場合は、最寄りのシスコ パートナーまたは Cisco Stealthwatch サポートに連絡してください。

## 用語

このガイドでは、Stealthwatch FlowSensor Virtual Edition（VE）などの仮想製品を含むすべての Stealthwatch 製品に対し「アプライアンス」という用語を使用しています。

「クラスタ」は、StealthWatch Management Console（SMC）で管理される Stealthwatch アプライアンスのグループです。

## 略語

このガイドでは、次の略語が使用される場合があります。

| 略語 | 定義 |
|---|---|
| DNS | ドメイン ネーム システム（サービスまたはサーバ） |
| dvPort | 分散仮想ポート |
| ESX | Enterprise Server X |
| GB | ギガバイト |
| IDS | 侵入検知システム |
| IPS | 侵入防御システム |
| ISO | International Standards Organization; 国際標準化機構 |
| IT | 情報技術 |
| KVM | カーネルベース仮想マシン |
| MTU | 最大伝送ユニット |
| NTP | ネットワーク タイム プロトコル |
| OVF | オープン仮想化フォーマット |
| SMC | Stealthwatch Management Console |
| TB | テラバイト |
| UUID | 汎用一意識別子 |
| VDS | vNetwork 分散型スイッチ |
| VE | バーチャル エディション |
| VLAN | 仮想ローカル エリア ネットワーク |
| VM | 仮想マシン |

# はじめる前に

設定プロセスを開始する前に、このガイドを確認して、プロセスについて、および設定のために計画する必要がある準備、時間、リソースについて理解してください。

## インストール要件

このガイドを使用して Stealthwatch を設定する前に、次のガイドを使用してハードウェアと仮想アプライアンスをインストールしてください。

### ハードウェア

- **ハードウェアのインストール**：この設定を開始する前に、『Stealthwatch x2xx Series Hardware Installation Guide』を使用してアプライアンスハードウェア（物理アプライアンス）をインストールします。
- **データストアを含むハードウェアのインストール**：Stealthwatch を データストア とともに展開する場合は、この設定を開始する前に、『Stealthwatch x2xx Series Hardware (with Data Store) Installation Guide』を使用してアプライアンスハードウェア（物理アプライアンス）をインストールします。また、この設定を開始する前に、『Stealthwatch Data Store Hardware Deployment and Configuration Guide』に従ってアプライアンスを Data Store 用に適切に設定します。
- **仕様**：ハードウェア仕様 [英語] は Cisco.com で入手できます。
- **サポートされているプラットフォーム**：各システムバージョンでサポートされているハードウェア プラットフォームについては、Cisco.com の Hardware and Software Version Support Matrix を参照してください。

### バーチャルエディション（VE）アプライアンス

- **バーチャルエディションのインストール**：この設定を開始する前に、『Stealthwatch Virtual Edition Installation Guide』を使用して仮想アプライアンスをインストールします。
- **Data Store を含むバーチャルエディションのインストール**：Stealthwatch バーチャルエディションを データストア とともに展開する場合は、この設定を開始する前に、『Stealthwatch Virtual Edition (with Data Store) Installation Guide』を使用して仮想アプライアンスをインストールします。また、この設定を開始する前に、『Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide』に従ってアプライアンスを Data Store 用に適切に設定します。

## 設定の詳細

システム設定には、次のようなものがあります。

- **設定の順序**：このガイドの手順に従い、指定された順序を使用してアプライアンスの設定を行ってください。
- **証明書**：アプライアンスは、一意の自己署名アプライアンス アイデンティティ証明書とともにインストールされます。
- **Central Management**：プライマリ SMC/Central Manager からアプライアンスを管理できます。

## ソフトウェアのダウンロード

Cisco Software Central を使用して、仮想アプライアンス（VE）のインストールファイル、パッチ、およびソフトウェア更新ファイルをダウンロードします。https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。

## ライセンス

Stealthwatch のライセンスを取得するには、スマートアカウントを使用して製品インスタンスを登録し、ライセンスを管理し、レポートを実行し、通知を設定します。
https://software.cisco.com で Cisco スマートアカウントにログインするか、管理者にお問い合わせください。

Stealthwatch を評価モードで使用すると、選択された機能を 90 日間使用できます。
Stealthwatch のデフォルト機能を最大限に活用してライセンスと機能をアカウントに追加するには、スマート ソフトウェア ライセンシングの製品インスタンスを登録します。詳細については、「**5.ライセンス**」を参照してください。

> ⚠ 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、フロー収集が停止します。フロー収集を再度開始するには、製品インスタンスを登録します。

## TLS

Stealthwatch には v1.2 が必要です。

## サード パーティ製アプリケーション

Stealthwatch は、アプライアンスへのサード パーティ製アプリケーションのインストールをサポートしていません。

## ブラウザ

Stealthwatch は Chrome、Firefox、および Microsoft Edge の最新バージョンをサポートしています。

## ホスト名

アプライアンスには一意のホスト名が必要です。他のアプライアンスとホスト名が同一のアプライアンスは設定できません。また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。

## ドメイン名

各アプライアンスには完全修飾ドメイン名が必要です。ドメインが空のアプライアンスはインストールできません。

## NTP サーバ

- **設定**：各アプライアンスに少なくとも 1 台の NTP サーバが必要です。
- **問題のある NTP**：130.126.24.53 NTP サーバがサーバのリストに含まれている場合は削除します。このサーバには問題があることが判明しており、シスコのデフォルトの NTP サーバ リストからはすでに除外されています。

## タイム ゾーン

すべての Stealthwatch アプライアンスは協定世界時（UTC）を使用します。

- **仮想ホスト サーバ**：仮想ホスト サーバが正しい時刻に設定されていることを確認します。

> ⚠ 仮想アプライアンスをインストールする仮想ホスト サーバに設定された時刻が正しい時刻に設定されていることを確認します。正しくない場合、アプライアンスを起動できないことがあります。

# 1. Stealthwatch の設定

初めてアプライアンスにログインする場合、アプライアンス設定ツールを使用してアプライアンスを設定し、Stealthwatch Management Console（SMC）で管理できるようにします。

## 準備

設定を開始する前に、手順を確認して、アプライアンスの設定順序、ベストプラクティス、および追加要件を理解してください。

## Stealthwatch とデータストア

データストア を展開する場合は、アプライアンス設定ツールを使用する前に、Stealthwatch アプライアンスの前提条件となる展開および設定要件を確認してください。

- **ハードウェア**：『Stealthwatch Data Store Hardware Deployment and Configuration Guide』に従います。
- **バーチャルエディション**：『Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide』に従います。

## アプライアンス設定ツールの要件

- ファイアウォールと ACL（アクセス制御リスト）でアクセスが許可されていることを確認します。
- アプライアンスのホスト名と次の IP アドレスを収集します。
    - アプライアンス
    - サブネット マスク
    - デフォルト ゲートウェイとブロードキャスト ゲートウェイ
    - NTP サーバと DNS サーバ
    - Central Management の SMC の IP アドレス

## 管理対象

アプライアンス設定ツールの実行の一環として、プライマリ Stealthwatch Management Console（SMC）によって管理されるようにアプライアンスを設定します。

アプライアンスが Stealthwatch Management Console（SMC）によって管理されている場合、Central Management を使用してアプライアンス設定の編集、ソフトウェアの更新、再起動、シャットダウンなどができます。

## SMC フェールオーバー

複数の Stealthwatch Management Console（SMC）がある場合、SMC フェールオーバーペアを設定して、SMC の 1 つを他方のバックアップコンソールとして動作させることができます。

- 各 SMC を設定するには、アプライアンス設定ツールを使用します。
- プライマリにする SMC とセカンダリにする SMC を計画します。
- 両方の SMC を設定し、システム設定を終了した後に、SMC フェールオーバー関係を定義できます。詳細については、「**SMC フェールオーバー関係の定義**」を参照してください。

## ベスト プラクティス

システムを正常に設定するには、このガイドの手順に従っていることを確認します。次のことを確認してください。

- **1 つずつ**：一度に 1 つのアプライアンスを設定します。お使いのクラスタ内で次のアプライアンスの設定を開始する前に、アプライアンスが［アップ（Up）］ステータスであることを確認します。
- **順序**：「アプライアンスの設定順序」に従います。
- **複数の Central Manager**：システムには複数の Central Manager を設定できます。ただし、各アプライアンスは 1 つのプライマリ SMC/Central Manager のみによって管理できます。
- **アクセス**：Central Management にアクセスするための管理者権限が必要です。

## アプライアンスの設定順序

次の順序でアプライアンスを設定し、各アプライアンスの詳細を書き留めます。

| 順序 | アプライアンス | 詳細 |
|---|---|---|
| 1. | プライマリ SMC | プライマリ SMC は、Central Manager です。<br>システム内で次のアプライアンスの設定を開始する前に、SMC が [アップ(Up)] として表示されていることを確認します。<br>Stealthwatch の展開時に Data Store を展開する場合、Data Store との互換性を確保するように SMC を適切に展開および設定する方法の詳細については、『Stealthwatch Data Store Hardware Deployment and Configuration Guide』または『Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide』を参照してください。 |
| 2. | UDP Director<br>(別名 FlowReplicators) | |
| 3. | すべての データノード | データストア Vertica データベースの展開と初期化の詳細については、『Stealthwatch Data Store Hardware Deployment and Configuration Guide』または『Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide』を参照してください。 |
| 4. | Flow Collector 5000<br>シリーズ データベース | エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [アップ(Up)] として表示されていることを確認します。 |
| 5. | Flow Collector 5000<br>シリーズ エンジン | エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [アップ(Up)] として表示されていることを確認します。 |

| | | |
|---|---|---|
| 6. | その他のすべての Flow Collector（NetFlow および sflow） | Stealthwatch の展開時に Data Store を展開する場合、Data Store との互換性を確保するようにフローコレクタを適切に展開および設定する方法の詳細については、『Stealthwatch Data Store Hardware Deployment and Configuration Guide』または『Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide』を参照してください。 |
| 7. | Flow Sensor | Flow Sensor の設定を開始する前に、Flow Collector が［アップ（Up）］として表示されていることを確認します。 |
| 9. | セカンダリ SMC（使用する場合） | セカンダリ SMC の設定を開始する前に、プライマリ SMC が［アップ（Up）］として表示されていることを確認します。<br>セカンダリ SMC は、自身を Central Manager として選択します。すべてのアプライアンスの設定後にフェールオーバーを設定します。詳細については、「**SMC フェールオーバー関係の定義**」を参照してください。 |

システムによっては、ここに示されているアプライアンスの一部が存在しない場合があります。

# 1. ログイン

アプライアンス設定ツールを使用して各アプライアンスを設定するには、次の手順を使用します。

1. ブラウザのアドレス フィールドに、**https://** およびアプライアンスの IP アドレスを入力します。

    - **プライマリ SMC**：最初にプライマリ SMC を設定します。
    - **アップ**：お使いのクラスタ内で次のアプライアンスの設定を開始する前に、アプライアンスが [アップ（Up）] ステータスであることを確認します。
    - **順番**：アプライアンスが正常に通信するように、必ずそれらを順番どおり設定します。

> アプライアンスにアクセスできない場合は、Stealthwatch ハードウェアまたはバーチャルエディションの設置ガイドの「**Configuring your Environment using First Time Setup: Troubleshooting**」の手順を参照してください。

2. 次のクレデンシャルを入力して、ログインします。

    - **ユーザ名**：admin
    - **パスワード**：lan411cope

## 2. アプライアンスの設定

初めてアプライアンスにログインする場合、アプライアンス設定ツールによって各設定手順が示されます。

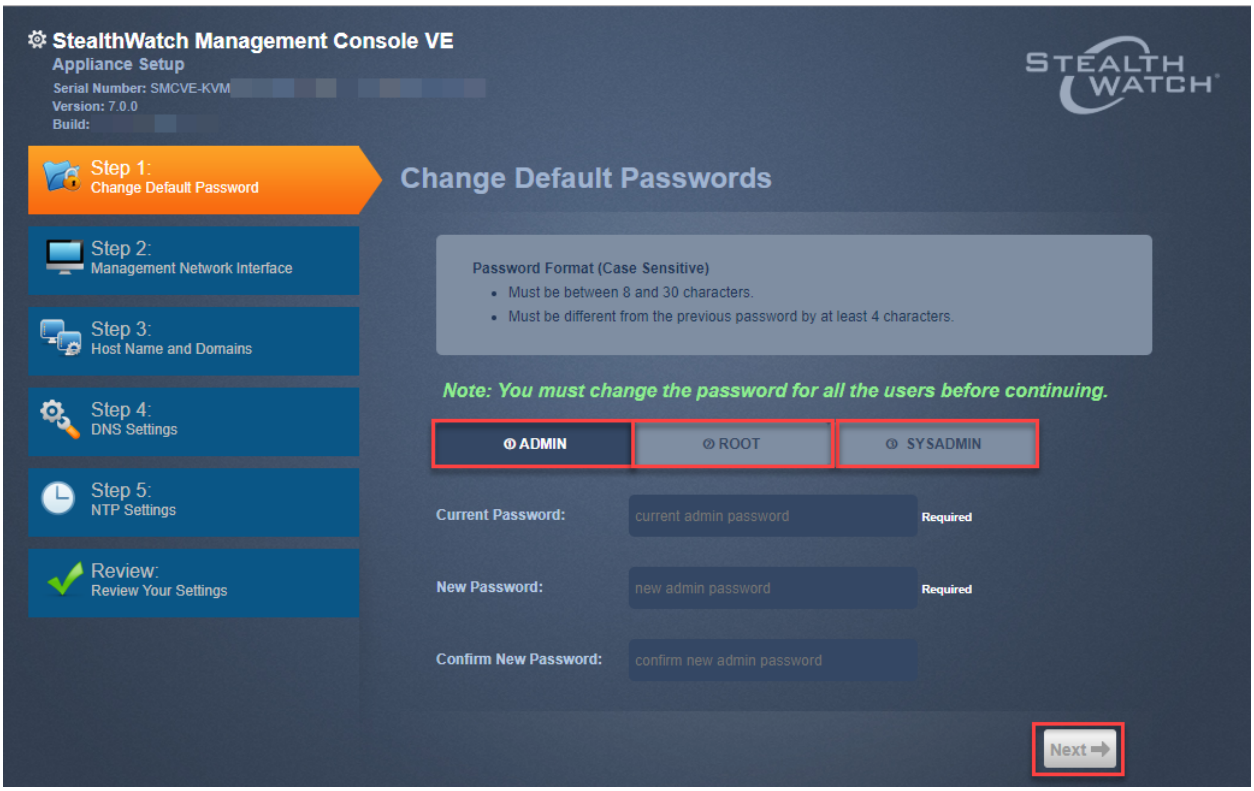
> ⚠ これが初回インストールではない場合、「トラブルシューティング」に移動して、ホスト名、ネットワークドメイン名、IP アドレスなどのアプライアンス ネットワーク設定を変更します。


1. **デフォルト パスワードの変更**：admin、root、および sysadmin の新しいパスワードを入力します。[次へ（Next）] をクリックして各ユーザにスクロールします。

   次の基準を使用します。

   - 長さ：8 ～ 256 文字
   - **変更**：新しいパスワードがデフォルト パスワードと最低 4 文字異なっていることを確認します。

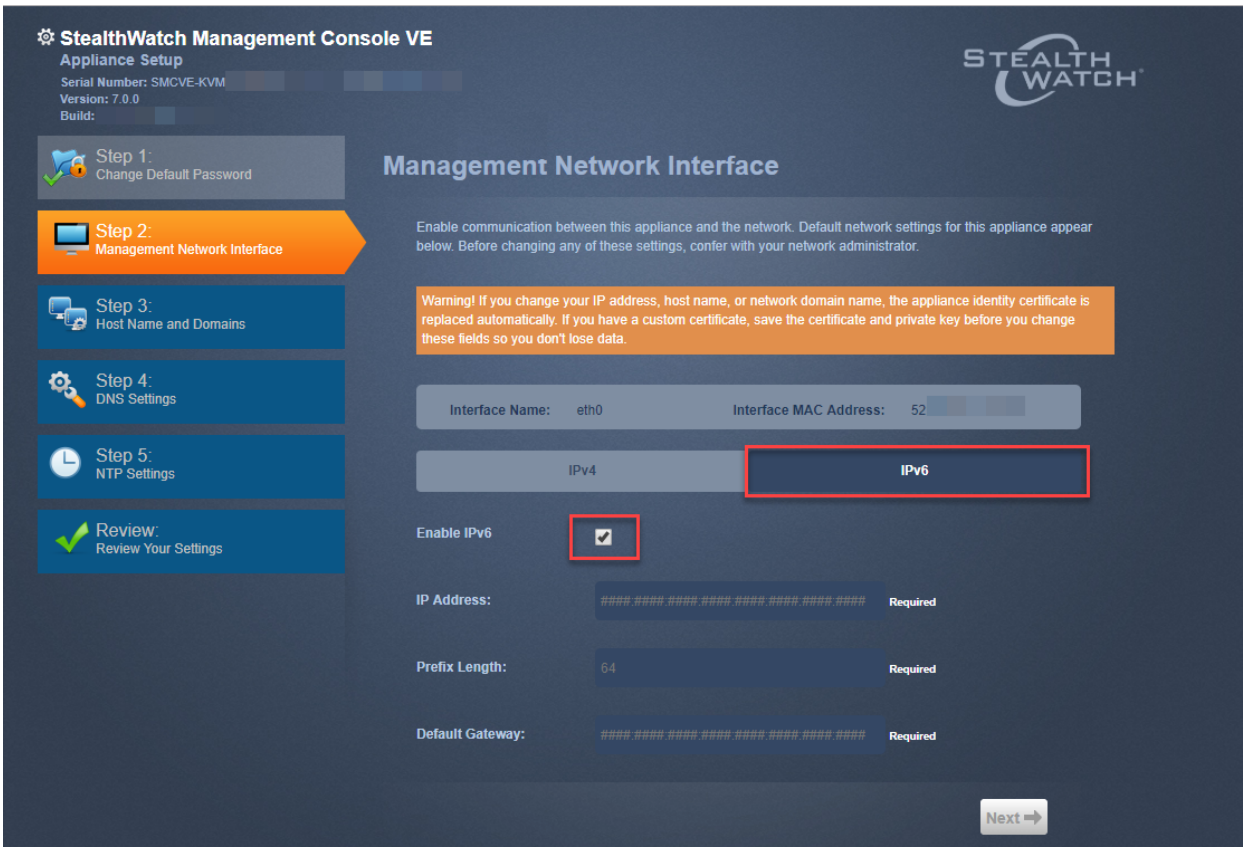
| ユーザ | デフォルト パスワード |
|---|---|
| admin | lan411cope |
| root | lan1cope |
| sysadmin | lan1cope |




> すでにハードウェア設置時にデフォルト パスワードを変更している場合は、[sysadmin] メニューと [root] メニューは使用できません。詳細については、『Stealthwatch x2xx Series Hardware Installation Guide』または『Stealthwatch x2xx Series Hardware (with Data Store) Installation Guide』を参照してください。

2. **管理ネットワーク インターフェイス**:IP アドレスおよびネットワーク インターフェイス フィールドを確認します。デフォルト設定が正しいことを確認します。[次へ (Next)] をクリックします。

   - **変更**:この情報を変更するには、ネットワーク管理者と協議し、トラブルシューティングを参照してください。
   - **IPv6 (オプション)**:IPv6 を有効にするには、[IPv6] をクリックします。[IPv6 の有効化 (Enable IPv6)] チェックボックスをオンにして、フィールドに入力します。




3. **ホスト名とドメイン**：ホスト名とネットワークドメイン名を入力します。[次へ（Next）] をクリックします。

   - **ホスト名**：各アプライアンスには一意のホスト名が必要です。複数のアプライアンスに同じホスト名を割り当てた場合、それらは正常にインストールされません。

     また、各アプライアンスのホスト名がインターネットホストのインターネット標準要件を満たしていることを確認します。

   - **ネットワークドメイン**：各アプライアンスには完全修飾ドメイン名が必要です。
   - **Stealthwatch ドメイン（SMC のみ）**：Stealthwatch アプライアンスの Stealthwatch ドメインを入力します。
   - **IP アドレスの範囲（SMC のみ）**：Stealthwatch ネットワークの IP アドレス範囲を選択します。

4. **DNS 設定**：デフォルトが正しいことを確認するか、ドメイン サーバ IP アドレスを入力します。[次へ（Next）] をクリックします。

   DNS サーバの追加または削除（オプション）

- **追加**：[+] アイコンをクリックします。
- **削除**：チェックボックスをクリックして DNS サーバを選択します。[–] アイコンをクリックします。

5. **NTP の設定**：デフォルトが正しいことを確認するか、[メニュー（Menu）] アイコンをクリックして Network Time Protocol（NTP）サーバを選択します。[次へ（Next）] をクリックします。


- **複数の NTPサーバ**：冗長性と精度を確保するために複数の NTP サーバを設定することをお勧めします。
- **パブリック ソース**：NTP の適切なパブリック ソースとして pool.ntp.org が適しています。

NTP サーバの追加または削除（オプション）

- **追加**：[+] アイコンをクリックします。
- **削除**：チェックボックスをクリックして NTP サーバを選択します。[–] アイコンをクリックします。

6. アプライアンスが SMC の場合は、「3. Stealthwatch Management Console の登録」に進みます。

   アプライアンスが SMC でない場合は、「4. Central Management へのアプライアンスの追加」に進みます。

## 3. Stealthwatch Management Console の登録

1. **設定を確認**:アプライアンスの情報が正確であることを確認します。
2. [適用(Apply)] または [再起動して続行(Restart and Proceed)] をクリックします。

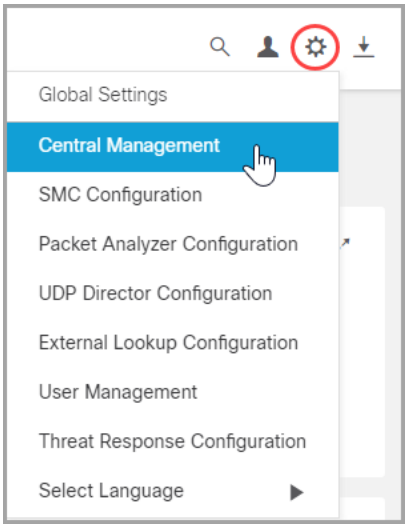
   アプライアンスの再起動中は、画面に表示される指示に従います。

   新しいシステム設定が有効になるまで数分待ちます。ページの更新が必要な場合があります。

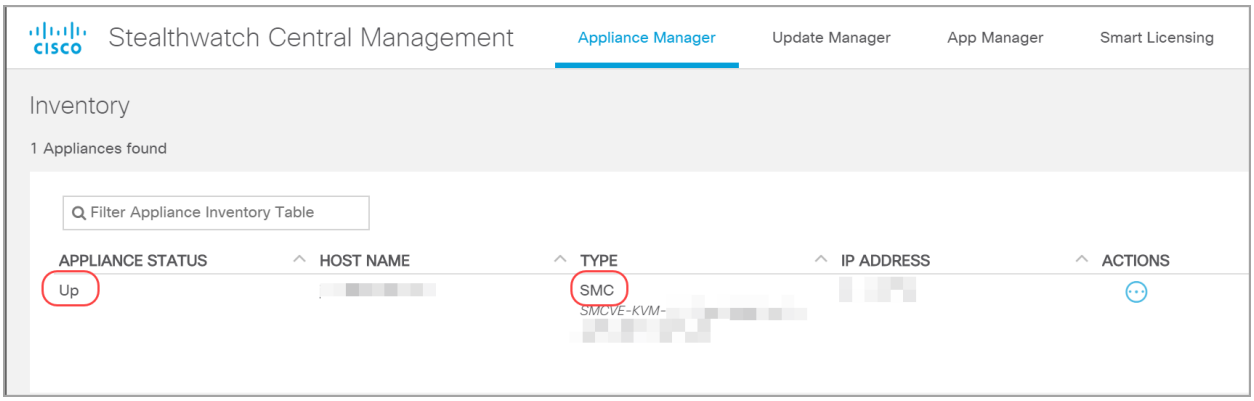
3. Stealthwatch Management Console にログインします。
4. アプライアンス設定ツールが再び開きます。[続行(Continue)] をクリックします。
5. [アプライアンスの登録(Register Your Appliance)] タブで IP アドレスを確認し、[保存(Save)] をクリックします。

   - Stealthwatch Management Console に Central Management がインストールされます。
   - SMC IP アドレスは自動的に検出されるため、変更できません。

6. アプライアンスの設定が完了したら、[ダッシュボードに移動(Go to Dashboard)] をクリックします。
7. [グローバル設定(Global Settings)] アイコンをクリックします。[Central Management] を選択します。




8. インベントリを確認します。SMC アプライアンスのステータスが [アップ(Up)] と表示されていることを確認します。




> クラスタ内の次のアプライアンスの設定を開始する前に、プライマリ SMC と各アプライアンスのステータスが [アップ(Up)] として表示されていることを確認してください(設定の順序と詳細を使用)。

9. システム内の次のアプライアンスを設定するには、「**1. ログイン**」に進み、「**5. アプライアンス ステータスの確認**」までの手順を完了します。

   設定する別のアプライアンスがない場合は、「**2. アプライアンス設定の完了**」に戻ります。

## 4. Central Management へのアプライアンスの追加

アプライアンス設定ツールを使用して、Central Management でのアプライアンスの設定を続けます。一部の手順は、アプライアンスによって異なる場合があります。画面に表示される指示に従って操作します。

1. [Central Management] タブで、プライマリ SMC の IP アドレスを入力します。

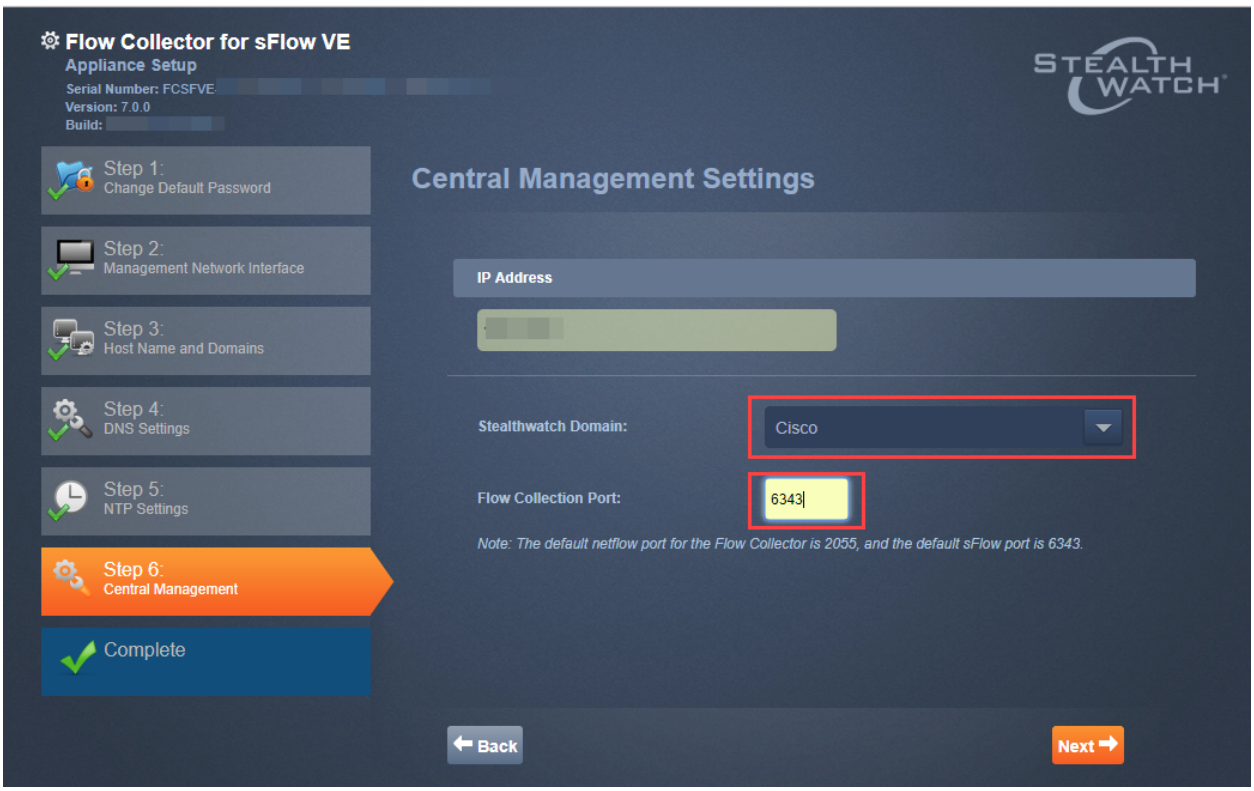
   プライマリ SMC は、Central Manager です。

2. [保存(Save)] をクリックします。
3. 画面に表示される指示に従って、プライマリ SMC アプライアンスのアイデンティティ証明書を信頼します。[はい(Yes)] をクリックして証明書を信頼し、アプライアンスと SMC との通信を許可します。
4. プライマリ SMC のログイン クレデンシャルを入力します。
5. Stealthwatch ドメインを選択します。

   - [フローコレクタ(Flow Collectors)]:フロー収集のポート番号を入力します。

     NetFlow のデフォルト:2055
     sFlow のデフォルト:6343

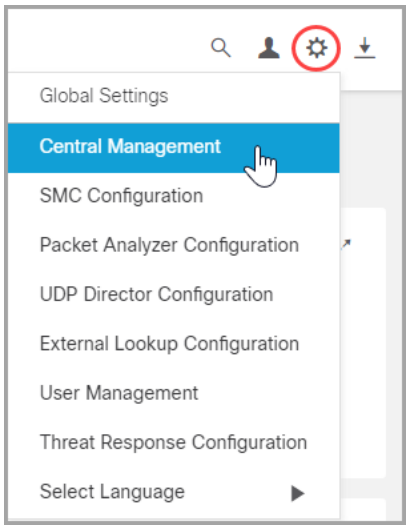
   - [フローセンサー(Flow Sensors)]:フローコレクタを選択します。



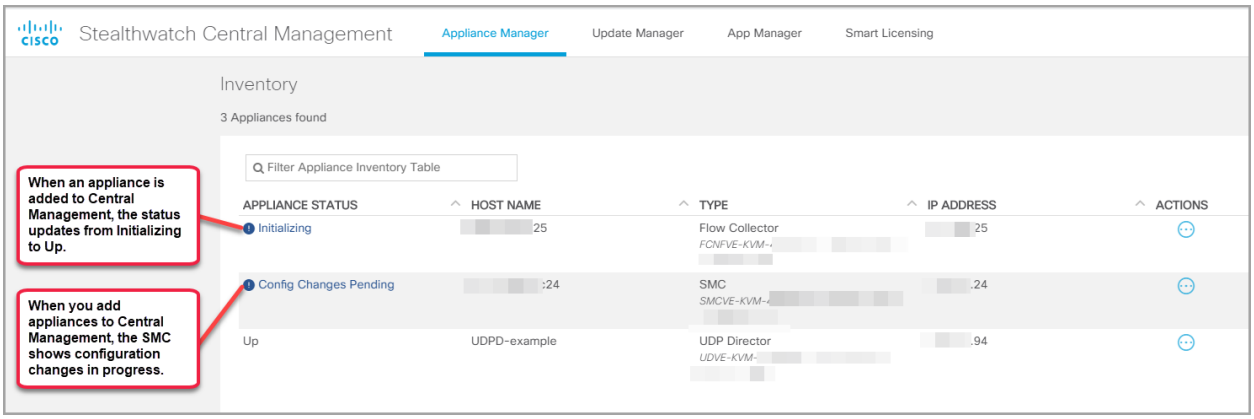

6. [Central Managementに移動（Go to Central Management）] をクリックします。「5. アプライアンス ステータスの確認」までの手順を完了します。

# 5. アプライアンス ステータスの確認

アプライアンス設定ツールでアプライアンスを設定したら、Central Management でアプライアンスのステータスを確認します。




1. アプライアンス設定ツールが Central Management インベントリで開きます。あるいは、次の手順で開くことができます。
   - プライマリ Stealthwatch Management Console にログインします。
   - [グローバル設定（Global Settings）] アイコンをクリックします。
   - [Central Management] を選択します。
2. Appliance Manager インベントリでアプライアンスを確認します。
   - アプライアンスがインベントリに表示されていることを確認します。
   - アプライアンスのステータスが [アップ（Up）] として表示されていることを確認します。




> ⚠ クラスタ内の次のアプライアンスの設定を開始する前に、プライマリ SMC と各アプライアンスのステータスが [アップ（Up）] として表示されていることを確認してください（設定の順序と詳細を使用）。

3. システム内の次のアプライアンスを設定するには、「**1. ログイン**」に進み、「**5. アプライアンス ステータスの確認**」までの手順を完了します。

   設定する別のアプライアンスがない場合は、「**2. アプライアンス設定の完了**」に戻ります。

# 2. アプライアンス設定の完了

各アプライアンスの設定を完了するには、次の手順を使用します。

> お使いの VM ホストの速度によっては、すべてのサービスが起動するまでに 30 分程度かかることがあります。

1. 設定しているアプライアンスのリンクをクリックします。

| アプライアンス | 必須設定 | オプション設定 |
|---|---|---|
| SMC | Stealthwatch の展開時に Data Store を展開しない場合、追加設定は必要ありません。<br>Stealthwatch の展開時に Data Store を展開する場合、Stealthwatch の展開手順の詳細については、『Stealthwatch Data Store Hardware Deployment and Configuration Guide』または『Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide』を参照してください。 | 適用対象外 |
| Flow Collector | Stealthwatch の展開時に Data Store を展開しない場合、追加設定は必要ありません。<br>Stealthwatch を データストア とともに展開する場合、Stealthwatch の展開手順の詳細については、『Stealthwatch Data Store Hardware Deployment and Configuration Guide』または『Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide』を参照してください。 | 適用対象外 |
| データノード | データストア データベースの展開と初期化、Vertica Management Console の設定、および データストア データ保持期間の設定の詳細については、『Stealthwatch Data Store Hardware Deployment and Configuration Guide』または『Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide』を参照してください。 | |
| UDP Director | | ハイアベイラビリティ<br>（ハードウェアでのみ使用可能） |
| Flow Sensor | アプリケーション ID およびペイロード | アプリケーションの識別 |

2. 表内の各アプライアンスの設定および再起動が完了したら、「3. Stealthwatch デスクトップ クライアントのインストール」に進みます。

## UDP Director

UDP Director の設定を完了するには、次の手順を使用します。

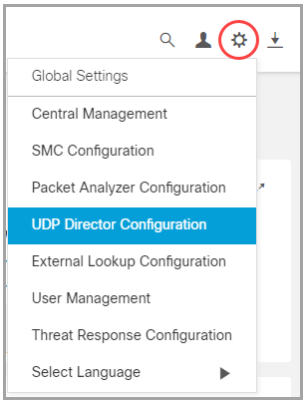
> 高可用性は、UDP Director ハードウェア アプライアンスでのみ使用できます。高可用性は、仮想アプライアンスでは使用できません。

- **転送ルール**：高可用性を設定する場合、少なくとも 1 つの転送ルールを設定します。「転送ルールの設定」を参照してください。
- **高可用性**：複数の UDP Director がある場合、高可用性ペアを設定することができます。高可用性を設定する場合、少なくとも 1 つの転送ルールを設定します（「ハイ アベイラビリティの設定」を参照）。

### 転送ルールの設定

UDP Director から Stealthwatch Management Console（SMC）へのメッセージ送信には SSL が使用されます。

1. SMC にログインします。
2. [グローバル設定（Global Settings）] アイコンをクリックします。[UDP Director設定（UDP Director Configuration）] を選択します。




3. アプライアンスの [アクション（Actions）] メニューをクリックします。[転送ルールの設定（Configure Forwarding Rules）] を選択します。
4. [Add New Rule] をクリックします。
5. **説明（Description）**：ルールを識別するための短い説明を入力します。
6. **送信元 IP アドレス：ポート（Source IP Address:Port）**：UDP Director にデータを送信するデバイスの IP アドレスを入力し、データ送信用のポート番号を入力します。
   - **形式**：[IP アドレス]:[ポート番号] の構文を使用します。

- **範囲**：Classless Inter-Domain Routing（CIDR）表記法を使用してIPアドレスの範囲を入力することができます。
- **すべて**：「All」と入力すれば、このポートで任意の送信元 IP アドレスからデータを受け入れられます。
- **組み合わせ**：「送信元 IP アドレス:ポート」の組み合わせをルールに追加するには、それらを新しい行に追加します。

**例**：

- 10.11.16.38:5322
- 192.168.0.0/16:9000
- All:2055

7. **宛先 IP アドレス（Destination IPAddress）**：UDP Director からデータを受け取るデバイスの IP アドレスを入力します。
8. **宛先ポート番号（Destination Port Number）**：受信するデバイスのポート番号を入力します。
9. [保存（Save）] をクリックします。
10. **オプション**：変更を同期するには、[同期（Sync）] をクリックします。
11. 必要に応じて、転送ルールを追加する手順を繰り返します。
12. 高可用性ペアを設定するには、「**ハイアベイラビリティの設定**」に進みます。

> 高可用性は、UDP Director ハードウェア アプライアンスでのみ使用できます。高可用性は、仮想アプライアンスでは使用できません。

高可用性ペアを設定する必要がない場合は、「**2. アプライアンス設定の完了**」に戻ります。

## ハイアベイラビリティの設定

複数の UDP Director がある場合は、アプライアンス管理インターフェイスを使用して高可用性を設定します。

> 高可用性は、UDP Director ハードウェア アプライアンスでのみ使用できます。高可用性は、仮想アプライアンスでは使用できません。

UDP Director HA（高可用性）では、冗長 UDP Director を設定できます。両方のノードが完全冗長ですが、任意の時点で 1 つのノードだけがオンラインになります。

### プライマリ ノードおよびセカンダリ ノード

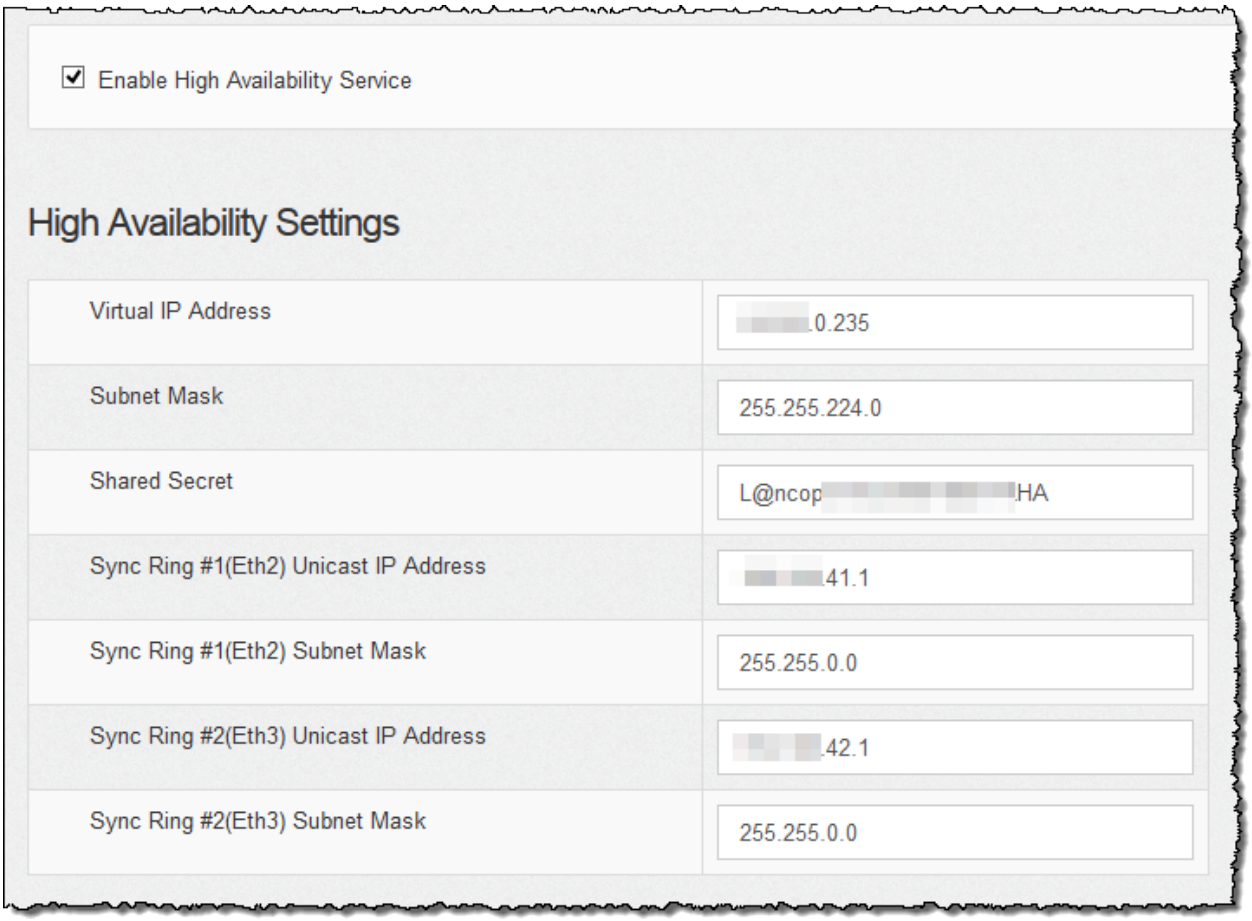
ペアの中でオンライン ノードをプライマリ、オフライン ノードをセカンダリといいます。ペアのプライマリ ノードで障害が発生した場合、セカンダリ ノードがそれを引き継いでプライマリになります。

## 要件

- **転送ルール**：HA システムの UDP Director 用の転送ルールを 1 つ以上設定します。
- **ルール設定ファイルを保存**：UDP Director 用のルールがすでに設定されている場合、UDP Director ルールをエクスポート（ルール設定ファイルを保存）します。次に、このファイルを 2 番目の UDP Director にインポートして、それぞれのルールが一致するようにします。
- **順序**：最初にプライマリ UDP Director を設定した後、セカンダリで設定を繰り返します。
- **新規または設定済み**：どちらも新しい UDP Director である場合、それぞれについてこのガイドの手順に従います。ただし、セカンダリがすでに Stealthwatch システム上のアプライアンスとして設定済みであれば、セカンダリ UDP Director にログインし、この項の説明に従って HA コンポーネントを設定します。

## 1. プライマリ UDP Director HA の設定

1. プライマリ UDP Director アプライアンス管理インターフェイスにログインします。
2. [設定（Configuration）] > [高可用性（High Availability）] をクリックします。
3. 高可用性設定の [高可用性サービスの有効化（Enable High Availability Service）] チェックボックスをオンにします。



4. [仮想IPアドレス(Virtual IP Address)]フィールドに、eth0 インターフェイスと同じサブネット上にある未使用の IP アドレスを入力します。サブネットマスク値を、eth0 インターフェイスで使用されるサブネットマスクの値に設定します。

> 仮想 IP アドレスが両方のノードで同じであることを確認します。

5. [共有シークレット(Shared Secret)]フィールドで、両方の UDP Director 用の文字列を入力します。(これはセキュアな転送用に暗号化されます。)
6. 同期リング 1(Eth2)ユニキャスト IP アドレス用のフィールドに、IP アドレスとサブネット マスクを入力します。(ユニキャスト IP アドレスは単一のネットワーク宛先を識別します。)
7. 同期リング 2(Eth3)ユニキャスト IP アドレス用のフィールドに、IP アドレスとサブネット マスクを入力します。

   各 IP アドレス(eth0、eth02、eth03)は、それぞれ別個のユニキャスト サブネット上である必要があります。

8. 設定を確認したら、[適用(Apply)]をクリックして、設定を適用します。
9. クラスターの 2 番目の UDP Director を設定するには、次のセクションに進みます。

## 2. セカンダリ UDP Director HA の設定

セカンダリ UDP Director を設定するには次の手順を実行します。

1. セカンダリ UDP Director アプライアンス管理インターフェイスにログインします。
2. [設定(Configuration)]>[高可用性(High Availability)]をクリックします。
3. この画面ですべてのパラメータを設定します(最初のアプライアンスで詳細パラメータを変更した場合にはそれも含みます)。その際、次の項目を除くすべてのフィールドで、最初のアプライアンスとまったく同じ値を設定してください。

   - 同期リング 1(Eth2)ユニキャスト IP アドレス:プライマリ上のこのフィールドで設定したものとは異なる IP アドレスを入力しますが、プライマリで指定した同期リング 1 ユニキャスト アドレスと同じサブネットにある必要があります。
   - 同期リング 2(Eth3)ユニキャスト IP アドレス:プライマリ上のこのフィールドで設定したものとは異なる IP アドレスを入力しますが、プライマリで指定した同期リング 2 ユニキャスト アドレスと同じサブネットにある必要があります。

4. [適用(Apply)]をクリックして変更内容を保存し、このアプライアンスのクラスタリング サービスを開始します。
5. プライマリ アプライアンスを指定するには、[昇格(Promote)]ボタンをクリックします。
6. **再起動**:[操作(Operations)]>[アプライアンスの再起動(Restart Appliance)]を選択します。
7. 「**2. アプライアンス設定の完了**」に戻ります。

# Flow Sensor

## 1. アプリケーション ID およびペイロードの設定

フロー センサーを設定するには、アプリケーション ID とペイロードを設定する追加の手順が必要です。

1. FlowSensor アプライアンス管理インターフェイスにログインします。
2. [設定(Configuration)] > [詳細設定(Advanced Settings)] をクリックします。

[詳細設定(Advanced Settings)] ページが開きます。

3. ネットワークに関する適切な設定を次のように選択します。

| 項目 | 説明 |
|---|---|
| [パケットペイロードのエクスポート(Export Packet Payload)] | フロー センサーがコレクタに送るデータの中に、最初の 26 バイトのバイナリ ペイロード データを含めるかどうかを指定できます。 |
| [アプリケーション識別情報のエクスポート(Export Applications Identification)] | コレクタにデータを送る前に、フロー センサーがアプリケーションの識別を試みるかどうかを指定できます。さらに、次の設定が効果を及ぼすには、この設定を有効にする必要があります。<br>Ipv6 を含める(Include IPv6) : フロー センサーで IPv4 と IPv6 の両方のパケットを分析するかどうかを指定できます。この設定を無効にすると、フロー センサーは IPv4 パケットのみを分析します。<br>HTTPS ヘッダー データのエクスポート(Export HTTPS Header Data) : フロー センサーからコレクタに送るデータの中に、HTTPS フローのヘッダー データを含めるかどうかを指定できます。データには SSL 共通名と SSL 組織名が含まれます。この設定を使用するには、フロータイプが IPFIX に設定されている必要があります。最大 256 バイトが可能です。<br>HTTP ヘッダー データのエクスポート(Export HTTP Header Data) : フロー センサーからコレクタに送るデータの中に、HTTP フローのヘッダー データを含めるかどうかを指定できます。この設定を選択した場合、セカンダリ フィールドを使用して、フロー センサーでフロー データに含める HTTP パスの最大長(バイト単位)を指定できます。この設定を使用するには、フロータイプが IPFIX に設定されている必要があります。 |
| [VXLAN カプセル化解除の有効化(Enable VXLAN Decapsulation)] | FlowSensor が Virtual Extensible Local Area Network(VXLAN)カプセル化解除機能を使用するかどうかを指定できます。VXLAN カプセル化解除を使用しない場合、FlowSensor は単純に 2 つの仮想トンネル エンドポイント(VTEP)間のフローとして VXLAN カプセル化トラフィック |

| 項目 | 説明 |
| --- | --- |
| | を検出します。カプセル化解除を使用すると、トンネル化されたトラフィックを分析して、ネットワーク内のトラフィックパターンをより詳細に把握できるため、より豊富なコンテンツを取得できます。<br>FlowSensor は、標準の VXLAN ポート(4789)に元々送信された VXLAN トラフィックだけをカプセル化解除します。 |
| [GENEVEカプセル化解除の有効化(Enable GENEVE Decapsulation)] | フローセンサーがモニタリングポートで受信したトラフィックに対して Generic Network Virtualization Encapsulation(GENEVE)カプセル化解除を使用するかどうかを指定できます。 |
| [ERSPANカプセル化解除の有効化(Enable ERSPAN Decapsulation)] | フローセンサーでカプセル化リモート スイッチ ポート アナライザ(ERSPAN)のカプセル化解除機能を使用することで、パケット内の ERSPAN ヘッダーを検出してヘッダーのカプセル化を解除し、カプセル化されていたパケットの中身を処理するかどうかを指定できます。<br>フローセンサーの ERSPAN トンネルを終了できるようにするには、モニタリング インターフェイスに IP アドレスを割り当てる必要があります。<br>FS 4210 の ERSPAN のカプセル化解除はサポートされていません。 |
| [X-Forwarded-For 処理の有効化(Enable X-Forwarded-For Processing)] | FlowSensor が X-Forwarded-For(XFF)処理を使用して、HTTP プロキシまたはロードバランサを介して Web サーバに接続しているクライアントの発信元 IP アドレスを識別するかどうかを指定できます。<br>ETA と X-Forwarded-For 処理を一緒に設定することはできません。 |
| [ETA 処理の有効化(Enable ETA Processing)] | FlowSensor が ETA 処理を使用して、IDP フィールドおよび SPLT フィールドを生成して SMC に送信するかどうかを指定できます。<br>ETA を有効にすると、特に v9 使用時の NetFlow 帯域幅の使用量が増加します。フローエクスポート形式には IPFIX を使用することをお勧めします。<br>ETA と X-Forwarded-For 処理を一緒に設定することはできません。<br>ETA を Dell または PowerEdge FlowSensor モデルで有効にすることはできません。 |

| 項目 | 説明 |
| --- | --- |
| [ロード バランシングの有効化(Enable Load Balancing)] | Flow Sensor 4000 シリーズが複数のフローコレクタにフローデータを配信できるかどうかを指定できます。<br>フローセンサーからのフローデータが 1 つのフローコレクタのキャパシティを超える場合には、このオプションを使用します。 |
| [インターフェイス選択のモニタリング(Monitoring Interface Selection)] | Flow Sensor 4240 が 2 x 40G インターフェイスを使用するか 4 x 10G (SFP)インターフェイスを使用するかを指定できます。<br>この設定が正常に機能するには、複数のフローコレクタを使用してロードバランシングを有効にしておく必要があります。詳細については、『Flow Sensor and Load Balancer Integration Guide』を参照してください。<br>このオプションは、フローセンサー 4240 でのみ使用できます。<br>デフォルトの設定は 2 x 40G です。 |
| [キャッシュモード(Cache Mode)] | 次のいずれかの設定を選択できます。<br><br>すべての監視ポートに単一の共有キャッシュを使用(Use single, shared, cache for all monitoring ports):<br>• 非対称ルーティングが存在する場合に使用します。<br>• アプリケーションと遅延計算に 1 つの状態テーブル。<br>• より少ないメモリを使用。<br>• 全体的により低い pps 処理率。<br>• 結果として複数のインターフェイス全体で 1 つの NetFlow イベントが作成されます。<br>• フロー センサーにポートが 2 つだけ存在し、TAP で接続されている場合にのみ、これを使用します。<br><br>監視ポートごとに独立したキャッシュを使用(Use independent caches for each monitoring port):<br>• フロー センサー インターフェイスごとにパケットの重複排除が行われます。<br>• より多くのメモリを使用。<br>• 全体的により高い pps 処理率。<br>• 各インターフェイスは独自の遅延とアプリケーション データベースを維持します。<br>• 結果として、特定のパケットを認識するインターフェイスごとに固有の NetFlow レコードが生成されます。 |

4. [適用(Apply)]をクリックして設定を保存します。

## 2. アプリケーションを識別するための Flow Sensor の設定（オプション）

フロー センサーでアプリケーションを識別する場合、次のように設定します。

1. FlowSensor アプライアンス管理インターフェイスにログインします。
2. [設定（Configuration）] > [詳細設定（Advanced Settings）] をクリックします。
3. [アプリケーションIDのエクスポート（Export Application Identification）] チェックボックスをオンにします。デフォルトでは、このオプションは選択されていません。
4. 複数の監視 NIC がある場合、[キャッシュ モード（Cache Mode）] セクションで次のいずれかのオプションを選択します。

   - **すべてのモニタリング ポートに単一の共有キャッシュを使用する（Use single, shared, cache for all monitoring ports）**：通常、TAP 方式でフローをモニタリングするシステムに対して使用します。

   - **モニタリング ポートごとに個別のキャッシュを使用する（Use independent caches for each monitoring port）**：通常、SPAN 方式でフローをモニタリングするシステムの場合、およびパフォーマンスを強化する必要がある場合に使用します。

## 3. アプライアンスの再起動

1. [操作（Operations）] > [アプライアンスの再起動（Restart Appliance）] を選択します。
2. 「**2. アプライアンス設定の完了**」に戻ります。

# 3. Stealthwatch デスクトップ クライアントのインストール

> Data Store を含む Stealthwatch が展開されている場合は、Stealthwatch デスクトップクライアントは使用しません。

以下の手順で、Windows または macOS を使用して Stealthwatch デスクトップ クライアントをインストールします。次の点に注意してください。

- Stealthwatch デスクトップ クライアントのさまざまなバージョンをローカルにインストールすることができます。
- Stealthwatch デスクトップ クライアントの複数のバージョンにアクセスするには、各 SMC において異なる実行ファイルが必要になります。
- プライマリ SMC とセカンダリ SMC の両方を使用している場合は、一方の SMC をログオフして、その後もう一方の SMC にログインする必要があります。
- Stealthwatch デスクトップ クライアントの複数のバージョンを同時に開くことができます。
- Stealthwatch の最新のバージョンに更新する場合は、Stealthwatch デスクトップ クライアントの新しいバージョンをインストールする必要があります。
- データストア を展開する場合は、Stealthwatch Web アプリケーションを使用して Stealthwatch インストールをモニタおよび設定します。Stealthwatch デスクトップクライアントは データストア と互換性がありません。

## Windows を使用したデスクトップ クライアントのインストール

> - Stealthwatch デスクトップ クライアントをインストール可能な権限を持っている必要があります。
> - Stealthwatch デスクトップ クライアントには、64 ビットのオペレーティング システムが必要です。32 ビットのオペレーティング システムまたは Linux では実行できません。

1. SMC にログインします。
2. [ダウンロード(Download)] アイコンをクリックします。

3. .exe ファイルをクリックして、インストール プロセスを開始します。
4. ウィザードの手順を実行して Stealthwatch デスクトップ クライアントをインストールします。
5. デスクトップ上の Stealthwatch デスクトップ クライアント アイコン をクリックします。
6. SMC ユーザ名およびパスワードを入力します。
7. SMC サーバ名または IP アドレス(IPv4 または IPv6)を入力します。

8. 画面に表示される指示に従ってデスクトップ クライアントを開き、アプライアンスのアイデンティティ証明書を信頼します。

## メモリサイズの変更

Stealthwatch デスクトップ クライアント インターフェイスを実行するために、クライアント コンピュータで割り当てるランダム アクセス メモリ(RAM)の量を変更できます。開いている多数のドキュメントや大量のデータ セット(100,000 個を超えるレコードが含まれたフロー クエリなど)を扱う場合は、割り当てるメモリを増やすことを検討してください。

1. Windows Explorer で、ホームディレクトリに移動します。
2. これらのフォルダを次の順に開きます。AppData > ローミング > Stealthwatch。

   フォルダが非表示の場合は、「Stealthwatch」を検索する必要がある場合があります。

3. Stealthwatch ディレクトリで、目的の Stealthwatch バージョンが含まれているフォルダを開きます。
4. 適切な編集アプリケーションを使用して **application.vmoptions** ファイルを開き、編集を開始します(このファイルは、Stealthwatch デスクトップ クライアントを最初に開いた後に作成されます)。

   **最小メモリサイズ(Xms)**:512 MB 以上を割り当てることをお勧めします。この番号は、ファイルの 3 番目の行に表示されます。

   コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、どの数字が最小メモリ サイズを表しているかを確認してください。

   ```
   # Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
   ```

   **最大メモリサイズ(Xmx)**:最大メモリサイズには、最大でコンピュータの RAM の半分のサイズを割り当てることができます。この番号は、ファイルの 4 番目の行に表示されます。

   コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、最大メモリサイズを表している数字を確認してください。

   ```
   # Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
   ```

   **すべての番号を使用します。**たとえば、Xmx0.5m ではなく、-xmx512m を入力します。

- Stealthwatch デスクトップ クライアントが頻繁に「ハング」する場合は、メモリサイズを大きくします。
- Java に関連するエラー メッセージが表示される場合は、これよりも小さなメモリ割り当て量を選択してください。

## macOS を使用したデスクトップ クライアントのインストール

- Stealthwatch デスクトップ クライアントをインストール可能な権限を持っている必要があります。
- Stealthwatch デスクトップ クライアントには、64 ビットのオペレーティング システムが必要です。32 ビットのオペレーティング システムまたは Linux では実行できません。

1. SMC にログインします。
2. [ダウンロード(Download)] アイコンをクリックします。

3. .dmg ファイルをクリックして、インストール プロセスを開始します。

   アイコンとフォルダは、以下に示すようにモニタに表示されます。

4. Stealthwatch デスクトップ クライアントのアイコンを ( ) アプリケーションのフォルダにドラッグします。

   アイコンは、スタート パッドに追加されます。

5. デスクトップ上の Stealthwatch デスクトップ クライアント アイコン をクリックします。
6. SMC ユーザ名およびパスワードを入力します。
7. SMC サーバ名または IP アドレス(IPv4 または IPv6)を入力します。
8. 画面に表示される指示に従ってデスクトップ クライアントを開き、アプライアンスのアイデンティティ証明書を信頼します。

## メモリサイズの変更

Stealthwatch デスクトップ クライアント インターフェイスを実行するために、クライアント コンピュータで割り当てるランダム アクセス メモリ（RAM）の量を変更できます。開いている多数のドキュメントや大量のデータ セット（100,000 個を超えるレコードが含まれたフロー クエリなど）を扱う場合は、割り当てるメモリを増やすことを検討してください。

1. 検索で、ホーム ディレクトリに移動します。
2. Stealthwatch フォルダを開きます。
3. Stealthwatch ディレクトリで、目的の Stealthwatch バージョンが含まれているフォルダを開きます。
4. 適切な編集アプリケーションを使用して application.vmoptions ファイルを開き、編集を開始します（このファイルは、Stealthwatch デスクトップ クライアントを最初に開いた後に作成されます）。

   **最小メモリサイズ（Xms）**：512 MB 以上を割り当てることをお勧めします。この番号は、ファイルの 3 番目の行に表示されます。

   コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、どの数字が最小メモリ サイズを表しているかを確認してください。

   ```
   # Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
   ```

   **最大メモリサイズ（Xmx）**：最大メモリサイズには、最大でコンピュータの RAM の半分のサイズを割り当てることができます。この番号は、ファイルの 4 番目の行に表示されます。

   コンテンツを連続した 1 行で表示するエディタの場合は、下の画像で強調表示されている数字を参照して、最大メモリサイズを表している数字を確認してください。

   ```
   # Enter one VM parameter per line# Use -Xms to specify the initial Java heap size and Use -Xmx to specify the maximum heap size-Xms512m-Xmx2048m
   ```

   **すべての番号を使用します。**たとえば、Xmx0.5m ではなく、-xmx512m を入力します。

- Stealthwatch デスクトップ クライアントが頻繁に「ハング」する場合は、メモリサイズを大きくします。
- Java に関連するエラー メッセージが表示される場合は、これよりも小さなメモリ割り当て量を選択してください。

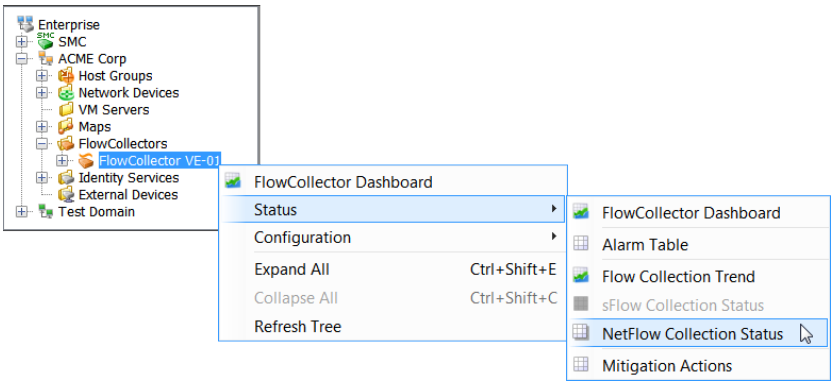
# 4. 通信の確認

次の手順を使用して、Stealthwatch Management Console が NetFlow データを受信していることを確認します。

> Stealthwatch を データストア とともに展開した場合、通信を確認するには『Stealthwatch Data Store Hardware Deployment and Configuration Guide』または『Stealthwatch Data Store Virtual Edition Deployment and Configuration Guide』を参照してください。

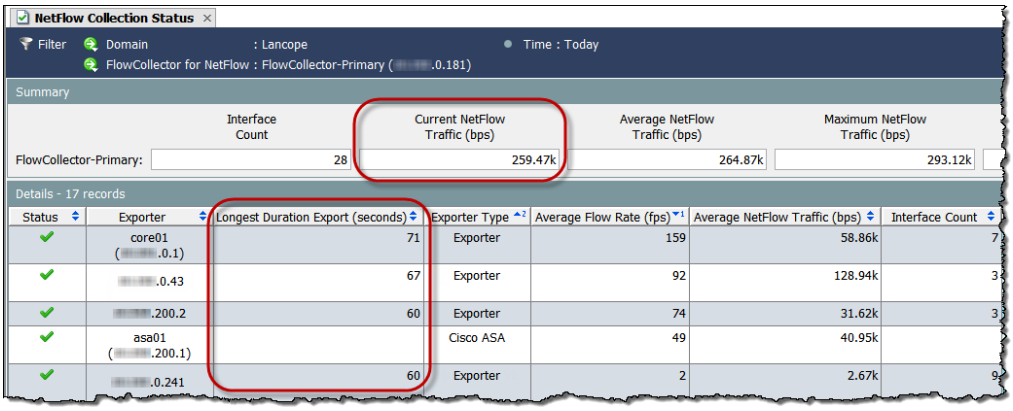
## NetFlow データ収集の確認

1. Stealthwatch デスクトップ クライアントのエンタープライズ ツリーで、フロー コレクタを右クリックします。[ステータス(Status)] > [NetFlowコレクションステータス(NetFlow Collection Status)] の順に選択します。




2. [NetFlowコレクションステータス(NetFlow Collection Status)] ページで、ドキュメントの上部にある [現在のNetFlowトラフィック(Current NetFlow Traffic)] フィールドを参照します。この統計情報は検出された NetFlow トラフィックの量を示します。

   - トラフィックが表示されている場合は、次の手順に進みます。
   - トラフィックが表示されていない場合は、エクスポータおよびルータの設定を確認します。詳細については、SMC クライアントのオンライン ヘルプを参照してください。次の手順に進みます。




3. [最も長い継続時間のエクスポート(Longest Duration Export)] 列を参照してください。

   **列の追加**:この列をダッシュボードに追加するには、列ヘッダーを右クリックし、メニューから [最も長い継続時間のエクスポート(Longest Duration Export)] を選択します。

4. 各エクスポータの値は 100 よりも下ですか。

   - 「はい」の場合、キャッシュのエクスポートタイマーは正常です。
   - 「いいえ」の場合、高い値はキャッシュのエクスポートタイマーが正しくないことを示し、誤ったアラームが発生する可能性があります。エクスポータおよびルータの設定を確認します。詳細については、SMC クライアントのオンライン ヘルプを参照してください。

5. Congratulations! Stealthwatch のシステム設定が完了しました。
6. **次の手順**:「5.ライセンス」を確認し、評価期間が終了する前に Cisco スマートアカウントに製品インスタンスを登録します。

> ⚠ 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、フロー収集が停止します。フロー収集を再度開始するには、製品インスタンスを登録します。

7. Stealthwatch に別のサービスと機能を追加するには、次のリソースを参照してください。

   - SMC フェールオーバー関係の定義
   - 脅威インテリジェンスフィードの有効化
   - SAML SSO の設定

> ℹ Cisco.com を参照して Stealthwatch のガイドを確認し、Cisco Threat Response、Cisco Identity Services(ISE)、TACACS+ などの追加機能を設定します。

**Stealthwatch の使用を開始するには、**このガイドの次の項を参照してください。

- **はじめに**:「Stealthwatch の概要」の項には、環境の管理、動作の調査、脅威への対応などに関する詳細が記載されています。
- **Central Management**:アプライアンス管理と設定変更の詳細については、このガイドの「Central Management」の項を参照してください。
- **トラブルシューティング**:このガイドの「トラブルシューティング」の項を参照してください。

# 5.ライセンス

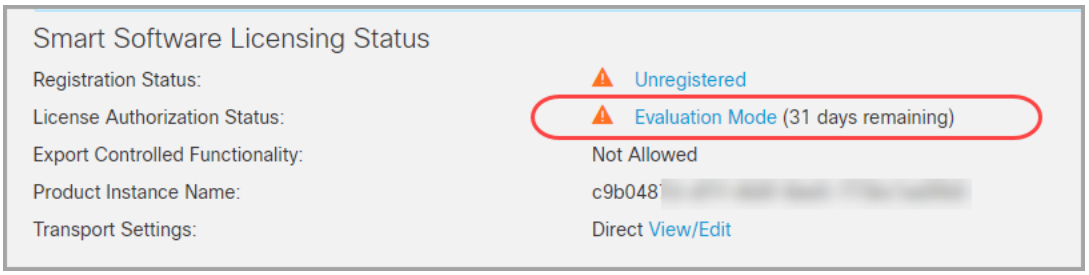
シスコ スマート ソフトウェア ライセンシングを使用して、Stealthwatch のアプライアンスおよび機能をライセンシングします。詳細については、cisco.com のスマートライセンシングを参照してください。

- **オンライン**:スマートライセンシング および Stealthwatch をオンラインで使用するには、『Stealthwatch Smart Software Licensing Guide』を参照してください。この設定にはインターネットアクセスが必要です。
- **オフライン**:クローズド/エアギャップネットワークのライセンスオプションの説明については、Cisco Stealthwatch サポートに連絡してください。
- **Cisco スマートアカウント**:Cisco スマートアカウントを設定するには、https://software.cisco.com で登録するか、管理者にお問い合わせください。

## 評価モード

Stealthwatch を評価モードで使用すると、選択された機能を 90 日間使用できます。Stealthwatch のデフォルト機能を最大限に活用してライセンスと機能をアカウントに追加するには、スマート ソフトウェア ライセンシングの製品インスタンスを登録します。

> ⚠ 90 日間の評価期間が終了する前に製品インスタンスを登録してください。評価期間が終了すると、フロー収集が停止します。フロー収集を再度開始するには、製品インスタンスを登録します。




- **管理者ユーザ**:Stealthwatch Management Console でスマートライセンシングのステータスと使用状況の詳細を確認するには、管理者ユーザとしてログインします。
- **残り日数**:評価モードの残り日数を確認するには、管理者ユーザとして Stealthwatch Management Console にログインします。[Central Management] > [スマートライセンシング(Smart Licensing)] の順に移動します。[ライセンス承認ステータス(License Authorization Status)] を確認します。
- **製品インスタンス**:製品インスタンスはお客様の Stealthwatch の製品インスタンスに使用する識別子であり、Stealthwatch管理コンソールと管理アプライアンスが含まれます。

# SMC フェールオーバー関係の定義

フェールオーバー設定を使用すると、2 つの Stealthwatch 管理コンソール（SMC）間にフェールオーバーペアを確立し、一方の SMC をもう一方のバックアップコンソールとして機能させることができます。

正しく設定して運用するには、『Stealthwatch Failover Configuration Guide』で要件を確認し、その手順に従ってください。

> ⚠ プライマリ SMC がオフラインになっても、SMC のロールは自動的に交換されない点に注意してください。『Stealthwatch フェールオーバー コンフィギュレーション ガイド』に記載されている順序で SMC のロールを変更してください。

## フェールオーバーの設定

SMC をフェールオーバーペアとして設定するには、『Stealthwatch Failover Configuration Guide』の手順に従います。

このガイドには、正常に設定するために重要な、次を含む詳細事項が記載されています。

- **証明書**：アプライアンス間に信頼を設定してアプライアンス同士が通信できるようにするために、必要なアプライアンスの信頼ストアに正しい証明書を保存していることを確認します。
- **バックアップファイル**：フェールオーバー設定を開始する前に、アプライアンスをバックアップします。
- **設定の順序**：セカンダリ SMC をフェールオーバー用に設定してからプライマリ SMC を設定します。
- **ロールの変更**：プライマリ SMC がオフラインになった場合は、このガイドに示されている順序で SMC のロールを変更してください。順序は重要で、ロールは自動的に交換されません。
- **トラブルシューティング**：解決策については、『Stealthwatch フェールオーバー コンフィギュレーション ガイド』を参照してください。

> ⚠ 正しく設定して運用するには、『Stealthwatch フェールオーバー コンフィギュレーション ガイド』の手順に従ってください。

## プライマリおよびセカンダリのロール

設定の一部として、プライマリ SMC とセカンダリ SMC を割り当てます。設定を保存すると、次の処理が行われます。

- **プライマリ SMC**：プライマリ SMC はそのドメイン設定、ユーザ設定、およびポリシーをセカンダリ SMC にプッシュします。プライマリ SMC では、アプライアンスの管理、アプライアンス設定の変更、パスワードの変更、アラームの定義、ポリシーの適用などを行います。
- **セカンダリ SMC**：セカンダリ SMC は自身の設定を削除します。したがってプライマリ SMC の構成および設定と同期できます。また、セカンダリ SMC がすべてのユーザに対して読み取り専用に変更されます。したがって、セカンダリ SMC のセクションにアクセスすることもセカンダリ SMC からファイルを取得することもできなくなります。

# 脅威インテリジェンスフィードの有効化

脅威インテリジェンスフィードは、ネットワークに対する脅威に関するグローバル脅威インテリジェンスフィードからのデータを提供します。フィードは頻繁に更新され、悪意のあるアクティビティに使用されたことがわかっている IP アドレス、ポート番号、プロトコル、ホスト名、および URL が含まれています。フィードには、コマンドアンド コントロール サーバ、bogon、および Tor の各ホストグループが含まれています。

## ライセンス

脅威インテリジェンスフィードのライセンスを Cisco スマートアカウントに追加します。手順については、Stealthwatch スマート ソフトウェア ライセンシング ガイド [英語] を参照してください。

## 有効

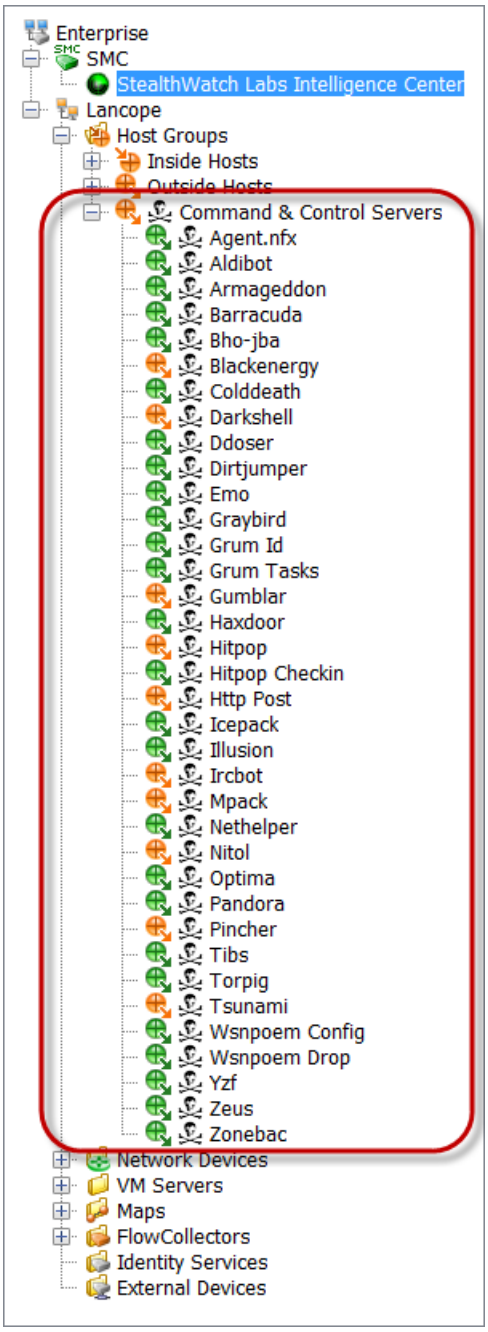
Central Management でフィードを有効にするには、オンラインヘルプの手順に従います。手順の一部として DNS サーバとファイアウォールを設定することに注意してください。

1. プライマリ Stealthwatch Management Console にログインします。
2. [グローバル設定 (Global Settings)] アイコンをクリックします。
3. [Central Management] を選択します。
4. [ユーザ (User)] アイコンをクリックします。[Stealthwatch オンライン ヘルプ (Stealthwatch Online Help)] を選択します。
5. [アプライアンス設定 (Appliance Configuration)] > [脅威インテリジェンスフィード (Threat Intelligence Feed)] を選択します。

## アラームとセキュリティイベントの確認

脅威インテリジェンスフィードが有効になっている場合、Stealthwatch Labs Intelligence Center のアイコンが Stealthwatch デスクトップクライアントの企業ツリーにアラームステータスとともに表示され、脅威は各ホストグループのブランチに表示されます。詳細については、Stealthwatch デスクトップ クライアント ユーザ ガイド [英語] またはオンラインヘルプを参照してください。

> **オンラインヘルプ**:オンラインヘルプにアクセスするには、[Stealthwatchラボインテリジェンスセンター (Stealthwatch Labs Intelligence Center)] ブランチを右クリックし、[設定 (Configuration)] > [SLIC脅威フィード設定 (SLIC Threat Feed Configuration)] の順に選択します。[ヘルプ (Help)] をクリックします。



# SAML SSO の設定

以下の手順に従って、セキュリティアサーション マークアップ言語シングル サインオン（SAML SSO）を設定します。SSO は、ユーザが 1 組のクレデンシャルで複数のアプリケーションにアクセスすることを可能にする認証プロセスです。

## サポートの詳細

次の設定がサポートされているかどうかに注意してください。

| サポート対象 | サポート対象外 |
|---|---|
| SAML/SSO 用の Microsoft Active Directory ファイルサーバ（ADFS） | Stealthwatch デスクトップ クライアント |
| Microsoft ADFS のオンプレミスソリューション | Microsoft ADFS のクラウドサービス |
| | 統合 Windows 認証（IWA） |
| | 追加のプロキシ |
| | 外部サービス（External Services） |

## 1. 設定の準備

SSO を設定するには次の情報が必要です。

| 要件 | 詳細 |
|---|---|
| アイデンティティ プロバイダーの URL | この URL には完全修飾ドメイン名または IPv4 アドレスを使用する必要があります。 |
| アイデンティティ プロバイダーの証明書 | IDP の URL が「HTTPS」で始まる場合は、CA 証明書をダウンロードしてください。 |

## 2. 信頼ストアへの証明書のアップロード

アイデンティティ サービス プロバイダー（IDP）の URL が「HTTPS」で始まる場合は、**ルート CA 証明書**を SMC 信頼ストアに追加します。

> IDP の URL が「HTTPS」で始まらない場合は、この手順をスキップして次の項「**3. サービス プロバイダーの設定**」に進むことができます。

以下の手順に従って、ルート CA 証明書を SMC 信頼ストアに追加します。

1. [Central Management] の [Appliance Manager] ページで、SMC の [アクション（Actions）] メニューをクリックします。
2. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。

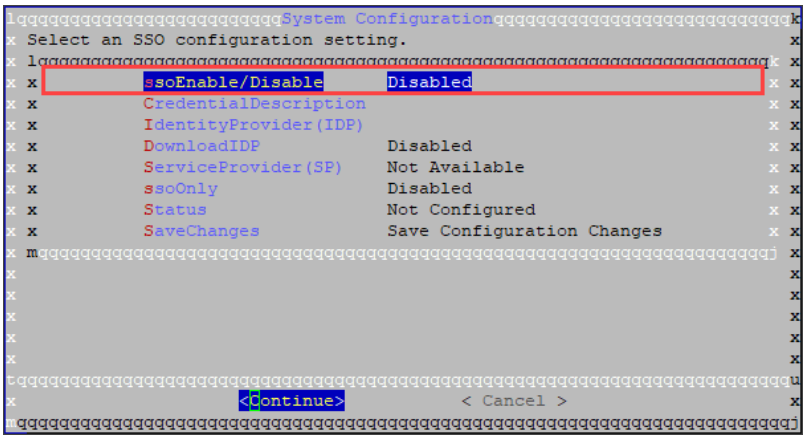
3. [Appliance Manager] > [全般(General)] タブで、[信頼ストア(Trust Store)] セクションを見つけます。
4. [新規追加(Add New)] をクリックします。
5. [フレンドリ名(Friendly Name)] フィールドに、証明書の名前を入力します。
6. [ファイルの選択(Choose File)] をクリックします。新しい証明書を選択します。
7. [証明書の追加(Add Certificate)] をクリックします。[信頼ストア(Trust Store)] リストに新しい証明書が表示されることを確認します。
8. [設定の適用(Apply settings)] をクリックします。画面に表示される指示に従って操作します。
9. **Up**:[Appliance Manager] ページで、SMC が設定変更を完了し、アプライアンスのステータスが **Up** に戻ることを確認します。

> ⚠ 設定の変更が保留中の間は、アプライアンスを再起動させないでください。

10. セカンダリ SMC がある場合は、この手順を繰り返して、ルート CA 証明書をセカンダリ SMC 信頼ストアに追加します。
11. ルート CA 証明書を SMC 信頼ストアに追加した場合は、次のセクションに進みます。

## 3. サービス プロバイダーの設定

1. SMC コンソールに root としてログインします。
2. `SystemConfig` と入力します。Enter を押します。
3. [詳細設定(Advanced)] を選択します。
4. [SSO] を選択します。
5. [SSO 有効/無効(ssoEnable/Disable)] が [無効(Disabled)] と表示されていることを確認します。



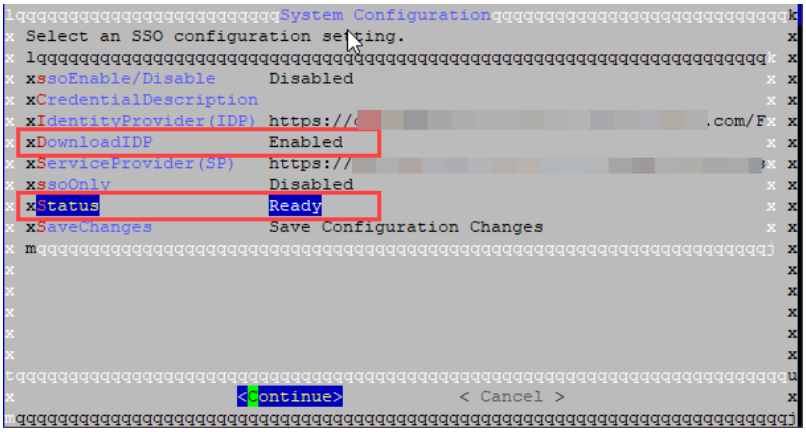

6. [アイデンティティプロバイダー(IDP)(IdentityProvider(IDP))] を選択します。[続行(Continue)] をクリックします。
7. アイデンティティプロバイダーの設定ファイルをダウンロードできる URL を入力します。

**Requirements（要件）**：完全修飾ドメイン名または IPv4 アドレスを入力します。

8. [IDP のダウンロード（DownloadIDP）] を選択します。画面に表示される指示に従って、有効にします。
9. [変更の保存（SaveChanges）] を選択します。[続行（Continue）] をクリックします。

   画面の指示に従って、IDP 設定ファイルをダウンロードします。

10. [SSO] を選択します。
11. [サービスプロバイダー（SP）（ServiceProvider(SP)）] を確認します。URL をコピーしてください。これは、アイデンティティプロバイダーの設定に使用します。
12. [ステータス（Status）] を確認します。これが [準備（Ready）] と表示されていることを確認してください。




## 4. SSO の有効化

1. [SSO 有効/無効（ssoEnable/Disable）] を選択します。
2. 画面に表示される指示に従って、SSO を有効にします。
3. [クレデンシャルの説明（CredentialDescription）] を選択します。[続行（Continue）] をクリックします。
4. ユーザがログインするために必要な SSO サービスクレデンシャルの説明を入力します。
5. [OK] をクリックします。
6. [IDP のダウンロード（DownloadIDP）] を選択します。新しい SSO 設定を保存する必要があるまで [IDP のダウンロード（DownloadIDP）] を無効にします。

   - [続行（Continue）] をクリックします。
   - 画面に表示される指示に従って、[IDP のダウンロード（DownloadIDP）] を無効にします。

7. [変更の保存（SaveChanges）] を選択します。[続行（Continue）] をクリックします。
8. システム設定を終了します。

## 5. アイデンティティ プロバイダーの設定

1. ブラウザのアドレス フィールドにサービス プロバイダーの URL を入力します。
2. サービス プロバイダーのメタ データファイル sp.xml をダウンロードします。
3. sp.xml を使用してアイデンティティ プロバイダーを設定します。
4. 発信クレーム タイプにユーザの電子メール アドレスが含まれていることを確認します。

   - **例**：属性ストアが Active Directory の場合、発信クレーム タイプを LDAP 属性タイプのユーザ ID の電子メール アドレスに設定します。
   - **Microsoft Active Directory ファイル サーバ（ADFS）**：IDP タイプが ADFS の場合は、次のカスタム ルールが表示されていることを確認します。

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, Value = c.Value, ValueType = c.ValueType, Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:2.0:nameid-format:transient", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
"http://<IDP FQDN>/adfs/com/adfs/service/trust", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<SMC FQDN>/fedlet");
```

## 6. SSO ユーザの追加

SSO ユーザを追加するには、次の手順を使用します。ユーザはアイデンティティ プロバイダーを介して（アイデンティティ プロバイダーによって）認証されます。

1. SMC（Stealthwatch Web アプリケーション）にログインします。
2. [グローバル設定（Global Settings）] アイコンをクリックします。
3. [ユーザ管理（User Management）] を選択します。
4. [作成（Create）] > [ユーザ（User）] の順に選択します。

   手順については、[ユーザ（User）] アイコンをクリックします。 [Stealthwatch オンライン ヘルプ（Stealthwatch Online Help）] を選択します。ユーザの追加の詳細については、「ユーザの設定」を参照してください。

5. フィールドに入力して、新しいユーザを作成します。次のようにユーザを設定してください。
   - **認証サービス（Authentication Service）**：[SSO] を選択します。
   - **ユーザ名（User Name）**：IDP アカウントの電子メール アドレスの最初の部分を入力します。ID がログイン時に SSO に使用されるものと同じであることを確認してください。たとえば、name @ cisco.com の場合、このフィールドに「 name 」と入力します。
6. [保存（Save）] をクリックします。
7. [ユーザ管理（User Management）] に [SSO ユーザ（SSO User）] が表示されていることを確認します。

## 7. SAML ログインのテスト

1. SMC（Stealthwatch Web アプリケーション）にログインします。
2. ログイン ページで、ドロップダウンをクリックします。
3. [SAML] を選択します。
4. クレデンシャル ボタンをクリックします。
5. ログイン クレデンシャルを入力します。[セキュリティ分析ダッシュボード（Security Insight Dashboard）] が開きます。

## トラブルシューティング

| シナリオ | 注記 |
|---|---|
| アカウントのロックアウト | 緊急アカウント アクセスを使用してシステム設定で [SSO のみ（SSO Only）] を無効にします。 |
| IDP XML をダウンロードできない | IDP 証明書が SMC 信頼ストアにアップロードされていることを確認します。 |
| IDP 設定を保存できない | IDP 設定を調べて、入力したデータが正確で、余分なスペースが含まれていないことを確認します。また、IDP イベント ログを調べます。 |
| その他の問題 | 使用しているブラウザ用の SAML トレーサーをダウンロードします。SSO ログインを繰り返して、IDP と SP の間の交換を確認します。 |

# Stealthwatch の概要

アプライアンスの設定が完了したら、Stealthwatch オンラインヘルプで、環境の管理、動作の調査、脅威への対応などに関する指示を得られます。

## 概要

Stealthwatch の概要については、Stealthwatch オンラインヘルプの情報を参照してください。

1. [ユーザ(User)] アイコンをクリックします。
2. [Stealthwatch オンライン ヘルプ(Stealthwatch Online Help)] を選択します。
3. ページの上部にある [Stealthwatch ヘルプ(Stealthwatch Help)] メニューを選択します。
4. [Stealthwatchコンポーネント(Stealthwatch Components)] > [Stealthwatch Management Console(SMC)の概要(Stealthwatch Management Console(SMC) Overview)] > [Stealthwatch Webアプリケーションのバージョン(About Stealthwatch Web App)] の順に選択します。

## 環境の管理

ネットワークセキュリティ管理の一環として、いくつかの準備作業を行う必要があります。各ページにアクセスするためのメニューが、次の各トピックとともに表示されます。手順については、任意のページから [ユーザ(User)] アイコン > [Stealthwatchオンラインヘルプ(Stealthwatch Online Help)] を選択して確認してください。

- ホストグループの設定([設定(Configure)] > [ホストグループ管理(Host Group Management)]))
- ポリシーの作成と管理([設定(Configure)] > [ポリシー管理(Policy Management)])
- フロー検索の作成([分析(Analyze)] > [フロー検索(Flow Search)])
- Stealthwatch を使用するためのユーザ権限の管理([グローバル設定(Global Settings)] アイコン > [ユーザ管理(User Management)])

## 動作の調査

アラーム、イベント、ホストなどの調査については、Stealthwatch オンラインヘルプの情報を参照してください。

1. [ユーザ(User)] アイコンをクリックします。
2. [Stealthwatch オンライン ヘルプ(Stealthwatch Online Help)] を選択します。
3. ページの上部にある [Stealthwatch ヘルプ(Stealthwatch Help)] メニューを選択します。
4. [動作の調査(Investigating Behavior)] を選択します。

## 脅威への対応

ポリシー情報については、Stealthwatch オンラインヘルプの情報を参照してください。

1. [ユーザ(User)] アイコンをクリックします。
2. [Stealthwatch オンライン ヘルプ(Stealthwatch Online Help)] を選択します。
3. ページの上部にある [Stealthwatch ヘルプ(Stealthwatch Help)] メニューを選択します。
4. [脅威への対応(Responding to Threats)] を選択します。

# Central Management

Central Management を使用して、プライマリ SMC からアプライアンスを管理します。ここでは、Central Management の概要について説明します。各セクションの詳細については、Stealthwatch オンライン ヘルプを参照してください。

- **Central Management について**：アプライアンスが Central Management によって管理されている場合、それらのステータスを確認できるのに加えて、アプライアンス設定の編集、ソフトウェアの更新、再起動、シャットダウンなどを管理できます。
- Stealthwatch オンラインヘルプ：Stealthwatch オンラインヘルプを開くには、[ユーザ（User）] アイコンをクリックします。[Stealthwatchオンラインヘルプ（Stealthwatch Online Help）] を選択します。

## Central Management とアプライアンス管理インターフェイス

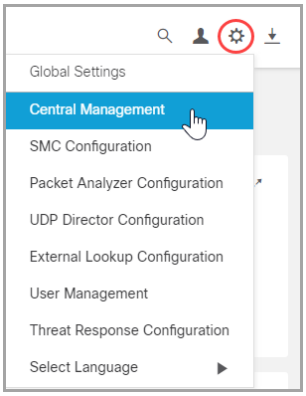
アプライアンスが Central Management で管理されている場合、アプライアンスの機能には、Central Management およびアプライアンス管理インターフェイス（アプライアンス管理）からアクセスします（次の表を参照）。

| Central Management | アプライアンス管理インターフェイス |
|---|---|
| アプライアンス構成の編集 | システム統計情報の表示 |
| ライセンス ステータスの確認（概要） | |
| 構成ファイルのバックアップ | データベースファイルのバックアップ |
| 監査ログの表示 | 診断パックの作成 |
| 再起動 | ネットワークホストと IP の検索 |
| シャットダウン | パケット キャプチャ |
| ソフトウェアのアップデート | DNS キャッシュのクリア |
| | アプライアンス固有の設定 |

Data Store との互換性を確保するようにフローコレクタを設定すると、アプライアンス管理インターフェイス（アプライアンス管理）によって特定の機能が非表示になります。フローコレクタやその他の関連タスクを設定するには、Central Management を使用します。

# Central Management を開く

1. プライマリ SMC にログインします。
2. [グローバル設定(Global Settings)] アイコンをクリックします。
3. [Central Management] を選択します。




# アプライアンス管理を開く

アプライアンス管理インターフェイスには、Central Management を通じて、またはアプライアンスに直接ログインすることでアクセスできます。

## Central Management を通じてアプライアンス管理を開く

1. [Central Management] の [Appliance Manager] ページで、アプライアンスの [アクション(Actions)] メニューをクリックします。
2. [アプライアンス統計情報の表示(View Appliance Statistics)] を選択します。
3. アプライアンス管理インターフェイスにログインします。

## 直接ログインを介してアプライアンス管理を開く

1. ブラウザのアドレスフィールドに、次のようにアプライアンスの IP アドレスを入力します。

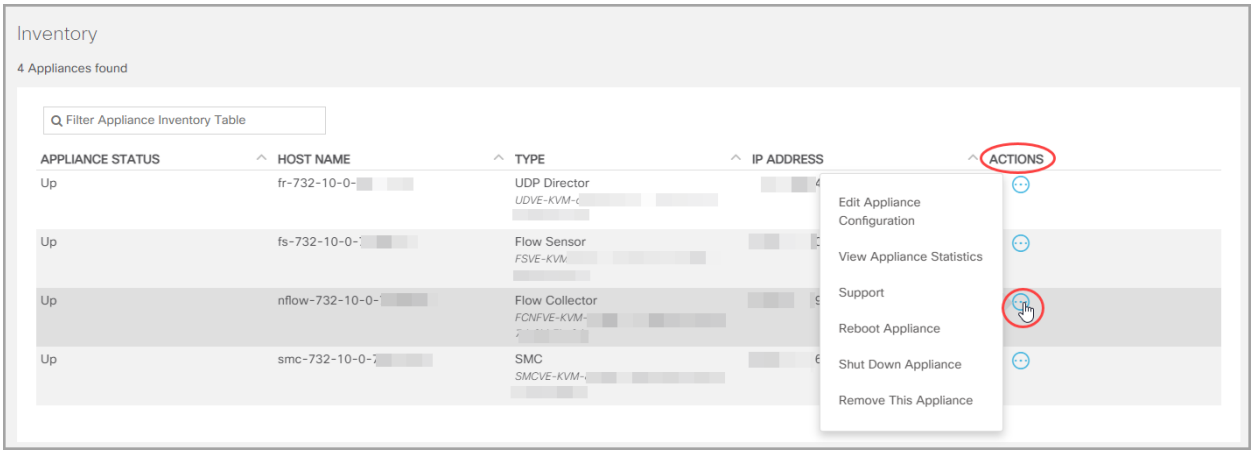
   **https://<IPAddress>**

   - **SMC**:IP アドレスの後ろに **/smc/index.html** を追加します。
   - **例**:https://1.1.1.1/smc/index.html

2. Enter を押します。

# アプライアンス設定の編集

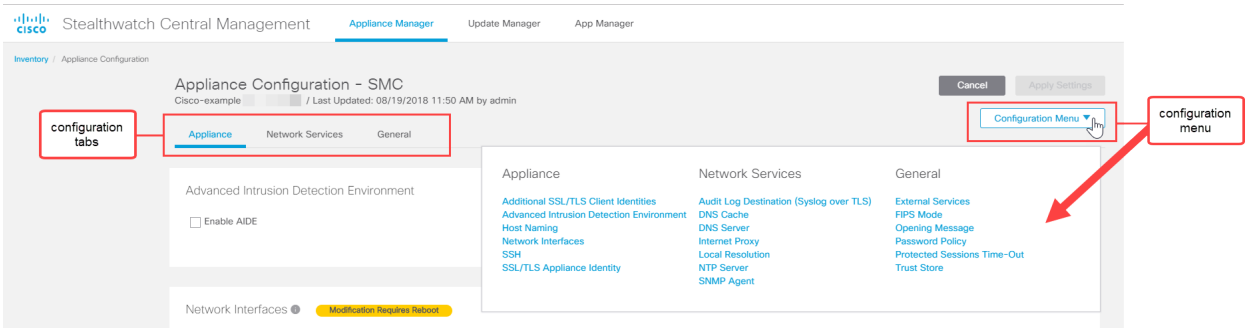
1. [Central Management] の [Appliance Manager] ページで、アプライアンスの [アクション (Actions)] メニューをクリックします。
2. [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。




3. [設定 (Configuration)] メニューをクリックします。リストから項目を選択します。

   または

   各タブをクリックして、各設定カテゴリを確認します。




4. 必要に応じて、各設定セクションに変更を加えます。各設定タブでは、複数の設定カテゴリを編集することができます。

> 手順については、[ユーザ (User)] アイコンをクリックします。

5. [設定の適用 (Apply settings)] をクリックします。画面に表示される指示に従って、設定変更を保存します。

   一部の変更には、システムの再起動が必要です。待機する場合は、変更を元に戻して、後で設定を編集して再起動します。

> ⚠ アプライアンスが自動的に再起動します。設定の変更が保留中の間は、アプライアンスを再起動させないでください。アプライアンスのステータスが [アップ(Up)] であることを確認するには、[Central Management] > [Appliance Manager] インベントリを参照します。

6. **Up**: [Appliance Manager] ページで、アプライアンスが設定変更を完了し、アプライアンスのステータスが **Up** に戻ることを確認します。

## アプライアンス統計情報の表示

**ホバー**: 各アプライアンス ステータスの詳細を確認する場合は、ステータスの上にマウス ポインタを置きます。

システムの統計情報、サービス、ディスク使用率、および Docker サービスを確認するには、アプライアンス管理インターフェイスにログインします。

1. [Central Management] の [Appliance Manager] ページで、アプライアンスの [アクション(Actions)] メニューをクリックします。
2. [アプライアンス統計情報の表示(View Appliance Statistics)] を選択します。
3. アプライアンス管理インターフェイスにログインします。

## Central Management からのアプライアンスの削除

次の手順に従って、Central Manager からアプライアンスを削除します。

1. [Central Management] の [Appliance Manager] ページで、アプライアンスの [アクション(Actions)] メニューをクリックします。
2. [このアプライアンスを削除(Remove This Appliance)] を選択します。

   **構成チャネルのダウン**: 構成チャネルがダウンしているためアプライアンスを削除する場合、「トラブルシューティング」の「構成チャネルのダウン」に移動して追加の手順を参照してください。

   トラブルシューティング: アプライアンス管理インターフェイスにログインしても、アプライアンスが Central Management から削除されない場合は、「トラブルシューティング」の「構成チャネルのダウン」の手順に進み、システム設定を使用して削除します。

   **Central Management**: 異なる Central Manager にアプライアンスを追加するには、アプライアンス設定ツールを使用します。

> ⚠ アプライアンスにカスタム証明書がある場合、アプライアンスを Central Management に追加する前に、アイデンティティ証明書と証明書チェーン(ルートおよび中間)を SMC 信頼ストアに保存してください。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

## Central Management へのアプライアンスの追加

Central Management にアプライアンスを追加するには、アプライアンス設定ツールを使用します。次を確認することが重要です。

- **カスタム証明書**：アプライアンスにカスタム証明書がある場合、アプライアンスを Central Management に追加する前に、アイデンティティ証明書と証明書チェーン（ルートおよび中間）をその独自の信頼ストアおよび SMC 信頼ストアに保存してください。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。
- **SMC 管理のクレデンシャル**：Central Management にアプライアンスを追加するには、SMC、ユーザ ID、およびパスワードが必要です。
- **RFD**：アプライアンスで工場出荷時のデフォルトにリセットした場合、アプライアンスを Central Management に追加する前にその IP アドレス、ホスト名、およびドメインを設定します（RFD 時にネットワーク設定を保持している場合でも設定します）。

  アプライアンスコンソールに **sysadmin** としてログインし、画面に表示される指示に従って IP アドレス、ホスト名、およびドメインを設定します。手順については、Stealthwatch ハードウェアまたはバーチャルエディションの設置ガイドを参照してください。

- **新規インストール**：新規インストールの場合は、インストールを完了し、Central Management に追加する前に IP アドレス、ホスト名、およびドメインを設定します。手順については、Stealthwatch ハードウェアまたはバーチャルエディションの設置ガイドを参照してください。

> ⚠ アプライアンスにカスタム証明書がある場合、アプライアンスを Central Management に追加する前に、アイデンティティ証明書と証明書チェーン（ルートおよび中間）を SMC 信頼ストアに保存してください。『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

1. アプライアンス管理インターフェイスにログインします。
2. アプライアンスのブラウザ アドレス バーで、IP アドレスの後ろの URL の終わりを /lc-ast に置き換えます。

   **https://<IPAddress>/lc-ast**

3. Enter を押します。
4. [次へ（Next）] をクリックして [Central Management] タブにスクロールします。
5. **IP アドレス**：SMC/Central Manager の IP アドレスを入力します。
6. [保存（Save）] をクリックします。
7. 画面の指示に従って SMC 管理者の資格情報を入力し、設定を終了します。アプライアンスの種類によっては、追加情報を入力する必要があります。
8. アプライアンス設定ツールの詳細については、「**1. Stealthwatch の設定**」を参照してください。

# SSH の有効化/無効化

このセクションは、SSH(セキュア シェル)を使用してアプライアンスにアクセスできるかどうかを制御する場合に使用します。

デフォルト:無効

> ⚠ SSH を有効にすると、システムの侵害リスクが増加します。SSH は必要な場合のみ有効にすることが重要です。SSH は、使用終了後に無効にします。

## SSH を開く

次の手順に従って、選択したアプライアンスの SSH を開きます。

1. Central Management を開きます。
2. アプライアンスの [アクション(Actions)] メニューをクリックします。
3. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
4. [アプライアンス(Appliance)] タブを選択します。

## SSH の有効化

1. [SSH] セクションを見つけます。
2. アプライアンスへの SSH アクセスを許可するには、[SSH の有効化(Enable SSH)] チェックボックスをオンにします。
3. アプライアンスへのルート アクセスの有効化を許可するには、[ルート SSH アクセスの有効化(Enable Root SSH Access)]チェックボックスをオンにします。
4. [設定の適用(Apply settings)] をクリックします。
5. 画面に表示される指示に従って操作します。

## SSH の無効化

1. アプライアンスへの SSH アクセスを削除するには、[SSH の有効化(Enable SSH)] チェックボックスをオフにします。
2. アプライアンスへのルート アクセスを削除するには、[ルート SSH アクセスの有効化(Enable Root SSH Access)] チェックボックスをオフにします。
3. [設定の適用(Apply settings)] をクリックします。
4. 画面に表示される指示に従って操作します。

# トラブルシューティング

## 構成チャネルのダウン

Appliance Manager で、アプライアンス ステータスとして [構成チャネルのダウン (Config Channel Down)] が表示されている場合は、次を確認します。

- **通信の設定**:ネットワーク通信の設定を確認します。
- **信頼ストア**:アプライアンス アイデンティティ証明書が正しい信頼ストアに保存されていることを確認します。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。
- **証明書**:アプライアンス アイデンティティ証明書を変更した場合は、その手順を確認し、証明書が正しい信頼ストアに保存されていることを確認します。手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。
- ライセンスの有効期限:詳細については、Stealthwatch スマート ソフトウェア ライセンシング ガイド [英語] を参照してください。
- **アプライアンスの削除**:構成チャネルのダウン中にアプライアンスを削除する場合は、システム設定からもアプライアンスを削除してください。
  - アプライアンスコンソールに sysadmin としてログインします。
  - **SystemConfig** と入力します。Enter を押します。
  - [リカバリ (Recovery)] > [アプライアンスの削除 (RemoveAppliance)] を選択します。

## アプライアンス管理インターフェイスを開く

アプライアンス管理インターフェイスには、Central Management を通じて、またはアプライアンスに直接ログインすることでアクセスできます。

トラブルシューティングのために Central Manager から SMC を削除した場合は、アプライアンス管理にログインする必要があります。

1. ブラウザのアドレス フィールドに、次のようにアプライアンスの IP アドレスを入力します。

   **https://<IPAddress>**

   - **SMC**:IP アドレスの後ろに **/smc/index.html** を追加します。
   - **例**:https://1.1.1.1/smc/index.html

2. Enter を押します。

## アプライアンス アイデンティティの交換

Stealthwatch バージョン 7.x アプライアンスはそれぞれ、固有の自己署名アプライアンス アイデンティティ証明書と一緒にインストールされます。アプライアンス アイデンティティ証明書を認証局からの証明書に置き換える場合の手順については、『SSL/TLS Certificates for Managed Appliances Guide』を参照してください。

> ⚠ 証明書はシステムのセキュリティにとって重要です。不適切に証明書を変更すると、Stealthwatch アプライアンスの通信が停止し、データ損失が発生します。

## ホスト名、ドメイン名、または IP アドレスの変更

アプライアンスの設置および設定後に、アプライアンスのホスト名、ネットワークドメイン名、または IP アドレスを変更するには、『SSL/TLS Certificates for Managed Appliances Guide』の手順に従います。

手順の一環として、アプライアンスを Central Management から一時的に削除します。アプライアンス アイデンティティ証明書が自動的に置き換えられます。

> ⚠ アプライアンス アイデンティティ証明書は、この手順の一環として自動的に置き換えられます。
>
> **アプライアンスがカスタム証明書を使用している場合は、**これらの設定の変更について Cisco Stealthwatch サポートにお問い合わせください。次に示す手順を使用しないでください。カスタム証明書と秘密キーのコピーがあることを確認してください。

## アプライアンス設定ツールを開く

アプライアンスの設定後にアプライアンス設定ツールを開くには、次の手順を使用します。

> ⚠ アプライアンス設定ツールを使用してホスト名、ネットワークドメイン名、または IP アドレスを変更する場合、アプライアンス アイデンティティ証明書が自動的に置き換えられます。
>
> **アプライアンスがカスタム証明書を使用している場合は、**これらの設定の変更について Cisco Stealthwatch サポートにお問い合わせください。次に示す手順を使用しないでください。カスタム証明書と秘密キーのコピーがあることを確認してください。

1. アプライアンスのブラウザ アドレス バーで、IP アドレスの後ろの URL の終わりを /lc-ast に置き換えます。

   **https://<IPAddress>/lc-ast**

2. Enter を押します。
3. 詳細については、次を参照してください。**1. アプライアンスの設定**

## システム設定の概要

新しいメニュー構造でシステム設定が更新されました。多くの場合、システム設定にはトラブルシューティングを伴います。サポートが必要な場合は、Cisco Stealthwatch サポートに連絡してください。

- [ユーザ(Users)]:使用可能なメニューは、ログイン ID(root、sysadmin、または admin)によって決まります。
- SSH:メニューにアクセスするには、SSH を有効にする必要があります。

1. アプライアンスコンソールにログインします。
2. **SystemConfig** と入力します。Enter を押します。
3. メインメニューから次のメニューを選択します。

- **ネットワーク**:アプライアンス管理ポートネットワーク、信頼できるホスト、およびネットワーク インターフェイスを変更するには、[ネットワーク(Network)]を選択します。
- セキュリティ:パスワードの変更またはリセット、Syslog コンプライアンスの管理を実行するには、[セキュリティ(Security)]を選択します。
- **リカバリ**:Central Management からのアプライアンスの削除、工場出荷時の初期状態へのリセットを実行するには、[リカバリ(Recovery)]を選択します。
- **詳細**:アプライアンスモデルの更新、ルートシェルのオープン、管理ユーザアカウントの管理、またはシングルサインオンの設定を実行するには、[詳細(Advanced)]を選択します。

## 信頼できるホストの変更

システム設定を使用すると、信頼できるホストのリストをアプライアンスのデフォルトから変更できます。ただし、信頼できるホストを変更する前に、Cisco Stealthwatch サポートにお問い合わせください。

> ⚠ 信頼できるホストを変更する前に、Cisco Stealthwatch サポートにお問い合わせください。

信頼できるホストのリストをデフォルトから変更する場合、各 Stealthwatch アプライアンスが展開内の他のすべての Stealthwatch アプライアンスの信頼できるホストのリストに含まれていることを確認してください。そうしない場合、アプライアンス間で通信できません。

1. アプライアンスコンソールに sysadmin としてログインします。
2. [ネットワーク(Network)] > [信頼できるホスト(Trusted Hosts)]を選択します。
3. 画面に表示される指示に従って、[信頼できるホスト(Trusted Hosts)]を変更します。

## 工場出荷時のデフォルトへのリセット

アプライアンスを工場出荷時のデフォルト(RFD)にリセットするには、次の手順を使用します。データを完全に消去するには、工場出荷時のデフォルトを 2 回リセットしてください。

- RFD を 2 回:データを完全に消去するには、工場出荷時のデフォルトを 2 回リセットしてください。
- 設定のバックアップ:アプライアンスの設定を復元する場合は、バックアップ設定とデータベースのバックアップファイルを保存してください。詳細については、Stealthwatch オンラインヘルプの「Backup Configuration Files (in Central Management)」および「Backup/Restore Database (Appliance Admin interface)」の各トピックを参照してください。RFD 後にバックアップを復元するには、Cisco Stealthwatch サポートにお問い合わせください。

> ⚠ アプライアンスを工場出荷時のデフォルト設定にリセット(RFD)すると、すべての既存データと設定情報が削除され、バックアップを作成した場合にのみ復元できます。

> ⚠ アプライアンスを工場出荷時のデフォルトにリセットすると、Central Management を使用して設定を復元できません。サポートが必要な場合は、Cisco Stealthwatch サポートに連絡してください。

1. アプライアンスコンソールに sysadmin としてログインします。
2. [リカバリ(Recovery)] > [工場出荷時のデフォルト(Factory Defaults)] を選択します。
3. 画面に表示される指示に従って工場出荷時のデフォルトにリセットし、アプライアンスを再起動します。

> ⚠ データを完全に消去するには、各アプライアンスで RFD を2 回 実行してください。

4. アプライアンスコンソールに **sysadmin** としてログインし、画面に表示される指示に従ってアプライアンスの IP アドレス、ホスト名、およびドメインを設定します。手順については、Stealthwatch ハードウェアまたはバーチャルエディションの設置ガイドを参照してください。この手順は、RFD 時にネットワーク設定を保持している場合でも必要です。
5. アプライアンス設定ツールにログインし、Central Management にアプライアンスを追加します。詳細については、「**Central Management へのアプライアンスの追加**」を参照してください。

## 管理者ユーザの有効化/無効化

デフォルトの管理者アカウントを有効または無効にするには、次の手順を使用します。

1. アプライアンスコンソールに sysadmin としてログインします。
2. [詳細設定(Advanced)] を選択します。
3. [Adminユーザ(Admin User)] を選択します。
4. 画面に表示される指示に従い、管理者ユーザ アカウントを有効または無効にします。
5. 上記の手順を繰り返して、Stealthwatch クラスタ内のすべてのアプライアンスで管理ユーザ アカウントを有効または無効にします。

## パスワードのリセットの有効化または無効化

パスワードのリセット機能を有効化または無効化するには、次の手順を使用します。[有効化(Enable)] を選択すると、GRUB コマンドライン インターフェイスを使用してパスワードをデフォルト設定にリセットできます。

> ⚠ パスワードのリセットを無効化し、パスワードを失った場合は、アプライアンスに保存されているデータへのアクセスが失われます。再度アプライアンスにアクセスするには、工場出荷時のデフォルトにリセットして再設定してください。

1. アプライアンスコンソールに root としてログインします。
2. **SystemConfig** と入力します。Enter を押します。
3. [セキュリティ(Security)] を選択します。
4. [パスワードのリセット(Password Reset)] を選択します。
5. 画面に表示される指示に従い、パスワードのリセットを有効または無効にします。

# パスワードをデフォルト設定にリセット

パスワードをデフォルト設定にリセットする方法は 2 つあります。

- **admin パスワード**:「SMC の admin パスワードのリセット」を使用します。
- **admin、root、sysadmin パスワード**:「admin、root、sysadmin パスワードをデフォルトにリセット」を使用します。

> ⚠ アプライアンスのパスワードをデフォルトにリセットしたら、必ずパスワードを変更してください。この手順は、セキュリティにとって重要です。手順については、「パスワードの変更」を参照してください。

## SMC の admin パスワードのリセット

次の手順を使用して、admin パスワードを SMC のデフォルト設定にリセットします。次に、セキュリティを最大限に高めるためにアプライアンスのパスワードを変更します。

- **要件**:次の手順を完了するには、アプライアンスのルート パスワードが必要です。
- **その他のユーザ**:次の手順により、admin ユーザがデフォルト パスワードにリセットされます。個人ユーザのパスワードは変更されません。
- **その他のアプライアンス**:これらの手順では、他の Stealthwatch アプライアンス(フローコレクタ、フローセンサー、または UDP Director)の admin パスワードはリセットされません。

1. アプライアンスコンソールに root としてログインします。
2. `rm /lancope/var/smc/config/users/admin/user.xml` と入力します。Enter を押します。
3. `docker restart smc` と入力します。Enter を押します。
4. `docker restart nginx` と入力します。Enter を押します。

   これにより、admin パスワードがデフォルト値にリセットされます。

5. アプライアンスコンソールを終了します。
6. admin パスワードをデフォルトから変更するには、「パスワードの変更」に進みます。この手順は、セキュリティにとって重要です。

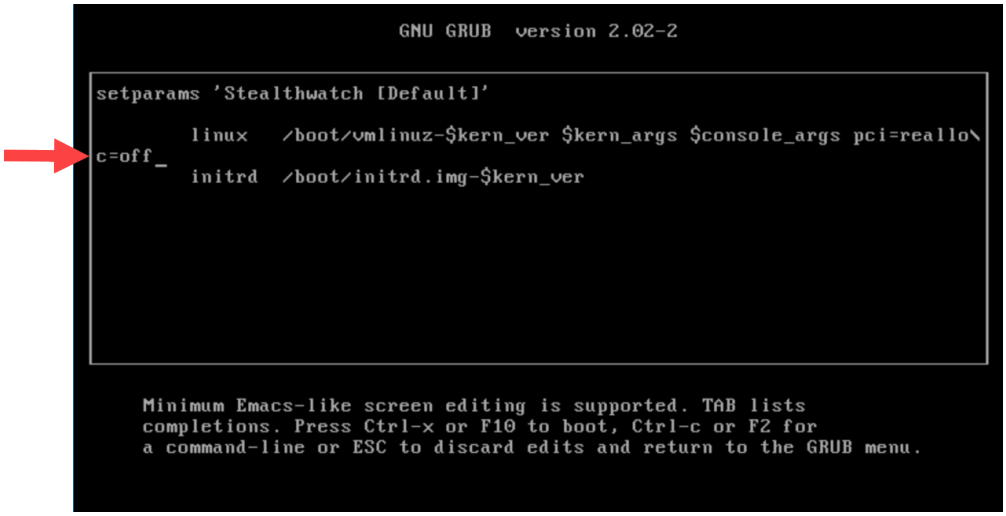
## admin、root、sysadmin パスワードをデフォルトにリセット

コンソールアクセスを使用して、アプライアンスの admin、root、および sysadmin パスワードをデフォルト設定にリセットします。次に、セキュリティを最大限に高めるためにアプライアンスのパスワードを変更します。

1. アプライアンスコンソール(CIMC またはハイパーバイザ)にログインします。
2. アプライアンスを再起動します。
3. コンソール画面に GRUB メニューが表示されたら、「e」と入力して編集モードに切り替えます。

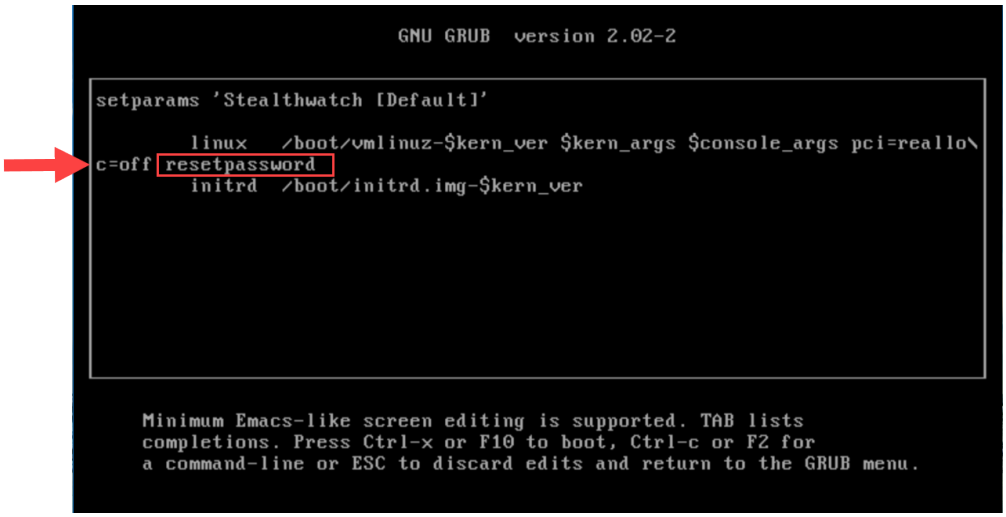

4. 2 番目の行にカーソルを移動します。

   コマンド ラインは、アプライアンスのバージョンによってわずかに異なる場合があります。




5. `c=off` の後に `resetpassword` と入力して、コマンド ラインを次の例のようにします。

```
linux /boot/vmlinuz-$kern_ver $kern_args $console_args
pci=reallo\
c=off resetpassword
```




6. Ctrl+X を押して起動を再開します。

   admin、root、および sysadmin パスワードがデフォルト値にリセットされます。

7. パスワードをデフォルトから変更するには、「**パスワードの変更**」に進みます。この手順は、セキュリティにとって重要です。

# パスワードの変更

デフォルトのパスワードまたは以前のパスワードからパスワードを変更するには、次の手順を使用します。次の基準を使用していることを確認します。

- 長さ:8 ～ 256 文字
- 変更:新しいパスワードが以前のパスワードと最低 4 文字異なっていることを確認します。

| ユーザ | デフォルト パスワード |
|---|---|
| admin | lan411cope |
| root | lan1cope |
| sysadmin | lan1cope |

## sysadmin パスワードの変更

1. アプライアンスコンソールに sysadmin としてログインします。
2. [セキュリティ(Security)]を選択します。
3. [パスワード(Password)]を選択します。
4. 画面に表示される指示に従って、sysadmin パスワードを変更します。
5. システム設定を終了します。

## ルート パスワードの変更

1. アプライアンスコンソールに root としてログインします。
2. **SystemConfig** と入力します。Enter を押します。
3. [セキュリティ(Security)] を選択します。
4. [パスワード(Password)] を選択します。
5. 画面に表示される指示に従って、ルート パスワードを変更します。
6. システム設定を終了します。

## SMC の admin パスワードの変更

1. SMC に admin としてログインします。

   - URL : https://<IPAddress>
   - ログイン : admin
   - デフォルトパスワード : lan411cope

2. [グローバル設定(Global Settings)] アイコンをクリックします。[ユーザ管理(User Management)] を選択します。
3. リスト内で admin ユーザを見つけます。
4. [アクション(Actions)] メニューをクリックします。[パスワードの変更] を選択します。
5. 画面に表示される指示に従って、admin パスワードを変更します。次の基準を使用します。

   - 長さ : 8 ～ 256 文字
   - **変更** : 新しいパスワードがデフォルト パスワードと最低 4 文字異なっていることを確認します。

## 他のすべてのアプライアンスの admin パスワードの変更

フローコレクタ、フローセンサー、または UDP Director の admin ユーザパスワードを変更するには、次の手順を使用します。

1. admin としてアプライアンス管理インターフェイスにログインします。

   - URL : https://<IPAddress>
   - ログイン : admin
   - デフォルトパスワード : lan411cope

2. [ユーザの管理(Manage Users)] > [パスワードの変更(Change Password)] を選択します。
3. 現在のパスワードと新しいパスワードを入力します。
4. [適用(Apply)] をクリックします。画面に表示される指示に従って、パスワードを変更します。
5. 別のアプライアンスの admin パスワードを変更するには、ステップ 1 ～ 4 を繰り返します。

# パッチのインストールとソフトウェアのアップデート

お使いのソフトウェアバージョンに対する最新のパッチをインストールすることで、Stealthwatch を最新の状態に保つようにしてください。詳細および手順については、Cisco Software Central にアクセスして確認してください。

ソフトウェアアップデートは、Cisco Software Central の Cisco スマートアカウントにも送信されます。正常に更新するには、Stealthwatch 更新ガイド [英語] の手順に従ってください。

# サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコ パートナーにご連絡ください。
- Cisco Stealthwatch サポートのお問い合わせ先：
- Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
- 電子メールでケースを開く場合：tac@cisco.com
- 電話でサポートを受ける場合：800-553-2447（米国）
- ワールドワイド サポート番号：
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

# 著作権情報