Cisco Secure Network Analytics

v7.4 管理対象アプライアンスの SSL/TLS 証明書ガイド

目次

はじめに

Cisco Secure Network Analytics（旧 Stealthwatch）v7.4 アプライアンスの SSL/TLS 証明書関連の設定を変更するには、このガイドを使用します。

- Cisco Secure Network Analytics Manager（旧 Stealthwatch Management Console）
- Cisco Secure Network Analytics Flow Collector
- Cisco Secure Network Analytics Flow Sensor
- Cisco Secure Network Analytics UDP Director

詳細については、「**概要**」を参照してください。

データストア

このガイドには、Cisco Secure Network Analytics データストア の情報は含まれていません。詳細については、Data Store 展開およびコンフィギュレーション ガイド [英語] を参照してください。

DoDIN およびコモンクライテリアへの準拠

米国国防総省情報ネットワーク（DoDIN）またはコモンクライテリア（CC）に準拠するように Secure Network Analytics を設定するには、*DoDIN 軍部固有導入ガイド* [英語] または*コモンクライテリア管理ガイド* [英語] の手順に従ってください。

対象読者

このガイドは、Secure Network Analytics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。SSL/TLS 証明書に精通していることを前提としています。サポートが必要な場合は、シスコサポートまでお問い合わせください。

用語

このガイドでは、Flow Sensor Virtual Edition（VE）などの仮想製品を含むすべての Secure Network Analytics 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、マネージャ によって管理される Secure Network Analytics アプライアンスのグループです。

計画時間

中断時間が最小限で済む時間帯に Secure Network Analytics を設定することが重要です。このガイドの手順には、証明書のインストール、設定の変更、および再起動が含まれる場合があります。これらの変更中はシステムが使用できなくなり、ネットワーク接続の問題が発生する可能性があります。サポートが必要な場合は、シスコサポートまでお問い合わせください。

ベストプラクティス

- **手順の確認**：開始する前に手順を確認し、要件と手順を理解していることを確認します。また、手順を順序どおりに実行してください。
- **再起動**：アプライアンスの再起動中または設定変更中は、アプライアンスを強制的に再起動しないでください。
- **1 つずつ**：一度に 1 つのアプライアンスを設定します。次のアプライアンス設定を開始する前に、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。
- **フレンドリ名**：アプライアンス アイデンティティ証明書を置き換える場合、クライアント アイデンティティ証明書を追加する場合、または信頼ストアに証明書を追加する場合は、各フレンドリ名が一意であることを確認します。フレンドリ名を重複させないでください。
- アプライアンスの削除/追加：このガイドの多くの手順には、Central Management から一時的にアプライアンスを削除する手順が含まれています。アプライアンスを（アプライアンス セットアップ ツールを使用して）Central Management から削除し、Central Management に再度追加する順序と手順に従ってください。

  Manager：マネージャ でホスト情報またはアプライアンス アイデンティティ証明書を変更する場合は、すべてのアプライアンスを（表示されている順序で）Central Management から削除し、変更後にクラスタを再構築する必要があります。

  マネージャ 以外のアプライアンス：マネージャ 以外の個別のアプライアンス（Flow Collector、Flow Sensor、または UDP Director）のホスト情報またはアプライアンス アイデンティティ証明書を変更する場合は、各アプライアンスを Central Management から削除し、変更後に Central Management に再度追加します。

アプライアンスのアイデンティティ証明書

各 Secure Network Analytics アプライアンスは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。

認証

Secure Network Analytics クラスタ内のアプライアンスの通信は x.509v3 証明書を使用して認証されます。

証明書の要件

Secure Network Analytics のデフォルトのアプライアンス アイデンティティ証明書を認証局からのアプライアンス アイデンティティ証明書に置き換えることができます。

- 手順については、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。
- Central Management で証明書署名要求（CSR）を生成するか、すでに認証局の証明書がある場合は CSR を省略できます。Central Management で CSR を生成する場合、記載されている要件は CSR に含まれます。

要件	CSR の作成 （Central Management で操作）	CSR のスキップ （Central Management で操作）
フォーマット	PEM（.cer、.crt、.pem）または PKCS#12（.p12、.pfx、.pks） PEM を使用する場合は、「PEM チェーンファイルの要件」を参照してください。	PKCS#12（p12、.pfx、pks）
RSA キーの長さ	4096 ビットまたは 8192 ビット	2048 ビット（非推奨）以上
認証 （拡張キーの使用状況）	CSR 要求サーバー（serverAuth）とクライアント（clientAuth）の認証。	サーバー（serverAuth）とクライアント（clientAuth）の認証は、アプライアンス アイデンティティ証明書に必要です。
日付の範囲	証明書の日付が最新であり、期限が切れていないことを確認します。	証明書の日付が最新であり、期限が切れていないことを確認します。

アプライアンス セットアップ ツール

アプライアンス セットアップ ツールを使用して Central Management にアプライアンスを追加すると、アプライアンス アイデンティティ証明書が Secure Network Analytics のデフォルトのアプライアンス アイデンティティ証明書に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する場合は、それらが保存されていることを確認します。これにより、デフォルトのアプライアンス アイデンティティを Central Management に追加した後にカスタム証明書に置き換えることができます。手順については、「SSL/TLS アプライアンス アイデンティティ証明書の置換」を参照してください。

マネージャ フェールオーバー

Manager がフェールオーバーペアとして設定されている場合は、証明書の手順によっては、フェールオーバーの関係を削除して再設定する必要があります。選択した手順の説明を必ず確認してください。

クライアント アイデンティティ証明書

クライアント アイデンティティは外部サービス間の通信に使用されます。手順については、「SSL/TLS クライアント アイデンティティの追加」を参照してください。

証明書の要件

クライアント アイデンティティ証明書を マネージャ に追加する場合は、認証局の証明書があることを確認します。

- 手順については、「SSL/TLS クライアント アイデンティティの追加」を参照してください。
- Central Management で証明書署名要求（CSR）を生成するか、すでに認証局の証明書がある場合は CSR を省略できます。証明書が要件を満たしていることを確認するには、表を参照してください。Central Management で CSR を生成する場合、記載されている要件は CSR に含まれます。

要件	CSR の作成 （Central Management で操作）	CSR のスキップ （Central Management で操作）
フォーマット	PEM（.cer、.crt、.pem）または PKCS#12（.p12、.pfx、.pks） PEM を使用する場合は、「PEM チェーンファイルの要件」を参照してください。	PKCS#12（p12、.pfx、pks）
RSA キーの長さ	2048 ビット（非推奨）、4096 ビット、または 8192 ビット	2048 ビット（非推奨）以上
認証 （拡張キーの使用状況）	CSR 要求サーバー（serverAuth）とクライアント（clientAuth）の認証。	クライアント アイデンティティ証明書には、クライアント（clientAuth）認証が必要です。
日付の範囲	証明書の日付が最新であり、期限が切れていないことを確認します。	証明書の日付が最新であり、期限が切れていないことを確認します。

PEM チェーンファイルの要件

PEM 形式の認証局（CA）証明書を使用してアプライアンス アイデンティティ証明書を置き換えるか、またはクライアント アイデンティティ証明書を マネージャ に追加する場合は、手順の一環として CA 証明書チェーンファイルをアップロードすることをお勧めします。チェーンファイルには、ルート証明書と中間証明書が含まれています。

チェーンファイルが次の要件を満たしていることを確認してください。

- **コンテンツ**：チェーンファイルにすべての署名証明書と認証局証明書が含まれるようにします。チェーンファイルのアップロードにアイデンティティ証明書を含めないでください。
- **順序**：証明書チェーンを手動で構築する場合は、証明書を降順で作成します。これにより、最後の中間証明書がファイルの最初に配置され、その後ろに残りの中間証明書が降順に配置されます。ルート証明書がファイル順序の最後になります。

  次に例を示します。

  ―BEGIN CERTIFICATE―
  中間証明書 #3
  ―END CERTIFICATE―
  ―BEGIN CERTIFICATE―
  中間証明書 #2
  ―END CERTIFICATE―
  ―BEGIN CERTIFICATE―
  中間証明書 #1
  ―END CERTIFICATE―
  ―BEGIN CERTIFICATE―
  ルート CA 証明書
  ―END CERTIFICATE―

チェーンファイルをアップロードしてアプライアンス アイデンティティを置き換える場合は、チェーンを 1 つのファイルとしてアップロードします。信頼ストアにチェーンファイルをアップロードすると、チェーンの各部分が個別にアップロードされます。選択した手順の説明に従ってください。

信頼ストアの要件

このガイドの多くの手順では、アプライアンスの信頼ストアで特定の順序で証明書を追加または削除する必要があります。これらの手順がシステム通信に不可欠です。証明書をアプライアンスの信頼ストアに保存すると、アプライアンスはそのアイデンティティを信頼し、通信できるようになります。証明書と要件は証明機関によって決定されます。

アプライアンス アイデンティティ証明書とクライアント アイデンティティ証明書を信頼ストアにアップロードする場合は、次の証明書をアップロードしてください。

- identity
- chain（ルート証明書と中間証明書）

ファイルに複数の証明書が含まれている場合は、各証明書を信頼ストアに個別にアップロードします。チェーン全体を 1 つのファイルとしてアップロードしないでください。

フレンドリ名：証明書を信頼ストアに追加する場合は、各フレンドリ名が一意であることを確認します。フレンドリ名を重複させないでください。

ワイルドカード証明書（クライアント アイデンティティのみ）

アプライアンスを 7.x に更新し、Secure Network Analytics（旧 Stealthwatch）の以前のバージョンから信頼ストアにクライアント アイデンティティ ワイルドカード証明書をインストールすると、有効期限が切れるまではワイルドカード証明書を使用できます。新しいワイルドカード証明書は、Central Management で CSR の手順を省略した場合にのみサポートされます。

追加の証明書の設定

このガイドでは、アプライアンス アイデンティティとクライアント アイデンティティの設定について説明します。証明書、およびサーバー ID 検証の要件を必要とする追加の設定が Secure Network Analytics で必要な場合があります。機能のヘルプまたはガイドの手順に従います。

- **監査ログの宛先**：ヘルプの手順に従います。（[ユーザ（User）]）アイコン を選択して [監査ログの宛先（Audit Log Destination）]検索します。
- **シスコISEまたは Cisco ISE-Pic**：『ISE and ISE-PIC Configuration Guide』の手順に従います。
- LDAP：ヘルプの手順に従います。（[グローバル設定（Global Settings）]）アイコン を選択して [LDAP] を検索します。
- パケットアナライザ：ヘルプの手順に従います。（[グローバル設定（Global Settings）]）アイコン 選択して「パケットアナライザ」を検索します。
- SAML SSO：システム コンフィギュレーション ガイド [英語] の手順に従います。
- 応答管理に対する SMTP の設定：ヘルプの手順に従ってください。（[ユーザ（User）]）アイコン を選択して「SMTP の設定」を検索します。

> その他のコンフィギュレーション ガイドについては、コンフィギュレーション ガイド [英語] を参照してください。

Central Management を開く

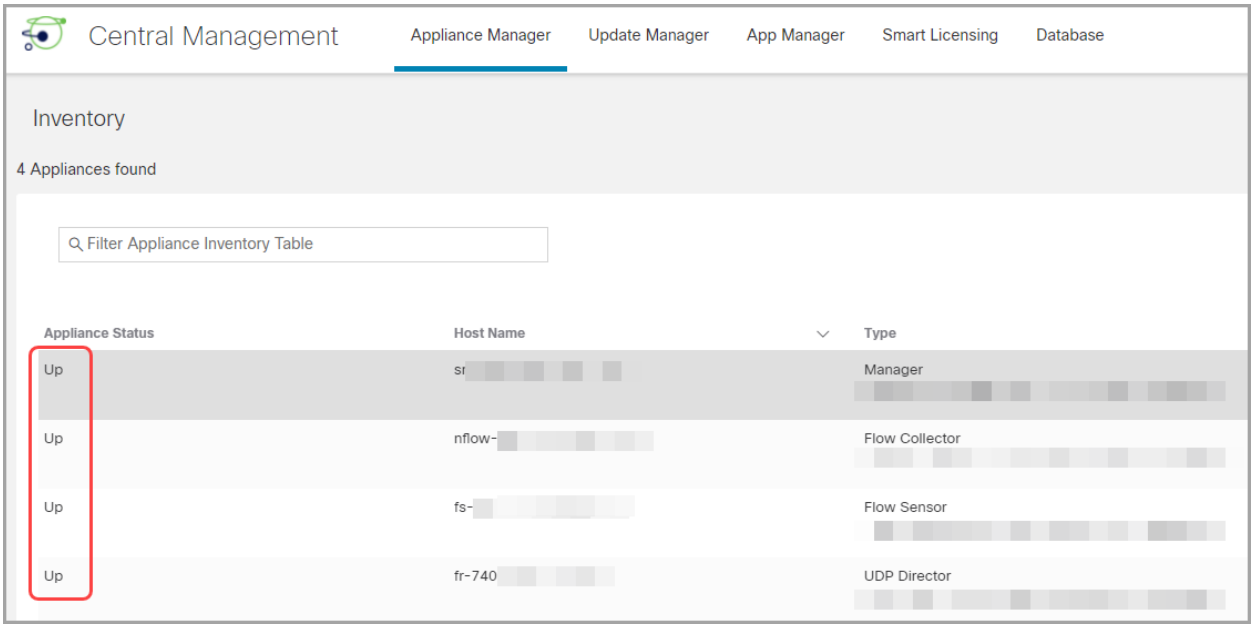
このガイドでは、主に Central Management を使用します。

1. アプライアンスに管理者としてログインします（https://<IPAddress>）。
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。

アプライアンスのステータス（Appliance Status）がアップ（Up）であることの確認

一度に 1 つのアプライアンスを設定します。Central Management にアプライアンスを追加するか、または設定を変更することで、アプリケーションのステータスは [初期化中（Initializing）] または [設定チャネル保留中（Config Channel Pending）] が [アップ（Up）] に変化します。

[アプライアンスのステータス（Appliance Status）] 列を確認します。他の変更を続行する前に、Central Management 内のすべてのアプライアンスの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。



概要

証明書は、Secure Network Analytics における複数の設定の変更に関係します。手順を選択する場合は、開始する前に証明書の要件と手順を確認してください。

> ⚠ 証明書はシステムのセキュリティにとって重要です。証明書を不適切に変更すると、Secure Network Analytics アプライアンスの通信が停止し、データ損失の原因となります。

タスク	注意
証明書の確認	選択したアプライアンスにインストールされているアプライアンス アイデンティティ証明書またはクライアント アイデンティティ証明書を確認します。
証明書の保存	アプライアンス アイデンティティ証明書を保存します。
シスコのバンドルのダウンロード	
証明書の有効期限の変更	アプライアンスに Secure Network Analytics v7.4 がインストールされている場合は、期限切れまたは期限切れになっていないシスコのデフォルトのアプライアンス アイデンティティ証明書の有効期限を更新できます。また、アプライアンスのホスト情報（IP アドレス、ホスト名、ドメイン名）は保持されます。 アプライアンスが認証局からのカスタム証明書を使用する場合の手順については、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。
アプライアンス アイデンティティ証明書の置換	各 Secure Network Analytics アプライアンスは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。手順に従って、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ます。
ホスト名の変更	シスコのデフォルト証明書を使用するアプライアンスのアプライアンスホスト名を変更します。 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シスコサポートにお問い合わせください。

ネットワークドメイン名の変更	シスコのデフォルトの証明書を使用するアプライアンスのネットワークドメイン名を変更します。 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シスコサポートにお問い合わせください。
IP アドレス（eth0）の変更	シスコのデフォルト証明書を使用するアプライアンスの IP アドレス（eth0 ネットワーク インターフェイス）を変更します。この項には、Central Management で eth1 または eth2 などを変更する手順も含まれています。 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シスコサポートにお問い合わせください。
クライアント アイデンティティ証明書	クライアント アイデンティティは外部サービス間の通信に使用されます。Secure Network Analytics アプライアンスが外部サービスを使用する場合は、手順に従って必要なクライアント アイデンティティ証明書を追加します。
トラブルシューティング	

証明書の確認

次の手順を実行して、選択したアプライアンスのアプライアンス アイデンティティ証明書またはクライアント アイデンティティ証明書を確認します。

1. Central Management を開きます。
2. アプライアンスの ••• ([省略記号(Ellipsis)])アイコン 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。
5. **アプライアンス アイデンティティ証明書を確認するには、**[SSL/TLS アプライアンス アイデンティティ(SSL/TLS Appliance Identity)] セクションに移動します。

   クライアント アイデンティティ証明書を確認するには、追加の SSL/TLS クライアント アイデンティティ(Additional SSL/TLS Client Identities)] セクションに移動します。

証明書の保存

次の手順を使用して、最新のアプライアンス アイデンティティ証明書を保存します。デフォルトに戻す必要がある場合は、変更を行う前に証明書を保存しておくと役立ちます。

> ブラウザのロックまたはセキュリティアイコンをクリックすることもできます。画面に表示される指示に従って証明書をダウンロードします。手順は、使用しているブラウザによって異なります。

1. アプライアンスにログインします。
2. ブラウザのアドレスバーで、IP アドレスの後のパスを **/secrets/v1/server-identity** に置き換えます。

   例：https://<IPaddress>/secrets/v1/server-identity
3. 画面に表示される指示に従って証明書を保存します。
   - **オープン**：ファイルを表示するには、テキストファイル形式を選択します。
   - **トラブルシューティング**：証明書をダウンロードするためのプロンプトが表示されない場合は、自動的にダウンロードされている場合があるため、[ダウンロード（Downloads）] フォルダを確認するか、あるいは別のブラウザまたは方法を試します。

シスコのバンドルのダウンロード

シスコでは厳選したルート認証局（CA）の事前検証済みのデジタル証明書をバンドルとして定期的にリリースしています。それらのバンドルはすべての Secure Network Analytics アプライアンス（v7.3.1 以降）に適用される共通のアプライアンスパッチ SWU ファイルとしてリリースされます。

各パッチには、シスコのサービスとの接続に使用するコア証明書バンドルと、シスコ以外のサービスとの接続に使用する外部証明書バンドルが含まれます。シスコでは、各バンドルの内容に関する情報を提供するパッチを含む readme ファイルも提供しています。

それらのバンドルと readme ファイルは、https://software.cisco.com の Software Central からダウンロードできます。

- すべてのアプライアンスに最新のシスコバンドルパッチをインストールする必要があります。
- アプライアンスのイメージを更新すると、シスコのバンドルパッチは再度適用されず、証明書バンドルは、リリースとともに出荷された証明書バンドルに戻ります。パッチの返却後は最新のバンドルに更新する必要があります。

更新時の証明書チェック

Secure Network Analytics へのアップグレードには、シスコのバンドルのアップグレードによって使用環境に問題が発生しないことを確認するための証明書チェックが含まれています。信頼ストアにエンドエンティティ証明書のみがある場合は、アップグレードは失敗します。Central Management の信頼ストアに証明書の完全なチェーンがあることを確認します。詳細および手順については、システム更新ガイド [英語] を参照してください。

追加された証明書の完全なチェーンが Central Manager の信頼ストアに存在しない場合、システムの更新は失敗します。詳細については、システム更新ガイド [英語] を参照してください。

証明書の有効期限の変更（概要）

アプライアンスが使用する証明書のタイプと、それらの期限がすでに切れているかどうかによって、証明書の有効期限を更新する方法を選択します。

証明書	手順
期限切れになっていないシスコのデフォルト証明書	手順については、「**期限切れになっていないシスコのデフォルトの証明書の置換**」を参照してください。 有効期限に加えてホスト情報を変更する必要がある場合は、「**ネットワーク インターフェイスの変更**」または「**ホスト名またはネットワークドメイン名の変更**」の手順を実行します。
期限切れのシスコのデフォルト証明書	手順については、「**期限切れになったシスコのデフォルト証明書の置換**」を参照してください。 有効期限に加えてホスト情報を変更する必要がある場合は、「**ネットワーク インターフェイスの変更**」または「**ホスト名またはネットワークドメイン名の変更**」の手順を実行します。
カスタム SSL/TLS 証明書	アプライアンスが認証局からのカスタム証明書を使用する場合の手順については、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。

アプライアンスにカスタム SSL/TLS 証明書がインストールされている場合、証明書の再生成はサポートされません。ただし、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を使用してカスタム証明書を置き換えることができます。

期限切れになっていないシスコのデフォルトの証明書の置換

各 Secure Network Analytics アプライアンスは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。次の手順を実行して、**期限切れになっていない**アプライアンス アイデンティティ証明書の有効期限を変更します。

- **ホスト情報**:アプライアンスのホスト情報(IPアドレス、ホスト名、ドメイン名)は保持されます。有効期限に加えてホスト情報を変更する必要がある場合は、(このセクションの手順ではなく)「**ネットワーク インターフェイスの変更**」または「**ホスト名またはネットワークドメイン名の変更**」の手順を実行します。
- **カスタム証明書**:カスタム アプライアンス アイデンティティ証明書を使用するアプライアンスでは、この手順はサポートされません。手順については、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。

> 証明書の有効期限が切れている場合は、「**期限切れになったシスコのデフォルト証明書の置換**」を参照してください。アプライアンスが認証局からのカスタム証明書を使用する場合は、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。

要件

開始する前に、「はじめに」の「**ベストプラクティス**」を確認し、次の要件を確認します。

- **ユーザー**:admin と sysadmin のユーザーアクセス権が必要です。
- **マネージャ フェールオーバー**:Manager がフェールオーバーペアとして設定されている場合にマネージャ 証明書を更新するには、次の手順を開始する前にフェールオーバーの関係を削除します。手順については、フェールオーバー コンフィギュレーション ガイド [英語] を参照してください。フェールオーバーペアを削除すると、セカンダリ マネージャ がクラスタから削除されます。この手順には、セカンダリ マネージャ を工場出荷時のデフォルトにリセットする手順が含まれています。

アプライアンスの手順の選択

- **マネージャ と管理対象アプライアンス**:**マネージャ および管理アプライアンス**を使用して、クラスタ内の マネージャ とその他の管理対象アプライアンスの証明書の有効期限を変更します。手順の一部として、Central Management からすべてのアプライアンスを(示されている順序で)削除し、変更後にクラスタを再構築します。
- **マネージャ 以外の個別のアプライアンス**:**マネージャ以外の個別のアプライアンス**を使用して、マネージャ 以外のアプライアンス(Flow Collector、Flow Sensor、または UDP Director)の証明書の有効期限を変更します。この手順では、個別のアプライアンスを Central Management から削除し、変更後に Central Management に再度追加します。

マネージャ および管理アプライアンス

次の手順に従って、クラスタ内の マネージャ とその他の管理対象アプライアンスの証明書の有効期限を変更します。Central Management からアプライアンスを削除し、指定した順序で再度追加してください。

マネージャ フェールオーバー：Manager がフェールオーバーペアとして設定されている場合は、これらの手順を開始する前に、フェールオーバーの関係を削除します。手順については、フェールオーバー コンフィギュレーション ガイド [英語] を参照してください。フェールオーバーペアを削除すると、セカンダリ マネージャ がクラスタから削除されます。この手順には、セカンダリ マネージャ を工場出荷時のデフォルトにリセットする手順が含まれています。

> 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。
>
> **カスタム証明書を使用するアプライアンス**の場合、アプライアンスでカスタム アプライアンス アイデンティティ証明書を使用するこの手順はサポートされていません。手順については、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。

概要

全体的な手順は次のとおりです。

1. **アプライアンスのステータスの確認**
2. **Central Management を使用したアプライアンスの削除**
3. **システム設定を使用したアプライアンスの削除**
4. **証明書の再生成**
5. **Central Management への マネージャ の登録**
6. **Central Management へのアプライアンスの追加**
7. **信頼ストアからの古い証明書の削除**
8. **マネージャ フェールオーバーペアの設定**

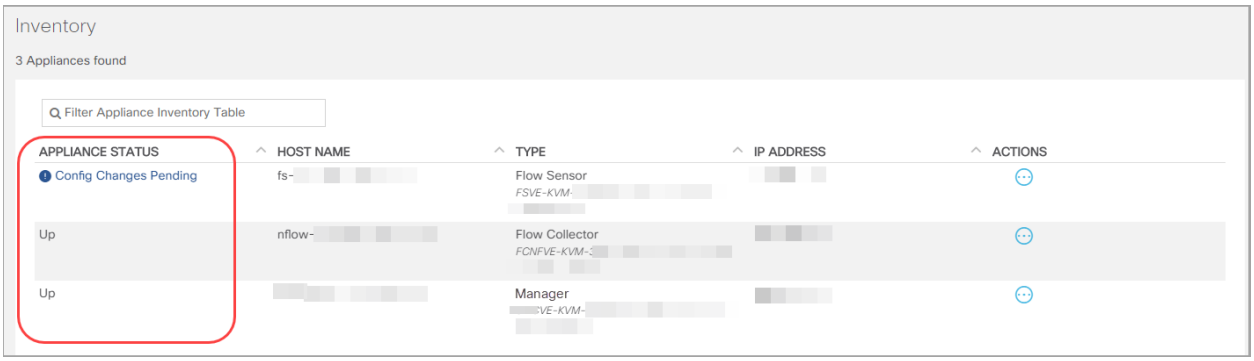
> マネージャ を変更するだけの場合は、すべてのアプライアンスを Central Management から削除する必要があります。マネージャ 以外の個別のアプライアンスのみを変更する必要がある場合は、「**マネージャ以外の個別のアプライアンス**を参照してください。

1. アプライアンスのステータスの確認

すべてのアプライアンスを Central Management から削除する前に、それらが [アップ（Up）] と表示されていることを確認します。

1. プライマリ マネージャ 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. [アプライアンスステータス（Appliance Status）] 列を確認します。すべてのアプライアンスが [アップ（Up）] と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 [設定チャネルのダウン（Config Channel Down）] または [設定の変更を保留中（Config Changes Pending）] と表示されている場合は、[アップ（Up）] に戻るまで数分間待ちます。解決しない場合は、「**2. Central Management を使用したアプライアンスの削除**」を使用して、Central Management からアプライアンスを削除します。次に、「**3. システム設定を使用したアプライアンスの削除**」の手順を実行します。



2. Central Management を使用したアプライアンスの削除

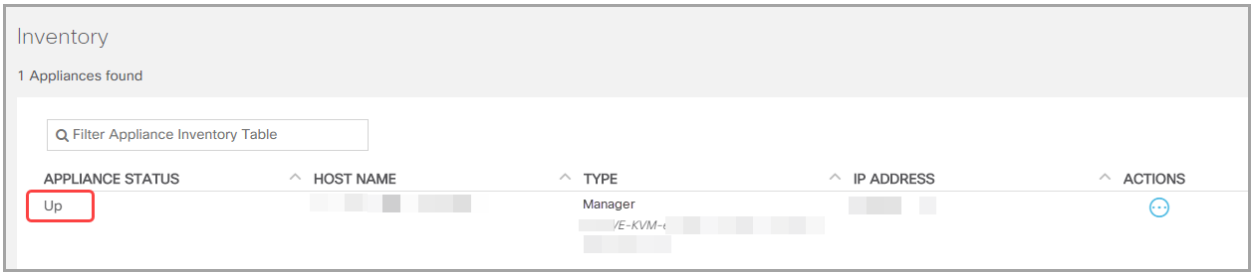
次の手順を実行して Central Management からアプライアンスを削除します。指定した順序ですべてのアプライアンスを Central Management から削除してください。

> ⚠ Central Management から最後に マネージャ を削除します。

1. すべてのアプライアンス（プライマリ マネージャ を除く）を Central Management から削除します。
   - アプライアンスの ••• （[省略記号（Ellipsis）]）アイコン をクリックします。
   - [このアプライアンスの削除（Remove This Appliance）] を選択します。

> ℹ Central Management からアプライアンスを削除すると、マネージャ アプライアンスのステータスが [設定の変更を保留中（Config Changes Pending）] から [アップ（Up）] に移行します。

2. マネージャ アプライアンスのステータスが [アップ（Up）] と表示され、Central Management に他のアプライアンスがないことを確認します。



3. Central Management からプライマリ マネージャ を削除します。
   - をクリックします。••• （[省略記号（Ellipsis）]）アイコン
   - [このアプライアンスの削除（Remove This Appliance）] を選択します。

3. システム設定を使用したアプライアンスの削除

アプライアンスが Central Management で [設定チャンネルのダウン（Config Channel Down）] または [設定の変更を保留中（Config Changes Pending）] と表示され、解決されない場合は、この手順を実行してください。

要件：sysadmin ユーザー

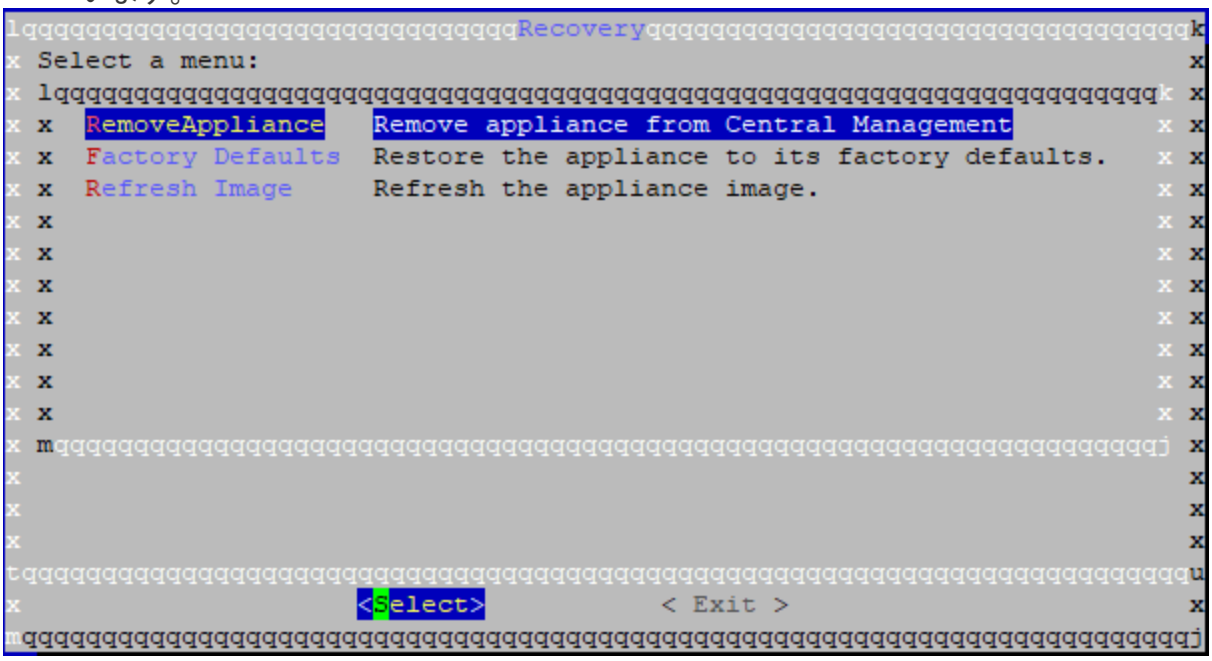
Central Management から削除したときにアプライアンスのステータスが [アップ(Up)] と表示された場合は、この手順を省略できます。「**4. 証明書の再生成**」に進みます。

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。
   - 最初：Flow Collector、Flow Sensor、および UDP Director に最初にログインします。
   - 最後：(必要に応じて他のすべてのアプライアンスで手順 1 ～ 5 を完了した後) 最後にマネージャ にログインします。

Central Management から最後に マネージャ を削除します。

2. **SystemConfig** と入力します。Enter を押します。
3. メインメニューから [リカバリ(Recovery)] を選択します。
4. [アプライアンスの削除(RemoveAppliance)] を選択します。

   メニューが表示されない場合、アプライアンスはすでに Central Management から削除されています。



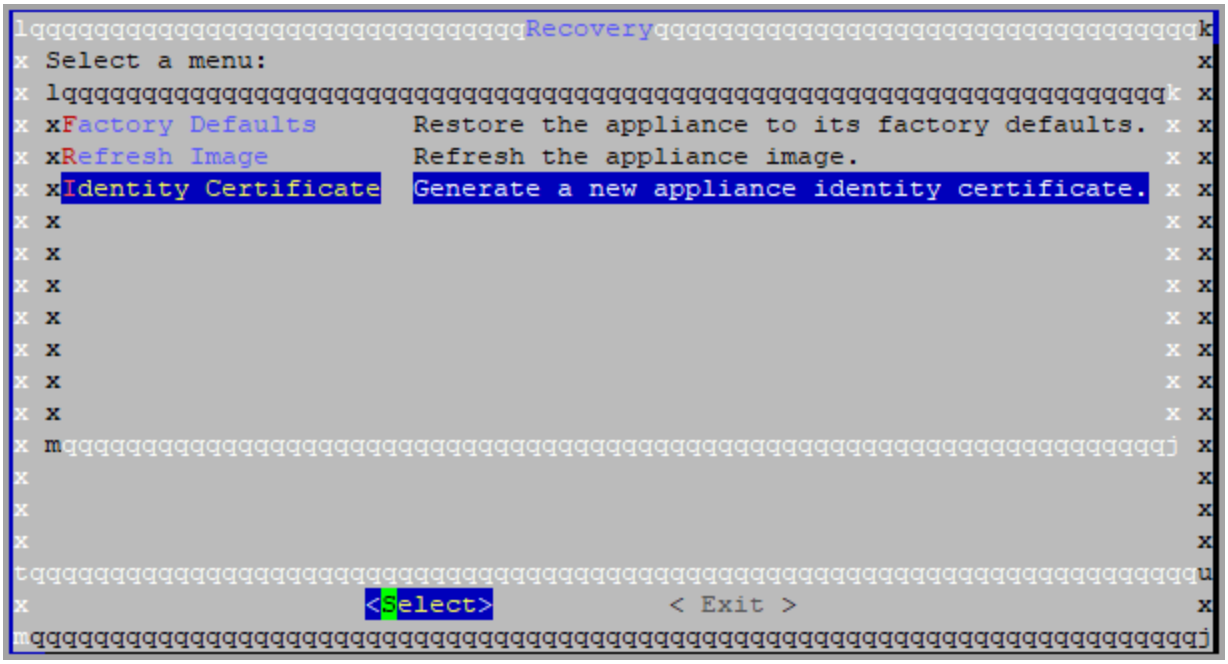
5. 画面に表示される指示に従ってアプライアンスを削除します。
6. 各アプライアンスで手順 1 ～ 5 を繰り返して、Central Management からアプライアンスを削除します。

4. 証明書の再生成

次の手順を実行して新しい有効期限を入力し、各アプライアンスで証明書を再生成します。

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. **SystemConfig** と入力します。Enter を押します。
3. メインメニューから [リカバリ(Recovery)] を選択します。

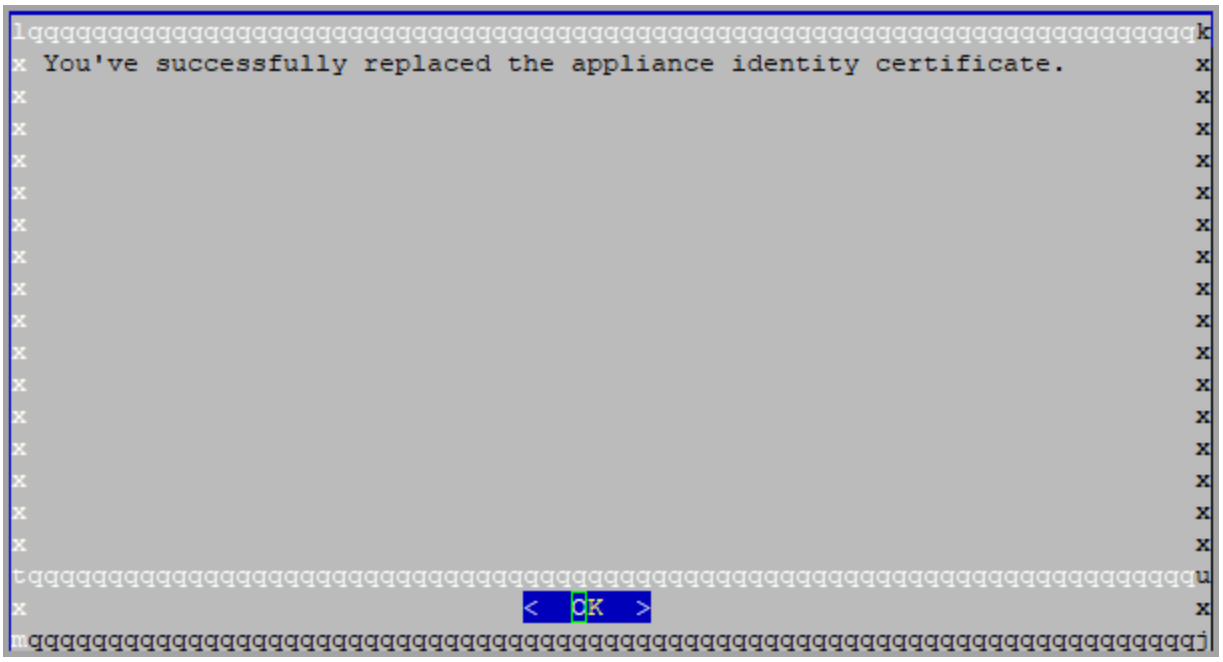
4. [アイデンティティ証明書(Identity Certificate)]を選択します。画面に表示される指示に従って、削除を確認します。



> [アイデンティティ証明書(Identity Certificate)]メニューが表示されない場合は、[Central Management]からアプライアンスを削除します。手順については、「**2. Central Management を使用したアプライアンスの削除**」と「**3. システム設定を使用したアプライアンスの削除**」を参照してください。

5. 1 ～ 5 年の有効期間を入力します。
6. [OK]をクリックします。

   証明書が正常に置き換えられたことを確認するまで待ちます。[OK]をクリックしてコンソールを閉じます。



7. 各アプライアンスで手順 1 ～ 6 を繰り返します。

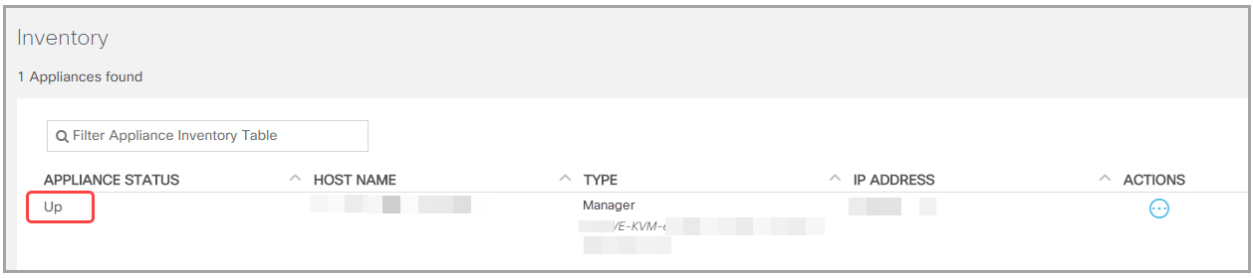
5. Central Management への マネージャ の登録

次の手順を実行し、アプライアンス セットアップ ツールを使用して マネージャ を登録します。IP アドレス、ホスト名などのアプライアンス設定が保持されていることに注意してください。

マネージャ フェールオーバー：2 つの Manager がある場合は、プライマリ マネージャ でこの手順を実行するだけです。セカンダリ マネージャ を登録します。「**6. Central Management へのアプライアンスの追加**」で、セカンダリ SMC を登録します。

> ⚠ この手順の一環としてホスト情報（IPアドレス、ホスト名、またはドメイン名）を変更することは推奨されません。詳細については、「ホスト情報」を参照してください。

1. マネージャ に管理者としてログインします（https://<IPAddress>）。
2. [続行/次へ（Continue/Next）] をクリックし、[アプライアンスの登録（Register Your Appliance）] タブまでスクロールします。
3. [再起動して続行（Restart and Proceed）] をクリックします。画面に表示される指示に従って マネージャ を再起動します。
4. マネージャ に再度ログインします。
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。
   - Central Management が マネージャ にインストールされます。
   - マネージャ 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. アプライアンスのセットアップが完了したら、[Central Management] でインベントリを確認します。マネージャ 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。



6. Central Management へのアプライアンスの追加

アプライアンス セットアップ ツールを使用して、別のアプライアンスを Central Management に追加します。

- **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。
- Central Management：マネージャ IP アドレス、マネージャ パスワード、および Secure Network Analytics ドメインが必要です。
- **順序**：「アプライアンスの設定順序」に従います。
- **アクセス**：Central Management にアクセスするには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.	UDP Director （別名 FlowReplicators）	
2.	Flow Collector 5000 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。
3.	Flow Collector 5000 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。
4.	その他のすべての Flow Collector （NetFlow および sflow）	
5.	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。

6.	Secondary マネージャ （使用する場合）	セカンダリ マネージャ の設定を開始する前に、プライマリ マネージャ が [アップ（Up）] として表示されていることを確認します。 セカンダリ マネージャ 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。手順については、「**8. マネージャ フェールオーバーペアの設定**」を参照してください。

アプライアンス セットアップ 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。IP アドレス、ホスト名などのアプライアンス設定が保持されていることに注意してください。

> ⚠ この手順の一環としてホスト情報（IPアドレス、ホスト名、またはドメイン名）を変更することは推奨されません。詳細については、「ホスト情報」を参照してください。

1. ブラウザのアドレスフィールドに、https:// に続けてアプライアンスの IP アドレスを入力します。

   - **アップ**：次のアプライアンスを Central Management に追加する前に、各アプライアンスが [アップ（Up）] 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。

2. **セカンダリ マネージャ**：次のログイン情報を入力してログインします。
   - **ユーザー名**：admin
   - **パスワード**：lan411cope

   その他のすべてのアプライアンス：手順 4 に進みます。

3. **セカンダリ マネージャ**：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ー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。

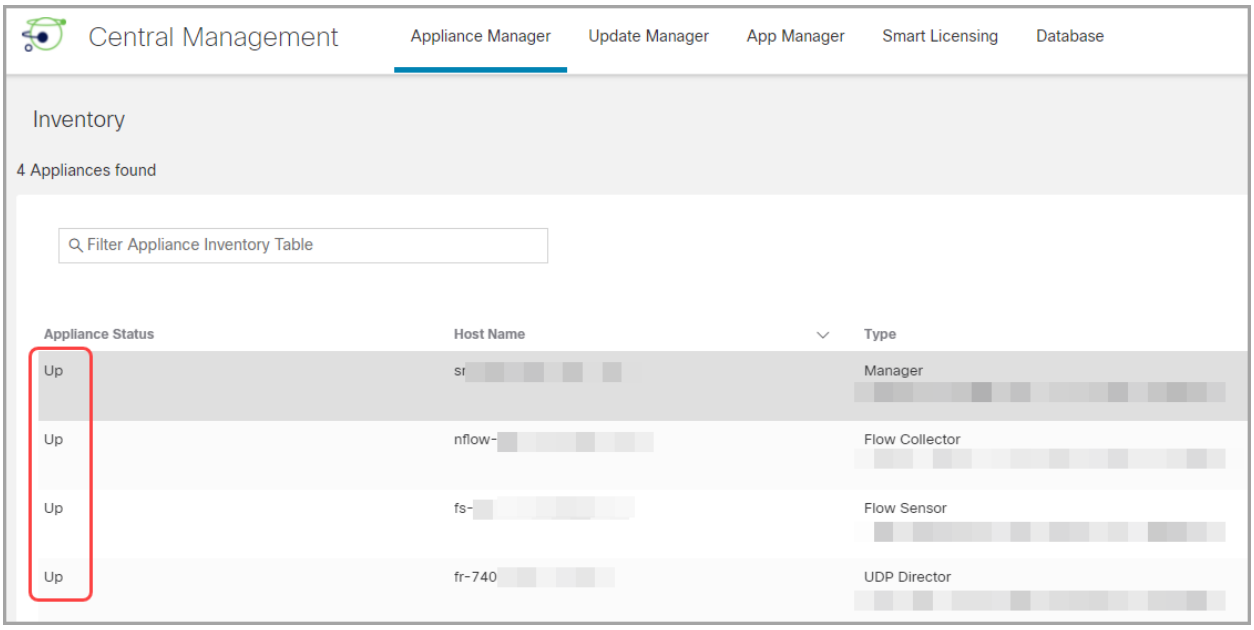
ユーザー	デフォルト パスワード
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

4. [次へ(Next)]をクリックし、[Central Management]タブまたは[アプライアンスの登録(Register Your Appliance)]タブ(セカンダリ マネージャ のみ)までスクロールします。
5. 次の手順に従って、アプライアンスを Central Management に登録します。
   - **セカンダリ マネージャ**:セカンダリ マネージャ がある場合は、それ自体が Central Manager として選択します。Secure Network Analytics ドメインを選択し、その他の必要な情報を入力します。アプライアンス セットアップ ツールですべてのアプライアンスを設定した後にフェールオーバーを設定します。手順については、「**8. マネージャ フェールオーバーペアの設定**」を参照してください。
   - **その他のすべてのアプライアンス**:プライマリ マネージャ の IP アドレスを入力します。**[保存(Save)]**をクリックします。画面に表示される指示に従って、プライマリ マネージャ アプライアンスのアイデンティティ証明書を信頼し、マネージャ の管理者ユーザー名とパスワードを入力します。Secure Network Analytics ドメインを選択し、その他の必要な情報を入力します。

> アプライアンスによっては、メニューが異なる場合があります。たとえば、Flow Sensor を設定する場合は、Flow Collector を選択します。

6. アプライアンスのセットアップが完了したら、[Central Management]でインベントリを確認します。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[初期化中(Initializing)]または[設定の変更を保留中(Config Changes Pending)]から[アップ(Up)]に変化します。プライマリ マネージャ と各アプライアンスが[アップ(Up)]と表示されていることを確認してから、次のアプライアンスを Central Management に追加します(設定の順序と詳細を使用)。



7. 手順 1 ～ 6 を繰り返して各アプライアンスを Central Management に追加します。

7. 信頼ストアからの古い証明書の削除

各アプライアンスの信頼ストアから期限切れの証明書や古い証明書を削除します。各アプライアンス アイデンティティ証明書の保存場所の詳細については、「**信頼ストアの場所**」を参照してください。

> ⚠ 無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。

1. アプライアンスの ••• ([省略記号(Ellipsis)])アイコン 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. **[全般(General)]** タブを選択します。
4. [信頼ストア(Trust Store)] リストを確認します。アプライアンス、マネージャ、およびその他のアプライアンスのすべての期限切れ証明書(アイデンティティ、ルート、および中間証明書)を見つけます。
5. [削除(Delete)] をクリックして古い証明書それぞれを削除します。
6. [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。
7. Central Management のインベントリで、アプライアンスと マネージャ アプライアンスのステータスが [アップ(Up)] に戻っていることを確認します。
8. 各 Flow Collector、Flow Sensor、および UDP Director で手順 1 ～ 7 を繰り返します。

8. マネージャ フェールオーバーペアの設定

Manager をフェールオーバーペアとして設定するには、フェールオーバー コンフィギュレーション ガイド [英語] の手順に従います。

マネージャ以外の個別のアプライアンス

この手順を実行し、マネージャ 以外の個別のアプライアンス(Flow Collector、Flow Sensor、および UDP Director)の証明書の有効期限を変更します。この手順では、個別のアプライアンスを Central Management から削除し、変更後に Central Management に再度追加します。

> 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。
>
> ⚠ **カスタム証明書を使用するアプライアンス**の場合、アプライアンスでカスタム アプライアンス アイデンティティ証明書を使用するこの手順はサポートされていません。手順については、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。

概要

全体的な手順は次のとおりです。

1. **Central Management からのアプライアンスの削除**
2. **証明書の再生成**
3. **信頼ストアからの古い マネージャ 証明書の削除**
4. **Central Management へのアプライアンスの追加**

> マネージャ 証明書の有効期限を変更する必要がある場合は、「**マネージャ および管理アプライアンス**と管理対象アプライアンス」を参照してください。

1. Central Management からのアプライアンスの削除

次の手順を実行して Central Management からアプライアンスを削除します。

1. Central Management を開きます。
2. [アプライアンスステータス(Appliance Status)] 列を確認します。すべてのアプライアンスが [アップ(Up)] と表示されていることを確認します。
   - 変更するアプライアンスが [アップ(Up)] と表示されていない場合は、後の手順で対処します。
   - マネージャ ステータスが [アップ(Up)] と表示されていない場合は、解決するまで数分間待ちます。
3. Central Management からのアプライアンスを削除するには、次の手順を実行します。

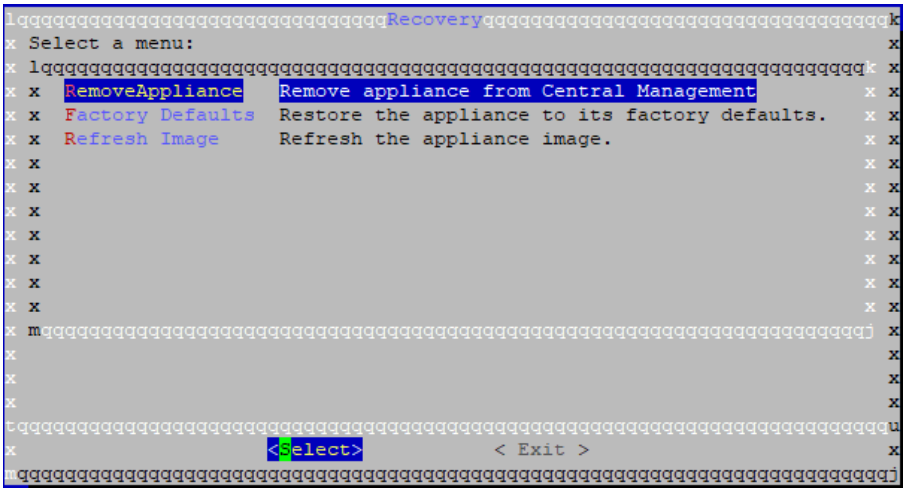
- アプライアンスの ••• ([省略記号(Ellipsis)]) アイコン をクリックします。
- [このアプライアンスの削除(Remove This Appliance)] を選択します。

> Central Management からアプライアンスを削除すると、マネージャ アプライアンスのステータスが [設定の変更を保留中(Config Changes Pending)] から [アップ(Up)] に移行します。

4. マネージャ 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。
5. アプライアンスコンソールに sysadmin としてログインします。
6. **SystemConfig** と入力します。Enter を押します。
7. メインメニューから [リカバリ(Recovery)] を選択します。

8. [アプライアンスの削除(RemoveAppliance)]を選択します。画面に表示される指示に従ってアプライアンスを削除します。

   メニューが表示されない場合、アプライアンスはすでに Central Management から削除されています。

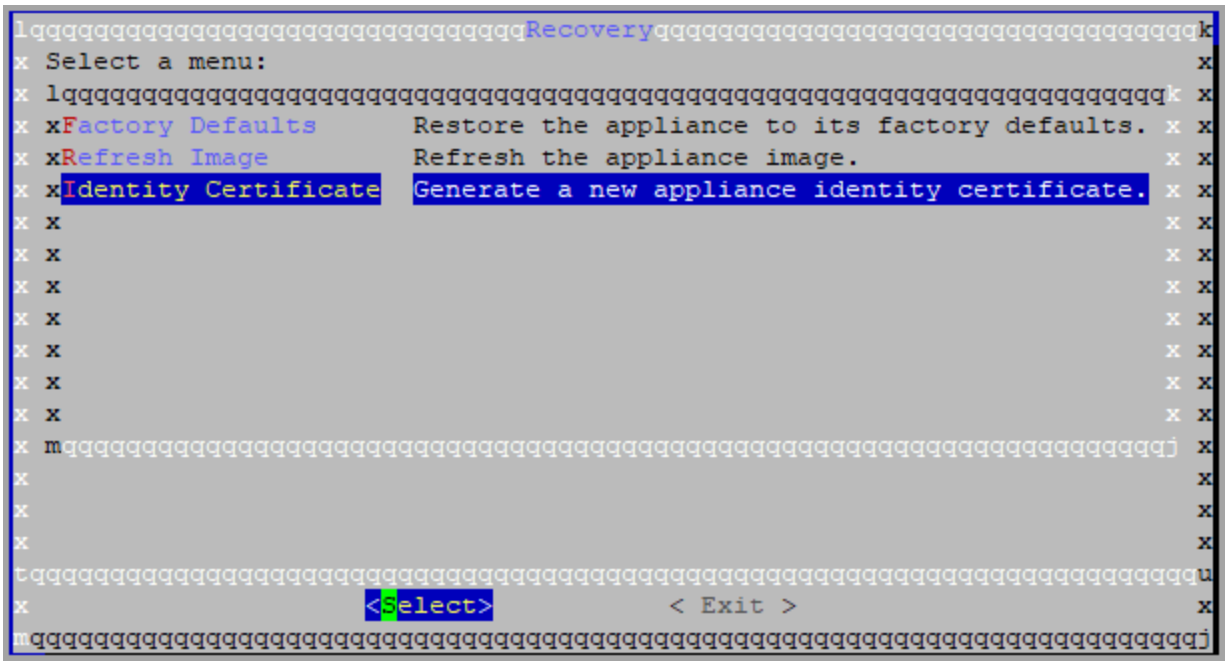


次の手順でシステム設定を続行します。

2. 証明書の再生成

次の手順を実行して新しい有効期限を入力し、証明書を再生成します。

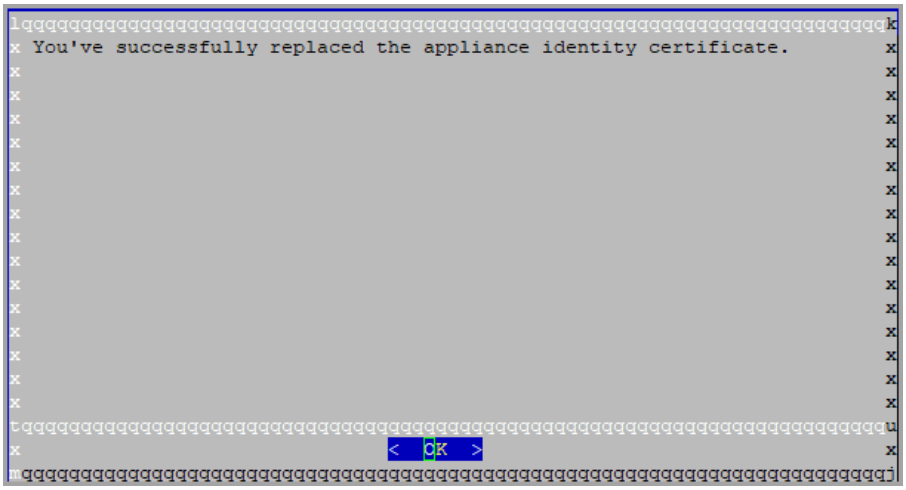
1. [システムの設定(System Config)]のメインメニューから、[リカバリ(Recovery)]を選択します。
2. [アイデンティティ証明書(Identity Certificate)]を選択します。画面に表示される指示に従って、削除を確認します。



> [アイデンティティ証明書(Identity Certificate)] メニューが表示されない場合は、[Central Management] からアプライアンスを削除します。詳細については、「1. Central Management からのアプライアンスの削除」を参照してください。

3. 1 ～ 5 年の有効期間を入力します。
4. [OK] をクリックします。

   証明書が正常に置き換えられたことを確認するまで待ちます。[OK] をクリックしてコンソールを閉じます。



3. 信頼ストアからの古い マネージャ 証明書の削除

次の手順を実行して、期限切れまたは古いアプライアンス証明書を マネージャ 信頼ストアから削除します。

> 無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。

1. Manager に管理者としてログインします(https://<IPAddress>)。
2. Central Management を開きます。
3. マネージャ 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。
4. マネージャ の ••• ([省略記号(Ellipsis)]) アイコンをクリックします。
5. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
6. **[全般(General)]** タブを選択します。
7. [信頼ストア(Trust Store)] リストを確認します。期限切れの証明書(アイデンティティ、ルート、および中間証明書)を見つけます。
8. [削除(Delete)] をクリックして古い証明書それぞれを削除します。
9. [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。
10. Central Management のインベントリで、マネージャ アプライアンスのステータスが [アップ(Up)] に戻っていることを確認します。

4. 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 セットアップ ツールを使用します。IP アドレス、ホスト名などのアプライアンス設定が保持されていることに注意してください。

> ⚠ この手順の一環としてホスト情報（IPアドレス、ホスト名、またはドメイン名）を変更することは推奨されません。詳細については、「ホスト情報」を参照してください。

- Central Management：マネージャ IP アドレス、マネージャ パスワード、および Secure Network Analytics ドメインが必要です。
- **順序**：2 つ以上のアプライアンスを Central Management に追加する場合は、「アプライアンスの設定順序」に従います。
- **アクセス**：Central Management にアクセスするには管理者権限が必要です。

1. ブラウザのアドレス フィールドに、**https://** に続けてアプライアンスの IP アドレスを入力します。
2. [次へ（Next）] をクリックして [Central Management] タブまでスクロールします。
3. 次の手順に従って、アプライアンスを Central Management に登録します。
    - プライマリ マネージャ の IP アドレスを入力します。**[保存（Save）]**をクリックします。
    - 画面に表示される指示に従って、プライマリ マネージャ アプライアンスのアイデンティティ証明書を信頼し、マネージャ の管理者ユーザー名とパスワードを入力します。
    - Secure Network Analytics ドメインを選択し、その他の必要な情報を入力します。

> ℹ アプライアンスによっては、メニューが異なる場合があります。たとえば、Flow Sensor を設定する場合は、Flow Collector を選択します。

4. アプライアンスのセットアップが完了したら、[Central Management] でインベントリを確認します。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 [初期化中（Initializing）] または [設定の変更を保留中（Config Changes Pending）] から [アップ（Up）] に変化します。アプライアンスが [アップ（Up）] に変化しない場合は、信頼ストアに古い証明書または重複している証明書が存在する可能性があります。詳細については、「**トラブルシューティング**」と「**信頼ストアからの証明書の削除**」を参照してください。

期限切れになったシスコのデフォルト証明書の置換

各 Secure Network Analytics アプライアンスは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。次の手順を実行して、**期限切れ**のアプライアンス アイデンティティ証明書の有効期限を変更します。

- **ホスト情報**:アプライアンスのホスト情報(IPアドレス、ホスト名、ドメイン名)は保持されます。有効期限に加えてホスト情報を変更する必要がある場合は、(このセクションの手順ではなく)「**ネットワーク インターフェイスの変更**」または「**ホスト名またはネットワークドメイン名の変更**」の手順を実行します。
- **カスタム証明書**:カスタム アプライアンス アイデンティティ証明書を使用するアプライアンスでは、この手順はサポートされません。手順については、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。

> 証明書が期限切れになっていない場合は、「**期限切れになっていないシスコのデフォルトの証明書の置換**」を参照してください。アプライアンスが認証局からのカスタム証明書を使用する場合は、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。

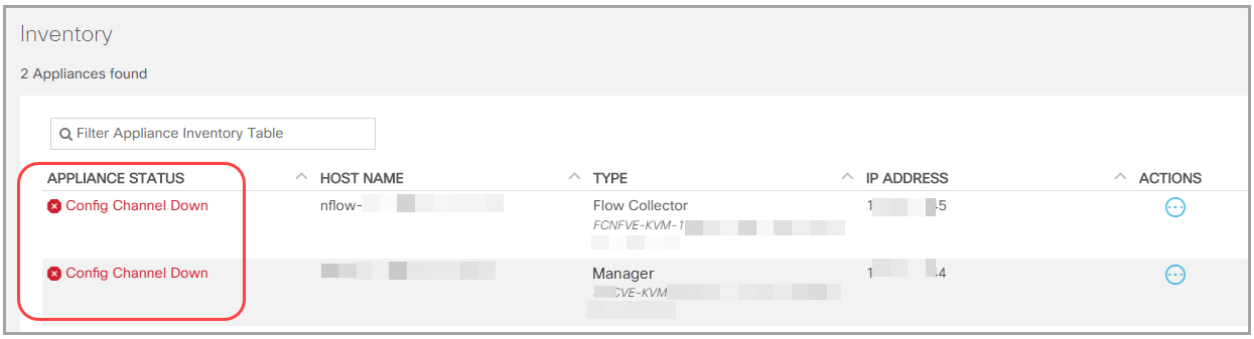
要件

開始する前に、「はじめに」の「**ベストプラクティス**」を確認し、次の要件を確認します。

- **ユーザー**:admin と sysadmin のユーザーアクセス権が必要です。
- **マネージャ フェールオーバー**:Manager がフェールオーバーペアとして設定されている場合にマネージャ 証明書を更新するには、次の手順を開始する前にフェールオーバーの関係を削除します。手順については、フェールオーバー コンフィギュレーション ガイド [英語] を参照してください。フェールオーバーペアを削除すると、セカンダリ マネージャ がクラスタから削除されます。この手順には、セカンダリ マネージャ を工場出荷時のデフォルトにリセットする手順が含まれています。

1. アプライアンスのステータスの確認

1. プライマリ マネージャ 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. [アプライアンスステータス(Appliance Status)] 列を確認します。アプライアンスのステータスが [設定チャネルのダウン(Config Channel Down)] と表示されている場合は、証明書の有効期限が切れています。



2. アプライアンスの手順の選択

- **マネージャと管理対象アプライアンス**：**マネージャ および管理アプライアンス**を使用して、クラスタ内の マネージャ とその他の管理対象アプライアンスの証明書の有効期限を変更します。手順の一部として、Central Management からすべてのアプライアンスを（示されている順序で）削除し、変更後にクラスタを再構築します。
- **マネージャ 以外の個別のアプライアンス**：**マネージャ以外の個別のアプライアンス**を使用して、マネージャ 以外のアプライアンス（Flow Collector、Flow Sensor、および UDP Director）の証明書の有効期限を変更します。この手順では、個別のアプライアンスを Central Management から削除し、変更後に Central Management に再度追加します。

マネージャ および管理アプライアンス

次の手順に従って、クラスタ内の マネージャ とその他の管理対象アプライアンスの証明書の有効期限を変更します。手順の一部として、Central Management からすべてのアプライアンスを（示されている順序で）削除し、変更後にクラスタを再構築します。

マネージャ フェールオーバー：Manager がフェールオーバーペアとして設定されている場合は、これらの手順を開始する前に、フェールオーバーの関係を削除します。手順については、フェールオーバー コンフィギュレーション ガイド [英語] を参照してください。フェールオーバーペアを削除すると、セカンダリ マネージャ がクラスタから削除されます。この手順には、セカンダリ マネージャ を工場出荷時のデフォルトにリセットする手順が含まれています。

> 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。
>
> ⚠ **カスタム証明書を使用するアプライアンス**の場合、アプライアンスでカスタム アプライアンス アイデンティティ証明書を使用するこの手順はサポートされていません。手順については、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。

概要

全体的な手順は次のとおりです。

1. **アプライアンスの削除と証明書の再生成**
2. **Central Management への マネージャ の登録**
3. **マネージャ 信頼ストアからの期限切れ証明書の削除**
4. **Central Management へのアプライアンスの追加**

1. アプライアンスの削除と証明書の再生成

次の手順に従って、クラスタ内の マネージャ とその他の管理対象アプライアンスの証明書の有効期限を変更します。指定した順序ですべてのアプライアンスを Central Management から削除してください。

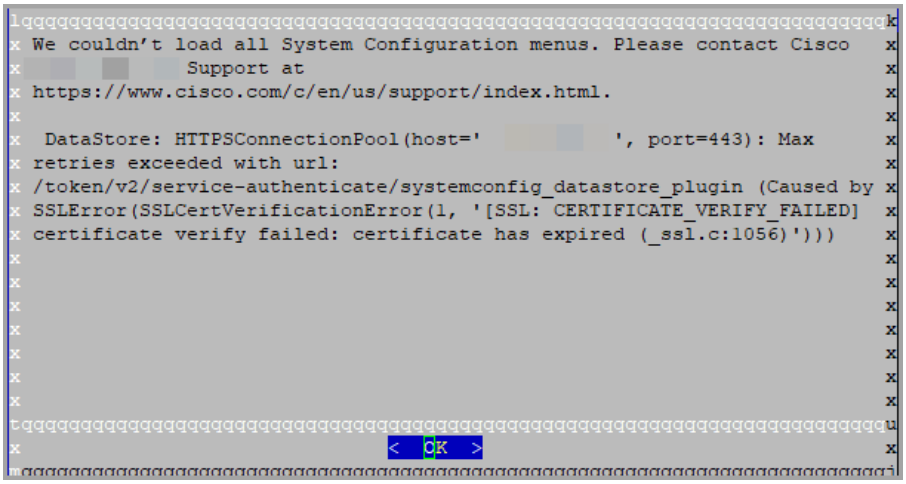
> マネージャ を変更するだけの場合は、すべてのアプライアンスを Central Management から削除する必要があります。マネージャ 以外の個別のアプライアンスのみを変更する必要がある場合は、「**マネージャ以外の個別のアプライアンス**を参照してください。

- 最初：すべての Flow Collector、Flow Sensor、および UDP Director で次の手順を実行します。
- 最後：マネージャ で最後にこれらの手順を実行します。
- **デフォルトの有効期間**：再生成された証明書のデフォルトは 5 年です。ただし、この期間は後の手順で変更できます。

> Central Management から最後に マネージャ を削除します。

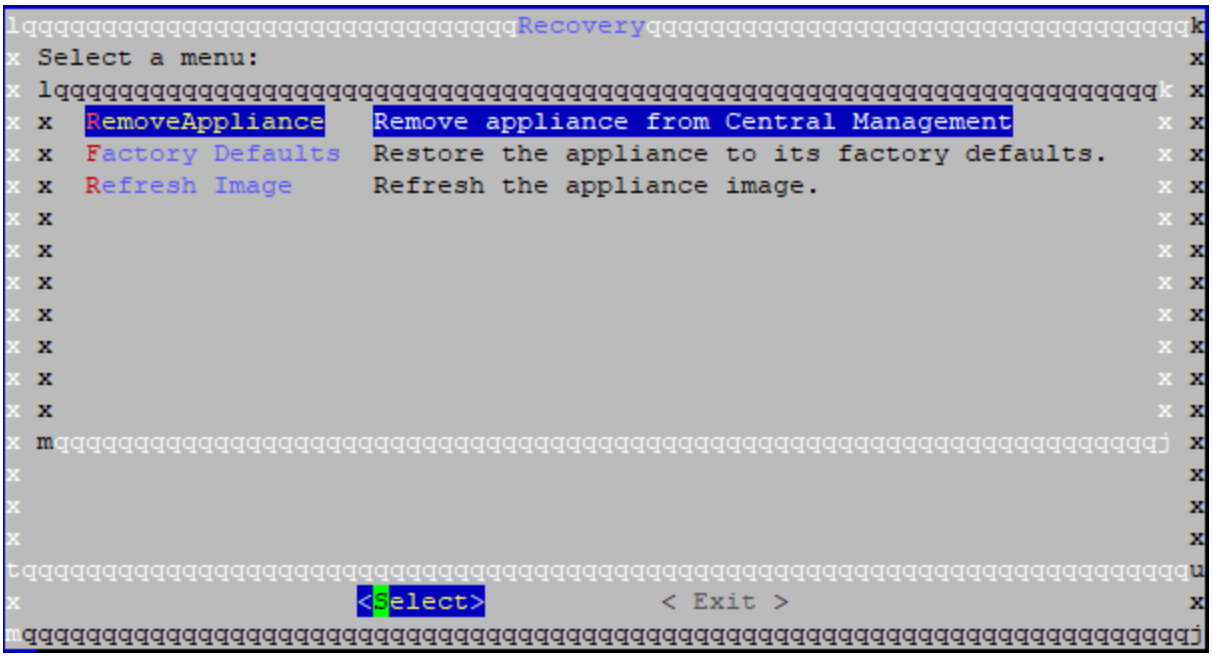
1. Central Management からのアプライアンスの削除：アプライアンスの ••• ([省略記号(Ellipsis)])アイコン をクリックします。[このアプライアンスの削除(Remove This Appliance)]を選択します。
   - 最初：Flow Collector、Flow Sensor、および UDP Director を最初に削除します。
   - 最後：他のすべてのアプライアンスで手順 1 ～ 9 を実行した後、プライマリ マネージャ を削除します。
2. アプライアンスコンソールに sysadmin としてログインします。
   - 最初：Flow Collector、Flow Sensor、および UDP Director に最初にログインします。
   - 最後：他のすべてのアプライアンスで手順 1 ～ 9 を実行した後、プライマリ マネージャ にログインします。
3. **SystemConfig** と入力します。Enter を押します。

   Manager：マネージャ にログインし、すべてのシステム設定のメニューをロードできなかったと

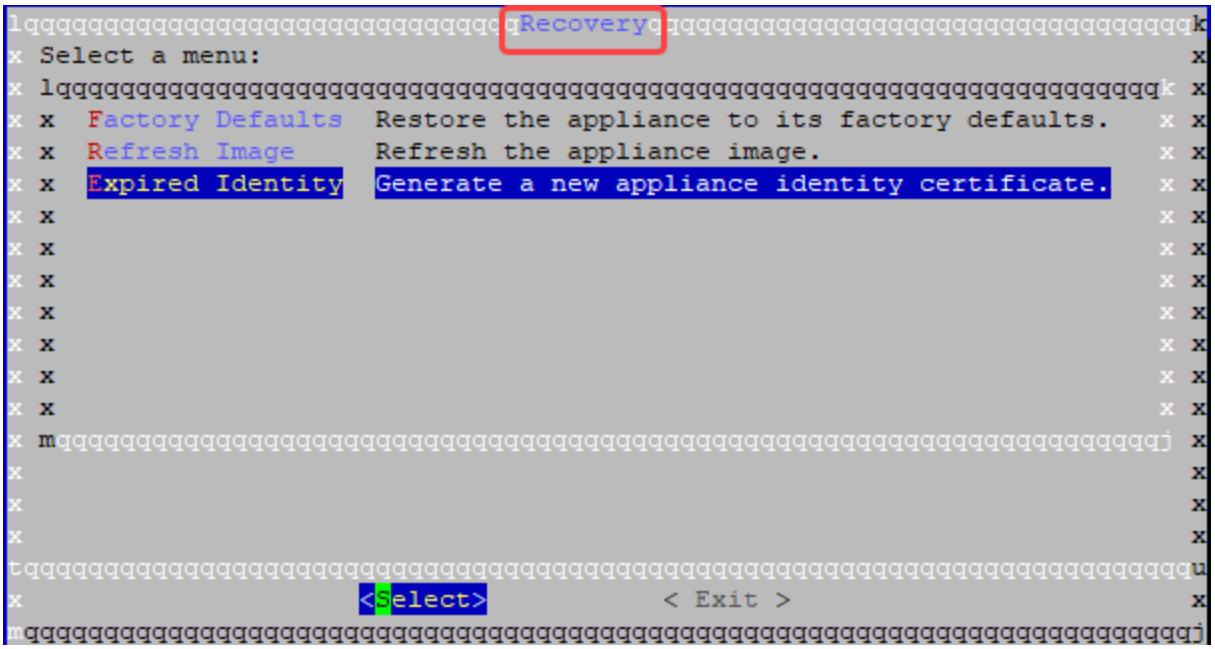


4. メインメニューから [リカバリ(Recovery)] を選択します。
5. [アプライアンスの削除(RemoveAppliance)] を選択します。

   メニューが表示されない場合、アプライアンスはすでに Central Management から削除されています。

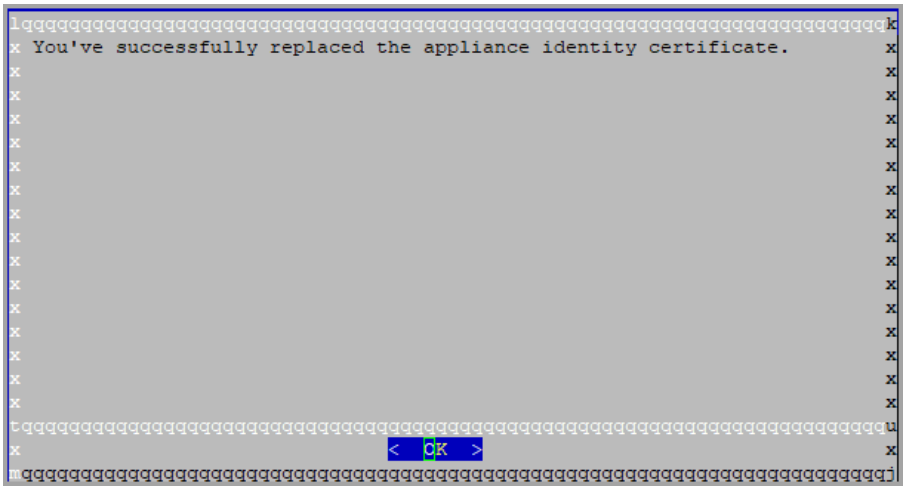


6. 画面に表示される指示に従ってアプライアンスを削除します。
7. [リカバリ(Recovery)] メニューから、[期限切れのアイデンティティ(Expired Identity)] を選択します。画面に表示される指示に従って、削除を確認します。



8. 証明書が正常に置き換えられたことを確認するまで待ちます。

   - **終了**：[OK] をクリックしてコンソールを閉じます。
   - **証明書の有効期限の変更（オプション）**：証明書の有効期限はデフォルトで 5 年です。有効期限を変更するには、[OK] をクリックして [リカバリ（Recovery）] メニューに戻ります。[アイデンティティ証明書（Identity Certificate）] を選択し、画面に表示される指示に従って 1 ～ 5 年の有効期限を入力します。証明書が正常に置き換えられたことを確認するまで待ちます。



9. 各アプライアンスで手順 1 ～ 8 を繰り返します。

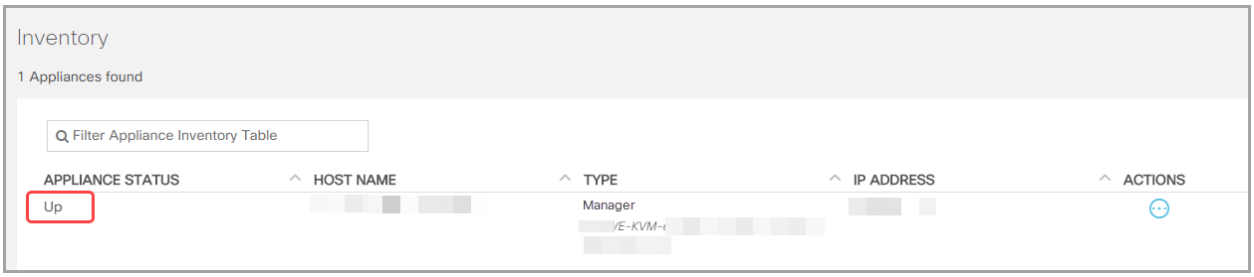
2. Central Management への マネージャ の登録

次の手順を実行し、アプライアンス セットアップ ツールを使用して マネージャ を登録します。IP アドレス、ホスト名などのアプライアンス設定が保持されていることに注意してください。

マネージャ フェールオーバー：2 つの Manager がある場合は、プライマリ マネージャ でこの手順を実行するだけです。セカンダリ マネージャ を登録します。「**4. Central Management へのアプライアンスの追加**」で、セカンダリ SMC を登録します。

> ⚠ この手順の一環としてホスト情報（IPアドレス、ホスト名、またはドメイン名）を変更することは推奨されません。詳細については、「ホスト情報」を参照してください。

1. マネージャ に管理者としてログインします（https://<IPAddress>）。
2. [続行/次へ（Continue/Next）] をクリックし、[アプライアンスの登録（Register Your Appliance）] タブまでスクロールします。
3. [再起動して続行（Restart and Proceed）] をクリックします。画面に表示される指示に従ってマネージャ を再起動します。
4. マネージャ に再度ログインします。
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。
   - Central Management が マネージャ にインストールされます。
   - マネージャ 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. アプライアンスのセットアップが完了したら、[Central Management] でインベントリを確認します。マネージャ 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。



3. マネージャ 信頼ストアからの期限切れ証明書の削除

Manager が 2 つある場合は、プライマリ マネージャ のみでこの手順を実行する必要があります（セカンダリ マネージャ は工場出荷時のデフォルトにリセットされたため）。

> ⚠ 無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。

1. マネージャ の ••• （[省略記号（Ellipsis）]）アイコンをクリックします。
2. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
3. **[全般（General）]** タブを選択します。
4. [信頼ストア（Trust Store）] リストを確認します。マネージャ と マネージャ 以外のその他のアプライアンスのすべての期限切れ証明書（アイデンティティ、ルート、および中間証明書）を見つけます。
5. [削除（Delete）] をクリックして古い証明書それぞれを削除します。
6. [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。

7. Central Management のインベントリで、マネージャ アプライアンスのステータスが [アップ（Up）] に戻っていることを確認します。

4. Central Management へのアプライアンスの追加

アプライアンス セットアップ ツールを使用して、別のアプライアンスを Central Management に追加します。

- **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。
- Central Management：マネージャ IP アドレス、マネージャ パスワード、および Secure Network Analytics ドメインが必要です。
- **順序**：「アプライアンスの設定順序」に従います。
- **アクセス**：Central Management にアクセスするには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。

	アプライアンス	詳細
1.	UDP Director （別名 FlowReplicators）	
2.	Flow Collector 5000 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。
3.	Flow Collector 5000 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。
4.	その他のすべての Flow Collector （NetFlow および sflow）	
5.	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。
6.	Secondary マネージャ （使用する場合）	セカンダリ マネージャ の設定を開始する前に、プライマリ マネージャ が [アップ（Up）] として表示されていることを確認します。 セカンダリ マネージャ 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。手順については、「**6. マネージャ フェールオーバーペアの設定**」を参照してください。

アプライアンス セットアップ 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。IP アドレス、ホスト名などのアプライアンス設定が保持されていることに注意してください。

> ⚠ この手順の一環としてホスト情報（IPアドレス、ホスト名、またはドメイン名）を変更することは推奨されません。詳細については、「ホスト情報」を参照してください。

1. ブラウザのアドレスフィールドに、https:// に続けてアプライアンスの IP アドレスを入力します。

   - **アップ**：次のアプライアンスを Central Management に追加する前に、各アプライアンスが［アップ（Up）］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。

2. **セカンダリ マネージャ**：次のログイン情報を入力してログインします。
   - **ユーザー名**：admin
   - **パスワード**：lan411cope

   その他のすべてのアプライアンス：手順 4 に進みます。

3. **セカンダリ マネージャ**：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ー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。

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

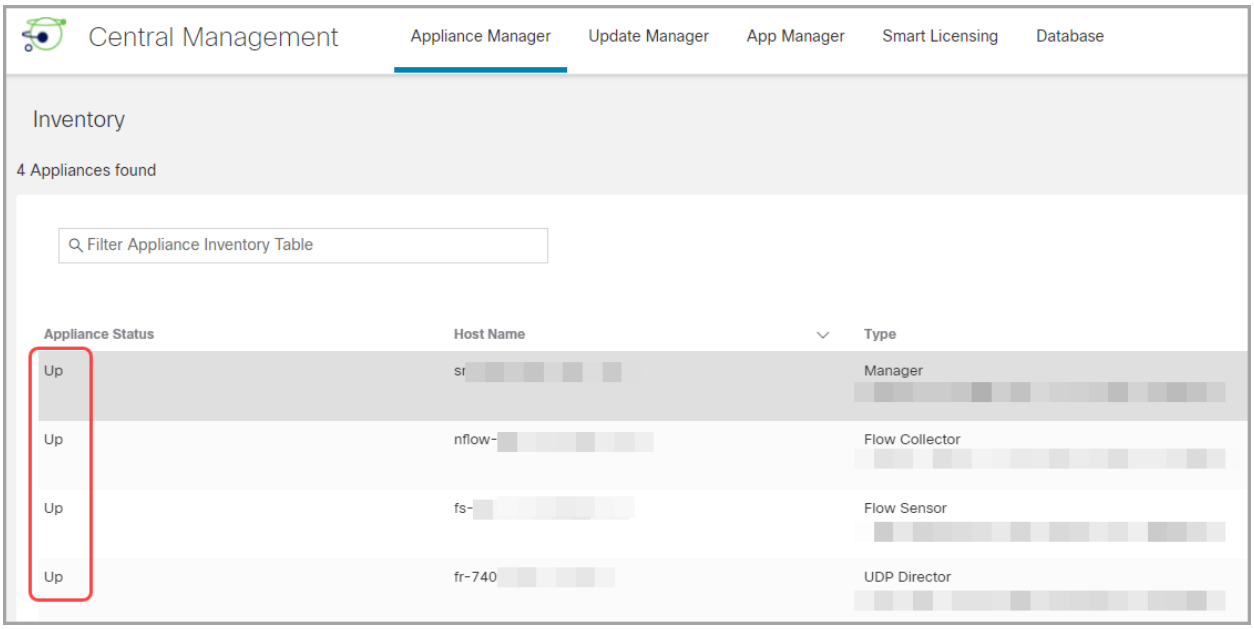
4. ［次へ（Next）］をクリックし、［Central Management］タブまたは［アプライアンスの登録（Register Your Appliance）］タブ（セカンダリ マネージャ のみ）までスクロールします。
5. 次の手順に従って、アプライアンスを Central Management に登録します。
   - **セカンダリ マネージャ**：セカンダリ マネージャ がある場合は、それ自体が Central Manager として選択します。Secure Network Analytics ドメインを選択し、その他の必要な情報を入力します。アプライアンス セットアップ ツールですべてのアプライアンスを設定した後にフェールオーバーを設定します。手順については、「**6. マネージャ フェールオーバーペアの設定**」を参照してください。

- **その他のすべてのアプライアンス**：プライマリ マネージャ の IP アドレスを入力します。**[保存（Save）]**をクリックします。画面に表示される指示に従って、プライマリ マネージャ アプライアンスのアイデンティティ証明書を信頼し、マネージャ の管理者ユーザー名とパスワードを入力します。Secure Network Analytics ドメインを選択し、その他の必要な情報を入力します。

アプライアンスによっては、メニューが異なる場合があります。たとえば、Flow Sensor を設定する場合は、Flow Collector を選択します。

6. アプライアンスのセットアップが完了したら、[Central Management] でインベントリを確認します。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 [初期化中（Initializing）] または [設定の変更を保留中（Config Changes Pending）] から [アップ（Up）] に変化します。プライマリ マネージャ と各アプライアンスが [アップ（Up）] と表示されていることを確認してから、次のアプライアンスを Central Management に追加します（設定の順序と詳細を使用）。



7. 手順 1 ～ 6 を繰り返して各アプライアンスを Central Management に追加します。

5. 信頼ストアからの期限切れ証明書の削除

各アプライアンスの信頼ストアから期限切れの証明書や古い証明書を削除します。各アプライアンス アイデンティティ証明書の保存場所の詳細については、「**信頼ストアの場所**」を参照してください。

無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。

1. アプライアンスの ••• （[省略記号（Ellipsis）]）アイコン 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. **[全般（General）]** タブを選択します。

4. [信頼ストア(Trust Store)]リストを確認します。アプライアンス、マネージャ、およびその他のアプライアンスのすべての期限切れ証明書(アイデンティティ、ルート、および中間証明書)を見つけます。
5. [削除(Delete)]をクリックして古い証明書それぞれを削除します。
6. [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。
7. Central Management のインベントリで、アプライアンスと マネージャ アプライアンスのステータスが [アップ(Up)] に戻っていることを確認します。
8. 各 Flow Collector、Flow Sensor、および UDP Director で手順 1 ～ 7 を繰り返します。

6. マネージャ フェールオーバーペアの設定

Manager をフェールオーバーペアとして設定するには、フェールオーバー コンフィギュレーション ガイド [英語] の手順に従います。

マネージャ以外の個別のアプライアンス

次の手順に従って、マネージャ 以外の個別のアプライアンス(Flow Collector、Flow Sensor、または UDP Director)の証明書の有効期限を変更します。この手順では、個別のアプライアンスを Central Management から削除し、変更後に Central Management に再度追加します。

デフォルトの有効期間:再生成された証明書のデフォルトは 5 年です。ただし、この期間は後の手順で変更できます。

> 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。
>
> ⚠ **カスタム証明書を使用するアプライアンス**の場合、アプライアンスでカスタム アプライアンス アイデンティティ証明書を使用するこの手順はサポートされていません。手順については、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」を参照してください。

概要

全体的な手順は次のとおりです。

1. **アプライアンスの削除と証明書の再生成**
2. **マネージャ 信頼ストアからの期限切れ証明書の削除**
3. **Central Management へのアプライアンスの追加**

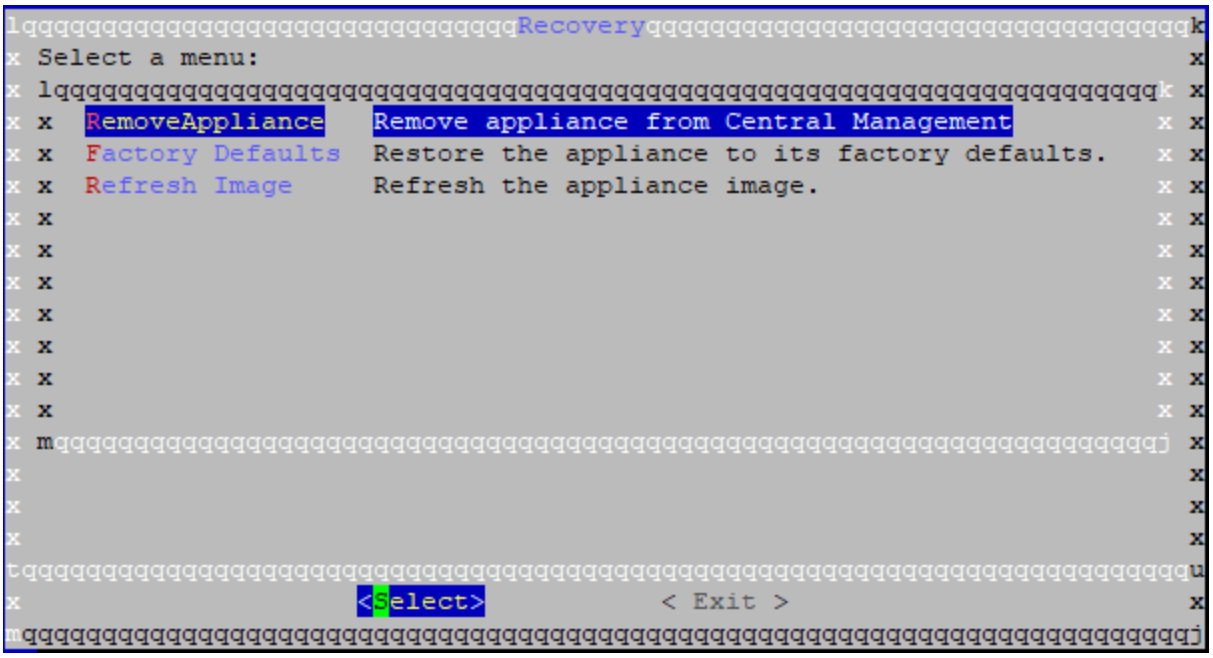
> ℹ マネージャ 証明書の有効期限を変更する必要がある場合は、「**マネージャ および管理アプライアンス**と管理対象アプライアンス」を参照してください。

1. アプライアンスの削除と証明書の再生成

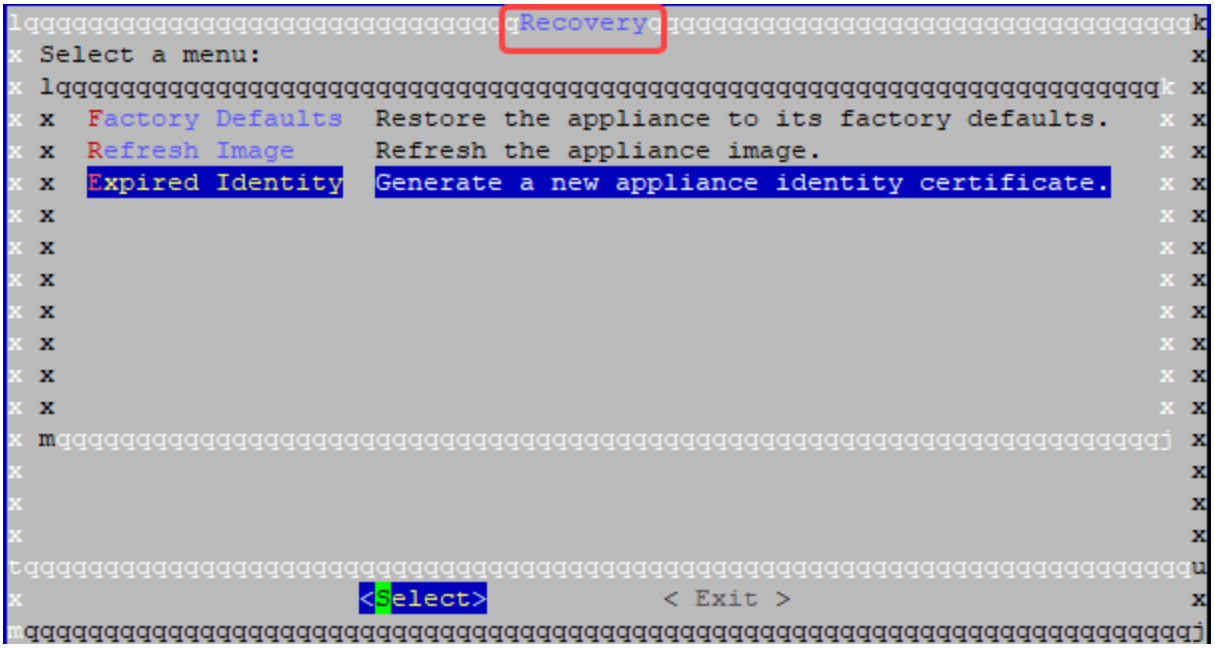
1. **Central Management からのアプライアンスの削除**:アプライアンスの ••• ([省略記号(Ellipsis)])アイコン をクリックします。[このアプライアンスの削除(Remove This Appliance)]を選択します。
2. アプライアンスコンソールに sysadmin としてログインします。
3. **SystemConfig** と入力します。Enter を押します。

4. メインメニューから [リカバリ(Recovery)] を選択します。
5. [アプライアンスの削除(RemoveAppliance)] を選択します。

   メニューが表示されない場合、アプライアンスはすでに Central Management から削除されています。

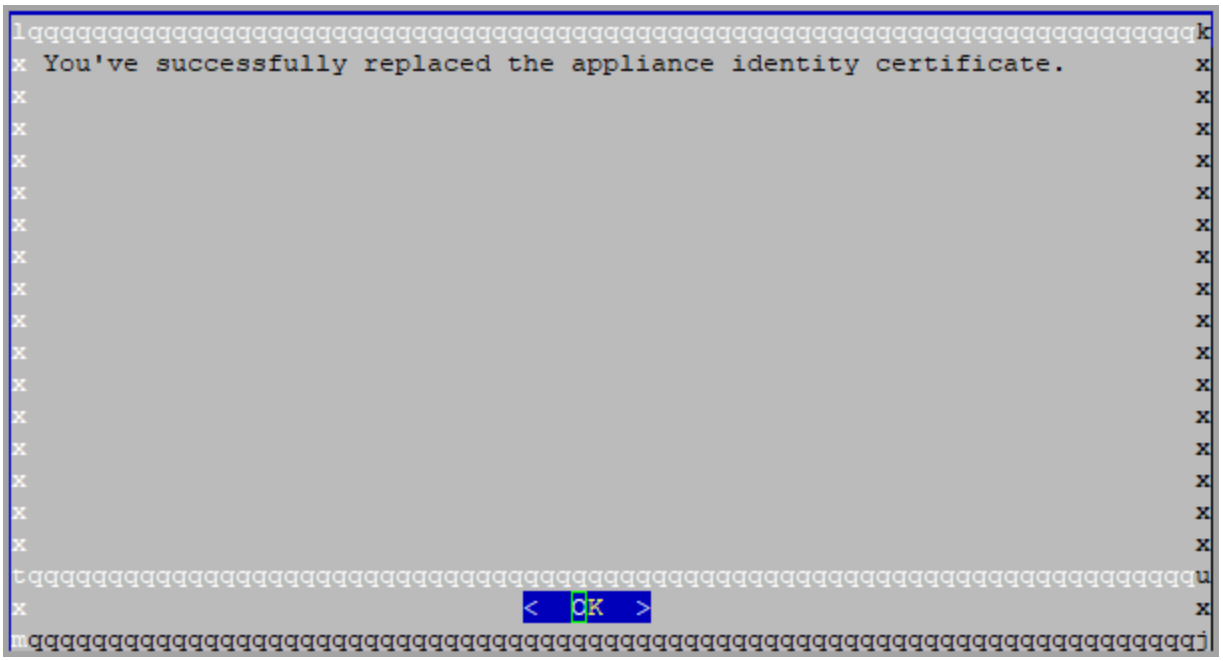


6. 画面に表示される指示に従ってアプライアンスを削除します。
7. [リカバリ(Recovery)] メニューから、[期限切れのアイデンティティ(Expired Identity)] を選択します。画面に表示される指示に従って、削除を確認します。



8. 証明書が正常に置き換えられたことを確認するまで待ちます。

   - **終了**：[OK] をクリックしてコンソールを閉じます。
   - **証明書の有効期限の変更（オプション）**：証明書の有効期限はデフォルトで 5 年です。有効期限を変更するには、[OK] をクリックして [リカバリ（Recovery）] メニューに戻ります。[アイデンティティ証明書（Identity Certificate）] を選択し、画面に表示される指示に従って 1 ～ 5 年の有効期限を入力します。証明書が正常に置き換えられたことを確認するまで待ちます。



9. 各アプライアンスで手順 1 ～ 8 を繰り返します。

2. マネージャ 信頼ストアからの期限切れ証明書の削除

次の手順を実行して、期限切れのアプライアンス証明書を マネージャ 信頼ストアから削除します。

> ⚠ 無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。

1. マネージャ に管理者としてログインします（https://<IPAddress>）。
2. マネージャ 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。
3. マネージャ の ••• （[省略記号（Ellipsis）]）アイコンをクリックします。
4. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
5. **[全般（General）]** タブを選択します。
6. [信頼ストア（Trust Store）] リストを確認します。期限切れの証明書（アイデンティティ、ルート、および中間証明書）を見つけます。
7. [削除（Delete）] をクリックして古い証明書それぞれを削除します。
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. Central Management のインベントリで、マネージャ アプライアンスのステータスが [アップ（Up）] に戻っていることを確認します。

3. 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 セットアップ ツールを使用します。IP アドレス、ホスト名などのアプライアンス設定が保持されていることに注意してください。

> ⚠ この手順の一環としてホスト情報（IPアドレス、ホスト名、またはドメイン名）を変更することは推奨されません。詳細については、「ホスト情報」を参照してください。

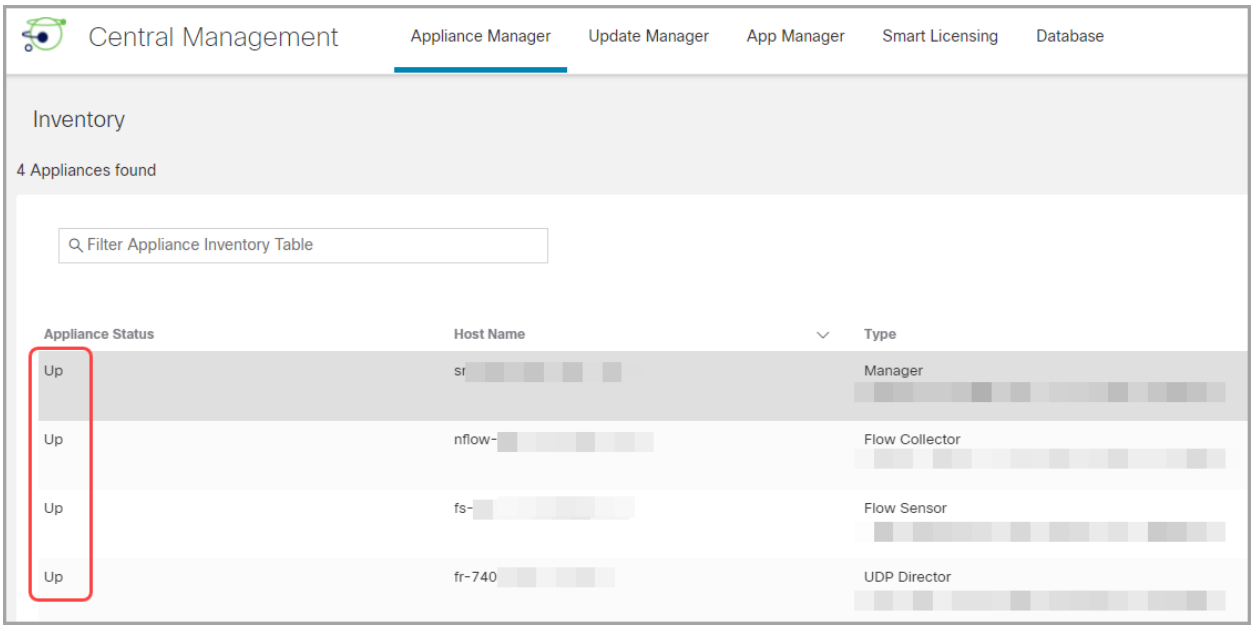
- Central Management：マネージャ IP アドレス、マネージャ パスワード、および Secure Network Analytics ドメインが必要です。
- **順序**：2 つ以上のアプライアンスを Central Management に追加する場合は、「アプライアンスの設定順序」に従います。
- **アクセス**：Central Management にアクセスするには管理者権限が必要です。

1. ブラウザのアドレス フィールドに、**https://** に続けてアプライアンスの IP アドレスを入力します。
2. [次へ（Next）] をクリックして [Central Management] タブまでスクロールします。
3. 次の手順に従って、アプライアンスを Central Management に登録します。
   - プライマリ マネージャ の IP アドレスを入力します。**[保存（Save）]**をクリックします。
   - 画面に表示される指示に従って、プライマリ マネージャ アプライアンスのアイデンティティ証明書を信頼し、マネージャ の管理者ユーザー名とパスワードを入力します。
   - Secure Network Analytics ドメインを選択し、その他の必要な情報を入力します。

> ℹ アプライアンスによっては、メニューが異なる場合があります。たとえば、Flow Sensor を設定する場合は、Flow Collector を選択します。

4. アプライアンスのセットアップが完了したら、[Central Management] でインベントリを確認します。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 [初期化中（Initializing）] または [設定の変更を保留中（Config Changes Pending）] から [アップ（Up）] に変化します。アプライアンスが [アップ（Up）] に変化しない場合は、信頼ストアに古い証明書または重複している証明書が存在する可能性があります。詳細については、「**トラブルシューティング**」と「**信頼ストアからの証明書の削除**」を参照してください。



SSL/TLS アプライアンス アイデンティティ証明書の置換

各 Secure Network Analytics アプライアンスは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。デフォルトの証明書は、認証局からのアプライアンス アイデンティティ証明書に置き換えることができます。

> ⚠ 証明書はシステムのセキュリティにとって重要です。証明書を不適切に変更すると、Secure Network Analytics アプライアンスの通信が停止し、データ損失の原因となります。

証明書の要件

アプライアンス アイデンティティ証明書を置換する場合は、認証局の証明書があることを確認します。ベストプラクティスと証明書の要件については、「はじめに」の「**アプライアンスのアイデンティティ証明書**」を参照してください。

環境に応じた手順の選択

Central Management で**証明書署名要求(CSR)**を生成するか、すでに認証局の証明書がある場合は CSR を省略できます。

- 証明書署名要求を生成するには、「**Central Management での CSR の生成**」に進みます。
- 証明書署名要求を省略するには、「**Central Management での CSR の省略**」に進みます。

Central Management での CSR の生成

Central Management で CSR を生成し、アプライアンス アイデンティティ証明書をカスタムアイデンティティ証明書に置き換えるには、次の手順を実行します。

概要

全体的な手順は次のとおりです。

1. **証明書署名要求の生成**
2. **信頼ストアへの証明書の追加**
3. **アプライアンス アイデンティティ証明書の置換**
4. **デスクトップクライアントの証明書を信頼**

1. 証明書署名要求の生成

次の手順を実行して証明書署名要求(CSR)を準備します。

1. Central Management を開きます。
2. [Appliance Manager] ページで、アプライアンスの ••• ([省略記号(Ellipsis)])アイコン 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. [SSL/TLS アプライアンス アイデンティティ(SSL/TLS Appliance Identity)] セクションに移動します。

5. [アイデンティティの更新(Update Identity)]をクリックします。
6. CSR(証明書署名要求)を生成する必要がある場合は、[はい(Yes)]を選択します。[次へ(Next)]をクリックします。

> CSR を生成する必要がない場合は、「Central Management での CSR の省略」に進みます。

7. 認証局でサポートされる **RSA キーの長さ**を選択します。
8. [CSRの生成(Generate a CSR)] セクションのフィールド(任意)に入力します。
9. [CSR の生成(Generate CSR)]をクリックします。生成プロセスは数分かかることがあります。

   キャンセル:CSR を生成した後、または CA 証明書を待っている間に[キャンセル(Cancel)]をクリックすると、キャンセルされた CSR は無効になります。この場合は新しい CSR を生成します。
10. [CSRのダウンロード(Download CSR)]をクリックします。

    複数のアプライアンス:クラスタ内にあるすべてのアプライアンスのアイデンティティを更新する場合は、アプライアンスごとに手順 1 ～ 10 を繰り返して CSR を生成します。

    キャンセル:CSR を生成した後で[キャンセル(Cancel)]をクリックすると、CSR は無効になり、アプライアンス アイデンティティの更新に使用できなくなります。この場合は新しい CSR を生成します。
11. ダウンロードした CSR を認証局に送信します。

    複数の CSR:同じ認証局にすべての CSR を送信します。

2. 信頼ストアへの証明書の追加

アプライアンス アイデンティティを更新する前に、認証局(CA)証明書を必要な信頼ストアに追加します。

フレンドリ名:新しい証明書に名前を付ける場合、または信頼ストアに追加する場合は、各フレンドリ名が一意であることを確認します。フレンドリ名を重複させないでください。

ファイルに複数の証明書が含まれている場合は、各証明書を信頼ストアに個別にアップロードします。チェーン全体を 1 つの証明書としてアップロードしないでください。

次の証明書をアップロードしてください。

- identity
- chain(ルート証明書と中間証明書)

> アプライアンスの信頼ストアに証明書を追加すると、アプライアンスはそのアイデンティティを信頼し、通信できるようになります。

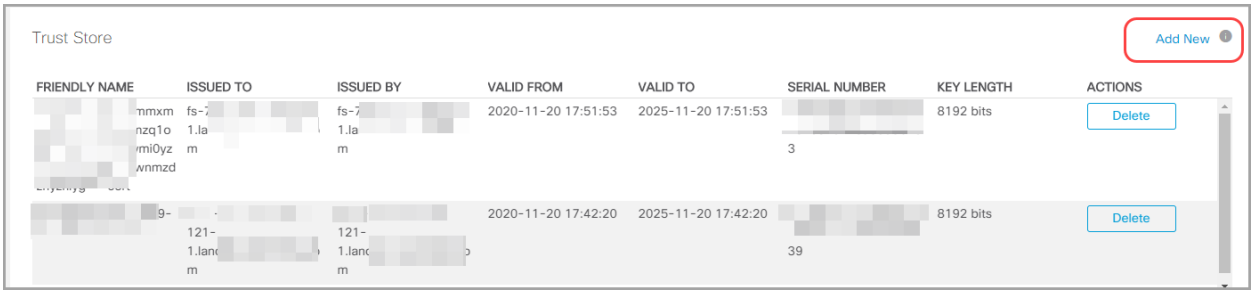
1. Central Management を開きます。
2. [Appliance Manager] ページで、アプライアンスの ••• ([省略記号(Ellipsis)])アイコン をクリックします。

   順序:次の順序でアプライアンスを選択します。

- Flow Collector
- フローセンサー
- UDP Director
- マネージャ

> ⚠ マネージャ 信頼ストアを更新する前に、選択順序に従ってアプライアンスの信頼ストアを更新します。

3. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
4. [全般(General)] タブで、[信頼ストア(Trust Store)] セクションを見つけます。
5. [新規追加(Add New)] をクリックします。



6. [フレンドリ名(Friendly Name)] フィールドに証明書の一意の名前を入力します。
7. [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。
8. [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。
   - **ファイルに複数の証明書が含まれている場合**は、各証明書を信頼ストアに個別にアップロードします。チェーン全体をアップロードしないでください。
   - アプライアンス アイデンティティ証明書と証明書チェーン(該当する場合)をアプライアンス信頼ストア(独自の信頼ストア)と [信頼ストアの要件(Trust Stores Requirements)]**信頼ストアの要件**テーブルに表示されている信頼ストアに追加してください。
9. 各アプライアンスの信頼ストアで手順 1 ～ 9 を繰り返します。

信頼ストアの要件

この表を使用して**アプライアンス アイデンティティと証明書チェーン**(該当する場合)をアプライアンス信頼ストアに追加します。ファイルチェーンに複数の証明書(ルート証明書と中間証明書)が含まれている場合は、各証明書を信頼ストアに個別にアップロードします。チェーン全体を 1 つの証明書としてアップロードしないでください。

アイデンティティ証明書とチェーン証明書を追加する場所を確認するには、[信頼ストアに追加(Add to Trust Stores)] 列を参照してください。

アプライアンス アイデンティティ証明書	詳細	信頼ストアへの追加
/ マネージャ Central Manager	マネージャ 信頼ストアと Central Management 内の各アプライアンスの信頼ストアに マネージャ 証明書を追加します。	• Primary マネージャ • Flow Collector • Flow Collector データベース（5000 シリーズのみ） • Flow Sensor • UDP Director • セカンダリ マネージャ（フェールオーバーのみ）
Secondary マネージャ （フェールオーバーのみ）	Manager がフェールオーバー用に設定されている場合にセカンダリ マネージャ アイデンティティ証明書を置き換えるには、新しいセカンダリ マネージャ 証明書をセカンダリ マネージャ 信頼ストア、プライマリ マネージャ 信頼ストア、および Central Management 内のすべてのアプライアンスの信頼ストアに追加します。 フェールオーバーペアをまだ設定していない場合は、アプライアンス アイデンティティの交換を完了し、フェールオーバー コンフィギュレーション ガイド [英語] を参照してフェールオーバーを設定します。	• Flow Collector • Flow Collector データベース（5000 シリーズのみ） • Flow Sensor • UDP Director • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ
Flow Collector	Flow Collector の証明書を、Flow Collector の信頼ストアとマネージャ の信頼ストアに追加します。 **5000 シリーズのみ**: • Flow Collector エンジン 証明書を Flow Collector データベースの信頼スト	• Flow Collector • Flow Collector データベース（5000 シリーズのみ） • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ

	アに追加します。 • Flow Collector データベース証明書を Flow Collector エンジンの信頼ストアに追加します。	
フローセンサー	Flow Sensor の証明書を Flow Sensor の信頼ストアと マネージャ 信頼ストアに追加します。	• フローセンサー • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ
UDP Director	UDP Director の証明書を UDP Director の信頼ストアと マネージャ 信頼ストアに追加します。	• UDP Director • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ
高可用性ペアの UDP Director	• セカンダリ UDP Director 証明書をプライマリ UDP Director 信頼ストアに追加します。 • プライマリ UDP Director 証明書をセカンダリ UDP Director 信頼ストアに追加します。	• セカンダリ UDP Director（高可用性のみ） • プライマリ UDP Director（高可用性のみ） • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ

3. アプライアンス アイデンティティ証明書の置換

準備：このプロセスでは、各アプライアンスが自動的に再起動するため、アプライアンスでのトラフィック量が比較的少ないタイミングで証明書を更新するよう計画します。

1. Central Management を開きます。
2. [Appliance Manager] ページで、アプライアンスの ••• ([省略記号(Ellipsis)]) アイコン をクリックします。

   複数のアプライアンス：Flow Collector、Flow Sensor、または UDP Director から開始します。
3. [アプライアンス(Appliance)] タブ > [SSL/TLS アプライアンス アイデンティティ(SSL/TLS Appliance Identity)] に戻ります。
4. [フレンドリ名 (Friendly Name)] フィールドに証明書の一意の名前を入力します。
5. [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。

   また、証明書ファイル形式に次の手順を実行します。

- PKCS#12：[バンドルパスワード（Bundle Password）] フィールドにファイルの復号に必要なパスワードを入力します。パスワードは保存されません。
- **PEM**：[証明書チェーンファイル（Certificate Chain File）] フィールドで、認証局（CA）チェーンファイルを個別にアップロードします（[ファイルの選択（Choose File）] をクリックします）。チェーンファイルが正しい順序であり、要件を満たしていることを確認します。詳細については、「はじめに」の「**PEM チェーンファイルの要件**」を参照してください。

> ⚠ チェーンファイルにアプライアンス アイデンティティ証明書を含めないでください。

6. [アイデンティティの置換（Replace Identity）] をクリックします。
7. [設定の適用（Apply settings）] をクリックします。
8. 画面に表示される指示に従って操作します。アプライアンスが自動的に再起動します。
9. [Central Management] > [Appliance Manager] でインベントリを確認します。[アプライアンスステータス（Appliance Status）] が [アップ（Up）] と表示されていることを確認します。
10. SSL/TLS アプライアンス アイデンティティのリストを確認します。新しい証明書が表示されていて、

    複数のアプライアンス：クラスタ内にあるすべてのアプライアンスのアイデンティティを更新する場合、アプライアンスごとに手順 1 ～ 11 を繰り返します。各アプライアンスの設定の変更が完了し、ステータスが [アップ（Up）] に戻っていることを確認してから次のアプライアンスに進みます。

4. デスクトップクライアントの証明書を信頼

デスクトップ クライアントは、ローカルコンピュータにインストールされたデフォルトの信頼ストアに保存されている証明書だけを信頼します。

1. マネージャ に管理者としてログインします（https://<IPAddress>）。
2. （[ダウンロード（Download）]）アイコンをクリックします。
3. 画面に表示される指示に従って、新しい証明書を確認して信頼します。

Central Management での CSR の省略

アプライアンスのアイデンティティ証明書の要件を満たす認証局からの証明書がすでにある場合は、次の手順を実行してアプライアンス アイデンティティ証明書をカスタムアイデンティティ証明書に置き換えます。

概要

全体的な手順は次のとおりです。

1. **信頼ストアへの証明書の追加**
2. **アプライアンス アイデンティティ証明書の置換**
3. **デスクトップクライアントの証明書を信頼**

1. 信頼ストアへの証明書の追加

アプライアンス アイデンティティを更新する前に、認証局（CA）証明書を必要な信頼ストアに追加します。

フレンドリ名：新しい証明書に名前を付ける場合、または信頼ストアに追加する場合は、各フレンドリ名が一意であることを確認します。フレンドリ名を重複させないでください。

ファイルに複数の証明書が含まれている場合は、各証明書を信頼ストアに個別にアップロードします。チェーン全体を 1 つの証明書としてアップロードしないでください。

次の証明書をアップロードしてください。

- identity
- chain（ルート証明書と中間証明書）

> ⚠ アプライアンスの信頼ストアに証明書を追加すると、アプライアンスはそのアイデンティティを信頼し、通信できるようになります。

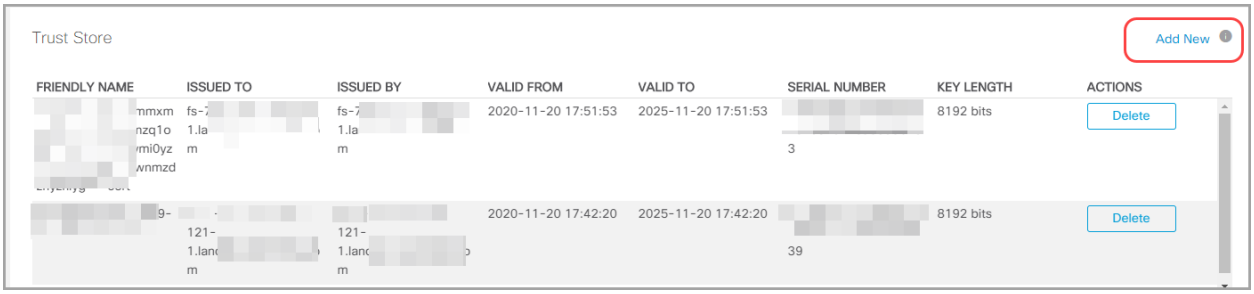
1. Central Management を開きます。
2. [Appliance Manager] ページで、アプライアンスの ••• （[省略記号（Ellipsis）]）アイコン をクリックします。

   順序：次の順序でアプライアンスを選択します。

   - Flow Collector
   - フローセンサー
   - UDP Director
   - マネージャ

> ⚠ マネージャ 信頼ストアを更新する前に、選択順序に従ってアプライアンスの信頼ストアを更新します。

3. [アプライアンス構成の編集（Edit Appliance Configuration）] を選択します。
4. [全般（General）] タブで、[信頼ストア（Trust Store）] セクションを見つけます。
5. [新規追加（Add New）] をクリックします。



6. [フレンドリ名（Friendly Name）] フィールドに証明書の一意の名前を入力します。
7. [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。

8. [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。
   - **ファイルに複数の証明書が含まれている場合**は、各証明書を信頼ストアに個別にアップロードします。チェーン全体をアップロードしないでください。
   - アプライアンス アイデンティティ証明書と証明書チェーン(該当する場合)をアプライアンス信頼ストア(独自の信頼ストア)と [信頼ストアの要件(Trust Stores Requirements)]**信頼ストアの要件**テーブルに表示されている信頼ストアに追加してください。
9. 各アプライアンスの信頼ストアで手順 1 ～ 9 を繰り返します。

信頼ストアの要件

この表を使用して**アプライアンス アイデンティティ**と**証明書チェーン**(該当する場合)をアプライアンス信頼ストアに追加します。ファイルチェーンに複数の証明書(ルート証明書と中間証明書)が含まれている場合は、各証明書を信頼ストアに個別にアップロードします。チェーン全体を 1 つの証明書としてアップロードしないでください。

アイデンティティ証明書とチェーン証明書を追加する場所を確認するには、[信頼ストアに追加(Add to Trust Stores)] 列を参照してください。

アプライアンス アイデンティティ証明書	詳細	信頼ストアへの追加
マネージャ Central Manager	マネージャ 信頼ストアと Central Management 内の各アプライアンスの信頼ストアに マネージャ 証明書を追加します。	• Primary マネージャ • Flow Collector • Flow Collector データベース(5000 シリーズのみ) • Flow Sensor • UDP Director • セカンダリ マネージャ(フェールオーバーのみ)
Secondary マネージャ (フェールオーバーのみ)	Manager がフェールオーバー用に設定されている場合にセカンダリ マネージャ アイデンティティ証明書を置き換えるには、新しいセカンダリ マネージャ 証明書をセカンダリ マネージャ 信頼ストア、プライマリ マネージャ 信頼ストア、および Central Management 内のすべてのアプライアンスの信頼ストアに追加します。	• Flow Collector • Flow Collector データベース(5000 シリーズのみ) • Flow Sensor • UDP Director • セカンダリ マネージャ(フェールオーバーのみ)

	フェールオーバーペアをまだ設定していない場合は、アプライアンス アイデンティティの交換を完了し、フェールオーバー コンフィギュレーション ガイド [英語] を参照してフェールオーバーを設定します。	• Primary マネージャ
Flow Collector	Flow Collector の証明書を、Flow Collector の信頼ストアとマネージャ の信頼ストアに追加します。 **5000 シリーズのみ**: • Flow Collector エンジン証明書を Flow Collector データベースの信頼ストアに追加します。 • Flow Collector データベース証明書を Flow Collector エンジンの信頼ストアに追加します。	• Flow Collector • Flow Collector データベース（5000 シリーズのみ） • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ
フローセンサー	Flow Sensor の証明書を Flow Sensor の信頼ストアと マネージャ 信頼ストアに追加します。	• フローセンサー • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ
UDP Director	UDP Director の証明書を UDP Director の信頼ストアと マネージャ 信頼ストアに追加します。	• UDP Director • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ
高可用性ペアの UDP Director	• セカンダリ UDP Director 証明書をプライマリ UDP Director 信頼ストアに追加します。 • プライマリ UDP Director 証明書をセカンダリ UDP Director 信頼ストアに追加します。	• セカンダリ UDP Director（高可用性のみ） • プライマリ UDP Director（高可用性のみ） • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ

2. アプライアンス アイデンティティ証明書の置換

準備:このプロセスでは、各アプライアンスが自動的に再起動するので、アプライアンスでのトラフィック量が比較的少ないタイミングで証明書を更新するよう計画します。

1. Central Management を開きます。
2. [Appliance Manager] ページで、アプライアンスの ••• ([省略記号(Ellipsis)]) アイコン をクリックします。

   複数のアプライアンス:Flow Collector、Flow Sensor、または UDP Director から開始します。マネージャ を最後に更新します。
3. [アプライアンス構成の編集(Edit Appliance Configuration)] を選択します。
4. [SSL/TLS アプライアンス アイデンティティ(SSL/TLS Appliance Identity)] セクションに移動します。
5. [アイデンティティの更新(Update Identity)] をクリックします。
6. CSR(証明書署名要求)を生成する必要がある場合は、[いいえ(No)] を選択し、[次へ(Next)] をクリックします。
7. [フレンドリ名(Friendly Name)] フィールドに証明書の一意の名前を入力します。
8. [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。
   - **形式**:PKCS#12 (.p12)。詳細については、「はじめに」の「**アプライアンスのアイデンティティ証明書**」を参照してください。
   - **パスワード**:[バンドルパスワード(Bundle Password)] フィールドにファイルの復号に必要なパスワードを入力します。パスワードは保存されません。
9. [アイデンティティの置換(Replace Identity)] をクリックします。
10. [設定の適用(Apply settings)] をクリックします。
11. 画面に表示される指示に従って操作します。アプライアンスが自動的に再起動します。
12. [Central Management] > [Appliance Manager] でインベントリを確認します。[アプライアンスステータス(Appliance Status)] が [アップ(Up)] と表示されていることを確認します。
13. SSL/TLS アプライアンス アイデンティティのリストを確認します。新しい証明書が表示されていて、

    複数のアプライアンス:クラスタ内にあるすべてのアプライアンスのアイデンティティを更新する場合は、アプライアンスごとにて手順 1 ～ 13 を繰り返します。各アプライアンスの設定の変更が完了し、ステータスが [アップ(Up)] に戻っていることを確認してから次のアプライアンスに進みます。

3. デスクトップクライアントの証明書を信頼

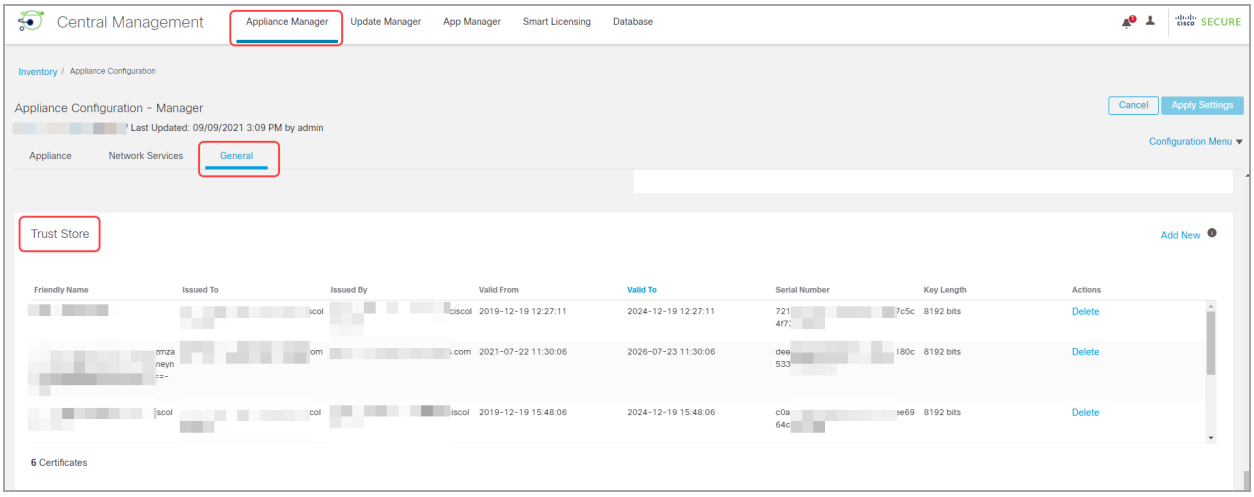
デスクトップ クライアントは、ローカルコンピュータにインストールされたデフォルトの信頼ストアに保存されている証明書だけを信頼します。

1. Manager に管理者としてログインします(https://<IPAddress>)。
2. ([ダウンロード(Download)])アイコンをクリックします。
3. 画面に表示される指示に従って、新しい証明書を確認して信頼します。

信頼ストアの証明書の確認

次の手順を実行して、選択したアプライアンスの信頼ストアに保存した証明書を確認します。

1. Central Management を開きます。
2. アプライアンスの ••• ([省略記号(Ellipsis)])アイコン 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. **[全般(General)]** タブを選択します。
5. [信頼ストア(Trust Store)] リストを確認します。



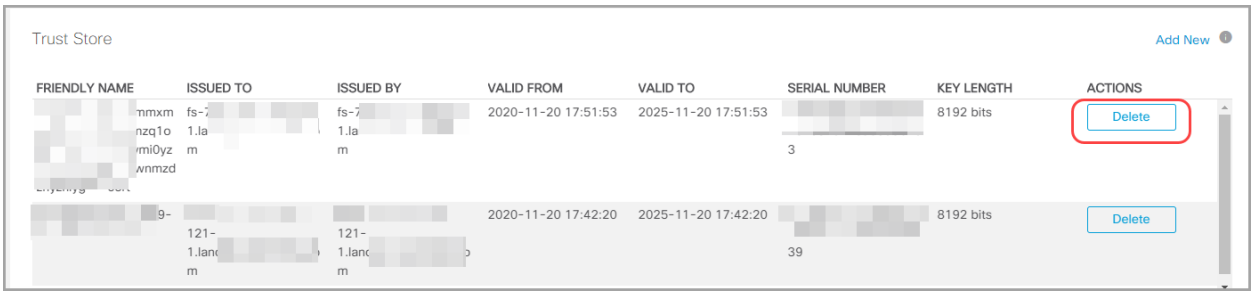
信頼ストアからの証明書の削除

次の手順を実行して、アプライアンスの信頼ストアから証明書を削除します。無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。

> ⚠ アプライアンス アイデンティティを置き換える場合は、新しい証明書(アイデンティティとチェーン)を追加し、「**SSL/TLS アプライアンス アイデンティティ証明書の置換**」の手順を完全に実行するまでは古い証明書を削除しないでください。

1. [信頼ストア(Trust Store)] のリストで、削除する証明書(アイデンティティ、中間、またはルート)を見つけます。
2. [削除(Delete)] をクリックします。

> ⚠ 無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。



3. [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。
4. Central Management のインベントリで、アプライアンスのステータスが[アップ(Up)]に戻っていることを確認します。

信頼ストアの場所

アプライアンス アイデンティティ証明書(アイデンティティとチェーン)が保存されている場所を確認するには、[信頼ストア(Trust Stores)]列を参照してください。チェーンファイルを信頼ストアにアップロードした場合は、ルート証明書ファイルと中間証明書ファイルが個別にリストされます。

アプライアンス アイデンティティ証明書	信頼ストア
マネージャ Central Manager	• Primary マネージャ • Flow Collector • Flow Collector データベース(5000 シリーズのみ) • Flow Sensor • UDP Director • セカンダリ マネージャ(フェールオーバーのみ)
Secondary マネージャ (フェールオーバーのみ)	• Flow Collector • Flow Collector Databases (5000 シリーズのみ) • Flow Sensor • UDP Director • セカンダリ マネージャ(フェールオーバーのみ) • Primary マネージャ **マネージャ フェールオーバー:** マネージャ フェールオーバーの関係を削除する場合は、すべてのアプライアンスの信頼ストアからセカンダリ マネージャ 証明書を削除し

	ます。詳細や手順については、フェールオーバー コンフィギュレーション ガイド [英語] を参照してください。
Flow Collector	• Flow Collector • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ **5000 シリーズのみ**： • Flow Collector エンジンの証明書は、Flow Collector データベースの信頼ストアに保存されます。 • Flow Collector データベースの証明書は、Flow Collector エンジンの信頼ストアに保存されます。
Flow Sensor	• Flow Sensor • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ
UDP Director	• UDP Director • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ
高可用性ペアの UDP Director	• セカンダリ UDP Director（高可用性のみ） • プライマリ UDP Director（高可用性のみ） • セカンダリ マネージャ（フェールオーバーのみ） • Primary マネージャ

ホスト名またはネットワークドメイン名の変更

アプライアンスのホスト名とネットワークドメイン名は、アプライアンス セットアップ ツールを使用したインストールプロセスの一環として設定されます。[Central Management] の [ホスト名（Host Naming）] セクションには、この情報は読み取り専用として表示されます。

> アプライアンスの IP アドレスを変更するには、「**ネットワーク インターフェイスの変更**」を参照してください。

最新の設定の確認

次の手順に従って、選択したアプライアンスのホスト名とネットワークドメイン名を確認します。

1. Central Management を開きます。
2. アプライアンスの ••• （[省略記号（Ellipsis）]）アイコン 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。

ホスト名またはネットワークドメイン名の変更

次の手順に従って、アプライアンスのホスト名とネットワークドメイン名を変更します。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シスコ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。

要件

アプライアンスのホスト名またはネットワークドメイン名を変更する前に、「はじめに」の「**ベストプラクティス**」を確認し、次の要件を見直してください。

- 一意のホスト名と完全修飾ドメイン名が各アプライアンスに必要です。
- フェールオーバー：Manager がフェールオーバーペアとして設定されている場合は、マネージャ ホスト名またはネットワークドメイン名を変更する前に、フェールオーバー関係を削除します。**マネージャ**フェールオーバー コンフィギュレーション ガイド [英語] の手順に従ってください。

アプライアンスの手順の選択

- **マネージャ**：**マネージャ**
- **Flow Collector、Flow Sensor、または UDP Director**：**マネージャ 以外のアプライアンス**

> マネージャ と別のアプライアンス（Flow Collector など）でホスト名やネットワークドメイン名を変更する場合は、最初に マネージャ の手順を実行します。

マネージャ

次の手順に従って、マネージャ のホスト名またはネットワークドメイン名を変更します。手順は、Central Management から一時的にアプライアンスを削除することが含まれています。指定した順序に従っていることを確認します。アプライアンスが複数ある場合、この手順は完了するまでかなりの時間がかかる場合があります。サポートが必要な場合は、シスコサポートまでお問い合わせください。

フェールオーバー：Manager がフェールオーバーペアとして設定されている場合は、Manager の設定を変更する前に、フェールオーバーの関係を削除します。**マネージャ**フェールオーバー コンフィギュレーション ガイド [英語] の手順に従ってください。

> 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シスコ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。

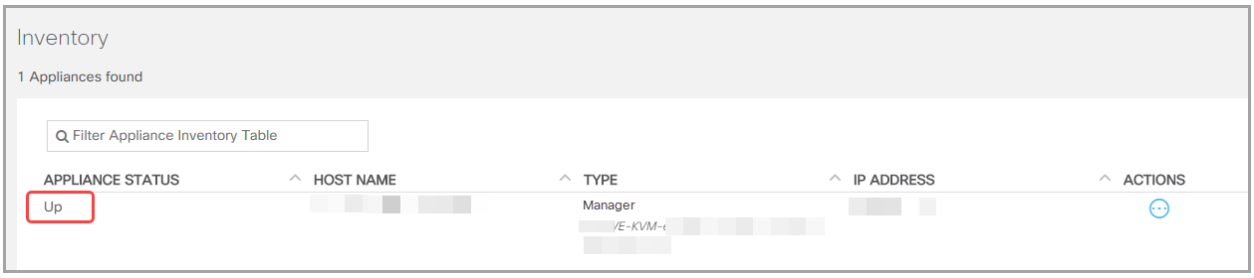
概要

全体的な手順は次のとおりです。

1. **Central Management からのアプライアンスの削除**
2. **マネージャホスト名またはネットワークドメイン名の変更**
3. **Central Management へのアプライアンスの追加**
4. **信頼ストアからの古い マネージャ 証明書の削除**
5. **マネージャ フェールオーバーペアの設定**

1. Central Management からのアプライアンスの削除

1. Central Management を開きます。
2. [アプライアンスステータス（Appliance Status）] 列を確認します。すべてのアプライアンスが [アップ（Up）] と表示されていることを確認します。
3. すべてのアプライアンス（プライマリ マネージャ を除く）を Central Management から削除します。
   - [Appliance Manager] ページで、アプライアンスの ••• （[省略記号（Ellipsis）]）アイコン をクリックします。
   - [このアプライアンスの削除（Remove This Appliance）] を選択します。
   - **コンフィギュレーションチャネルのダウン**：アプライアンスのステータスが [コンフィギュレーションチャネルのダウン（Config Channel Down）] と表示されている場合は、アプライアンスコンソールにログインします。メインメニューから、[リカバリ（Recovery）] > [アプライアンスの削除（RemoveAppliance）] を選択します。
4. マネージャ 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。



5. Central Management からプライマリ マネージャを削除します。
    - [Appliance Manager] ページで、プライマリ マネージャの ••• ([省略記号(Ellipsis)])アイコン をクリックします。
    - [このアプライアンスの削除(Remove This Appliance)] を選択します。
    - [コンフィギュレーションチャネルのダウン(Config Channel Down)]:アプライアンスのステータスが [コンフィギュレーションチャネルのダウン(Config Channel Down)] と表示されている場合は、マネージャ アプライアンスコンソールにログインします。メインメニューから、[リカバリ(Recovery)] > [アプライアンスの削除(RemoveAppliance)] を選択します。

2. マネージャホスト名またはネットワークドメイン名の変更

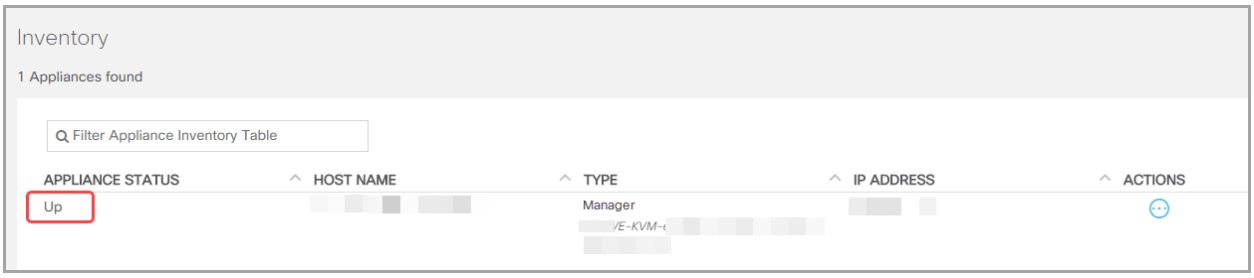
アプライアンス セットアップ ツールを使用して マネージャ のホスト名またはネットワークドメイン名を変更(および Central Management でアプライアンスを登録)するには、次の手順を実行します。

マネージャ フェールオーバー:2 つの Manager がある場合は、プライマリ マネージャ でこの手順を実行するだけです。セカンダリ マネージャ を登録します。「**3. Central Management へのアプライアンスの追加**」に進みます。

1. マネージャ に管理者としてログインします(https://<IPAddress>)。

    アプライアンス セットアップ ツール:アプライアンス セットアップ ツールが自動的に開かない場合は、マネージャ アプライアンスコンソールにログインします。メインメニューから、[リカバリ(Recovery)] > [アプライアンスの削除(RemoveAppliance)] を選択します。

2. [続行/次へ(Continue/Next)] をクリックし、[ホスト名とドメイン(Host Name and Domains)] タブまでスクロールします。
3. フィールドに新しいホスト名またはネットワークド メイン名を入力します。
4. [確認と再起動(Review and Restart)] ダイアログが開くまで [次へ(Next)] をクリックします。
5. 新しい設定が正しいことを確認します。[再起動して続行(Restart and Proceed)] をクリックします。画面に表示される指示に従って マネージャ を再起動します。
6. マネージャ に再度ログインします。
7. [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。
    - Central Management が マネージャ にインストールされます。
    - マネージャ IP アドレスは自動的に検出されるため、変更できません。
8. アプライアンスのセットアップが完了したら、[Central Management] でインベントリを確認します。マネージャ 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。



3. Central Management へのアプライアンスの追加

アプライアンス セットアップ ツールを使用して、別のアプライアンスを Central Management に追加します。

- **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。
- Central Management：マネージャ IP アドレス、マネージャ パスワード、および Secure Network Analytics ドメインが必要です。
- **順序**：「アプライアンスの設定順序」に従います。
- **アクセス**：Central Management にアクセスするには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.	UDP Director （別名 FlowReplicators）	
2.	Flow Collector 5000 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。
3.	Flow Collector 5000 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。
4.	その他のすべての Flow Collector （NetFlow および sflow）	
5.	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。

6.	Secondary マネージャ （使用する場合）	セカンダリ マネージャ の設定を開始する前に、プライマリ マネージャ が [アップ（Up）] として表示されていることを確認します。 セカンダリ マネージャ 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。手順については、「**5. マネージャ フェールオーバーペアの設定**」を参照してください。

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

   - **アップ**：次のアプライアンスを Central Management に追加する前に、各アプライアンスが [アップ（Up）] 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。

2. **セカンダリ マネージャ**：次のログイン情報を入力してログインします。
   - **ユーザー名**：admin
   - **パスワード**：lan411cope

   その他のすべてのアプライアンス：手順 4 に進みます。

3. **セカンダリ マネージャ**：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ー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。

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

4. [次へ（Next）] をクリックし、[Central Management] タブまたは [アプライアンスの登録（Register Your Appliance）] タブ（セカンダリ マネージャ のみ）までスクロールします。
5. 次の手順に従って、アプライアンスを Central Management に登録します。
   - **セカンダリ マネージャ**：セカンダリ マネージャ がある場合は、それ自体が Central Manager として選択します。Secure Network Analytics ドメインを選択し、その他の必要

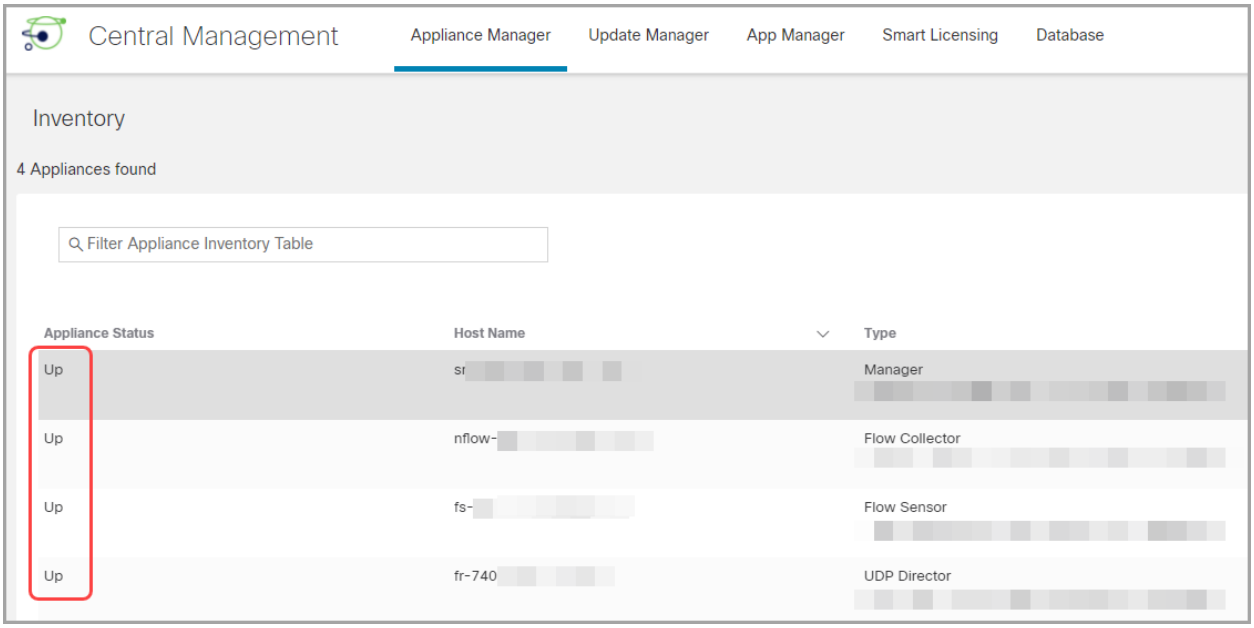
な情報を入力します。アプライアンス セットアップ ツールですべてのアプライアンスを設定した後にフェールオーバーを設定します。手順については、「**5. マネージャ フェールオーバーペアの設定**」を参照してください。

- **その他のすべてのアプライアンス**：プライマリ マネージャ の IP アドレスを入力します。**[保存(Save)]**をクリックします。画面に表示される指示に従って、プライマリ マネージャ アプライアンスのアイデンティティ証明書を信頼し、マネージャ の管理者ユーザー名とパスワードを入力します。Secure Network Analytics ドメインを選択し、その他の必要な情報を入力します。

アプライアンスによっては、メニューが異なる場合があります。たとえば、Flow Sensor を設定する場合は、Flow Collector を選択します。

6. アプライアンスのセットアップが完了したら、[Central Management] でインベントリを確認します。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 [初期化中(Initializing)] または [設定の変更を保留中(Config Changes Pending)] から [アップ(Up)] に変化します。プライマリ マネージャ と各アプライアンスが [アップ(Up)] と表示されていることを確認してから、次のアプライアンスを Central Management に追加します(設定の順序と詳細を使用)。



7. 手順 1 ～ 6 を繰り返して各アプライアンスを Central Management に追加します。

4. 信頼ストアからの古い マネージャ 証明書の削除

マネージャ 以外の各信頼ストアを確認し、古い マネージャ 証明書を削除します。各アプライアンス アイデンティティ証明書の保存場所の詳細については、「**信頼ストアの場所**」を参照してください。

無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。

1. アプライアンスの ••• ([省略記号(Ellipsis)])アイコン 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. **[全般(General)]** タブを選択します。
4. [信頼ストア(Trust Store)] リストを確認します。すべての古い マネージャ 証明書(アイデンティティ、中間、ルート)を見つけます。
5. [削除(Delete)] をクリックして古い証明書それぞれを削除します。
6. [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。
7. Central Management のインベントリで、アプライアンスと マネージャ アプライアンスのステータスが [アップ(Up)] に戻っていることを確認します。
8. 各 Flow Collector、Flow Sensor、および UDP Director で手順 1 ～ 7 を繰り返します。

5. マネージャ フェールオーバーペアの設定

Manager をフェールオーバーペアとして設定するには、フェールオーバー コンフィギュレーション ガイド [英語] の手順に従います。

マネージャ 以外のアプライアンス

次の手順に従って、マネージャ 以外のアプライアンス(Flow Collector、フローセンサー、および UDP Director)のホスト名とネットワークドメイン名を変更します。

> 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シスコ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。

概要

全体的な手順は次のとおりです。

1. **Central Management からのアプライアンスの削除**
2. **アプライアンスのホスト名またはネットワークドメイン名の変更**

> ℹ マネージャ ホスト名またはネットワークドメイン名を変更するには、**マネージャ**の手順を使用します。

1. Central Management からのアプライアンスの削除

1. Central Management を開きます。
2. [アプライアンスステータス(Appliance Status)] 列を確認します。すべてのアプライアンスが [アップ(Up)] と表示されていることを確認します。
3. 変更するアプライアンスを特定します。••• ([省略記号(Ellipsis)])アイコンをクリックします。
4. [このアプライアンスの削除(Remove This Appliance)] を選択します。

コンフィギュレーションチャネルのダウン：アプライアンスのステータスが [コンフィギュレーションチャネルのダウン（Config Channel Down）] と表示されている場合は、アプライアンスコンソールにログインします。メインメニューから、[リカバリ（Recovery）] > [アプライアンスの削除（RemoveAppliance）] を選択します。

2. アプライアンスのホスト名またはネットワークドメイン名の変更

アプライアンス セットアップ ツールを使用して設定を変更し、アプライアンスを Central Management に追加します。

1. アプライアンスに管理者としてログインします（https://<IPAddress>）。

   アプライアンス セットアップ ツール：アプライアンス セットアップ ツールが自動的に開かない場合は、アプライアンスコンソールにログインします。メインメニューから、[リカバリ（Recovery）] > [アプライアンスの削除（RemoveAppliance）] を選択します。

2. [続行/次へ（Continue/Next）] をクリックし、[ホスト名とドメイン（Host Name and Domains）] タブまでスクロールします。
3. フィールドに新しいホスト名またはネットワークド メイン名を入力します。
4. [確認と再起動（Review and Restart）] ダイアログが開くまで [次へ（Next）] をクリックします。
5. 設定の確認[再起動して続行（Restart and Proceed）] をクリックします。
6. アプライアンスが再起動します。
7. アプライアンスにログインします。
8. [続行/次へ（Continue/Next）] をクリックしてアプライアンス セットアップ ツールの [Central Management] タブまでスクロールします。
   - プライマリ マネージャ/Central Manager の IP アドレスを入力します。[保存（Save）] をクリックします。
   - 画面上の指示に従い、[Central Management] タブでの変更を完了させます。
9. プライマリ マネージャ/Central Manager にログインします。
   - アプライアンス Manager インベントリに、アプライアンスが表示されていることを確認します。
   - [アプライアンスステータス（Appliance Status）] が [アップ（Up）] と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 [初期化中（Initializing）] または [設定の変更を保留中（Config Changes Pending）] から [アップ（Up）] に変化します。アプライアンスが [アップ（Up）] に変化しない場合は、信頼ストアに古い証明書または重複している証明書が存在する可能性があります。詳細については、「**トラブルシューティング**」と「**信頼ストアからの証明書の削除**」を参照してください。

ネットワーク インターフェイスの変更

アプライアンス ネットワーク インターフェイスは、アプライアンス セットアップ ツールを使用したインストールプロセスの一環として設定されます。Central Management で選択したネットワーク インターフェイスの変更やアプライアンス セットアップ ツールを使用した IP アドレス（eth0 ネットワーク インターフェイス）の変更が可能です。

- **IP アドレス**：アプライアンスの IP アドレスを変更するには、「**アプライアンスの IP アドレスの変更**」を参照してください。
- **ホスト名またはドメイン名**：アプライアンスのホスト名またはドメイン名を変更するには、「**ホスト名またはネットワークドメイン名の変更**」を参照してください。

最新の設定の確認

次の手順に従って、選択したアプライアンスの［ネットワーク インターフェイス（Network Interfaces）］を確認します。

1. Central Management を開きます。
2. アプライアンスの ••• （［省略記号（Ellipsis）］）アイコン 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。

Central Management でのネットワーク インターフェイスの変更

Central Management で **eth1 または eth2 ネットワーク インターフェイス**を追加もしくは変更するには、次の手順を実行します。

次のインターフェイスは、Central Management では変更できません。

- **eth0**：アプライアンスの IP アドレスを変更するには、「**アプライアンスの IP アドレスの変更**」を参照してください。
- **eth2（Flow Collector 5000 シリーズのみ）**ネットワーク インターフェイス
- Flow Sensor のネットワーク インターフェイス
- UDP Director のネットワーク インターフェイス

1. ［ネットワーク インターフェイス（Network Interfaces）］セクションで、追加または変更するインターフェイス（eth1 や eth2 など）を特定します。
2. 矢印をクリックします。
3. 次のフィールドに必要な情報を入力します。

    - IPv4 アドレス（IPv4 Address）
    - サブネット マスク
    - デフォルト ゲートウェイ
    - ブロードキャスト

4. [保存(Save)]をクリックします。
5. [設定の適用(Apply settings)]をクリックします。
6. 画面に表示される指示に従って操作します。アプライアンスが自動的に再起動します。

アプライアンスの IP アドレスの変更

次の手順を実行して、アプライアンスの **IP アドレス**が含まれた **eth0 ネットワーク インターフェイス**を変更します。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シスコ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。

要件

アプライアンスの IP アドレス(eth0 ネットワーク インターフェイス)を変更する前に、「はじめに」の「**ベストプラクティス**」を確認し、次の点を再確認してください。

- **レコード**:変更を加える前に、現在のネットワーク設定を記録します。また、新しい eth0 値を入力する場合は、必ずその値が正しいことを確認してください。eth0 に誤った値を入力すると接続が失われ、修正にルートアクセスが必要となります。
- **マネージャ フェールオーバー**:Manager がフェールオーバーペアとして設定されている場合は、マネージャ IP アドレスを変更する前に、フェールオーバーの関係を削除します。フェールオーバー コンフィギュレーション ガイド [英語] の手順に従ってください。

アプライアンスの手順の選択

- **マネージャ**:**マネージャ**
- **Flow Collector、Flow Sensor、または UDP Director**:**マネージャ 以外のアプライアンス**

> ⚠ マネージャ と別のアプライアンス(Flow Collector など)の IP アドレスを変更する場合は、最初に マネージャ の手順を実行します。

マネージャ

次の手順を実行して、マネージャ の IP アドレス(eth0 ネットワーク インターフェイス)を変更します。手順は、Central Management から一時的にアプライアンスを削除することが含まれています。指定した順序に従っていることを確認します。アプライアンスが複数ある場合、この手順は完了するまでかなりの時間がかかる場合があります。サポートが必要な場合は、シスコサポートまでお問い合わせください。

フェールオーバー:Manager がフェールオーバーペアとして設定されている場合は、Manager の設定を変更する前に、フェールオーバーの関係を削除します。**マネージャ**フェールオーバー コンフィギュレーション ガイド [英語] の手順に従ってください。

> 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シスコ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。

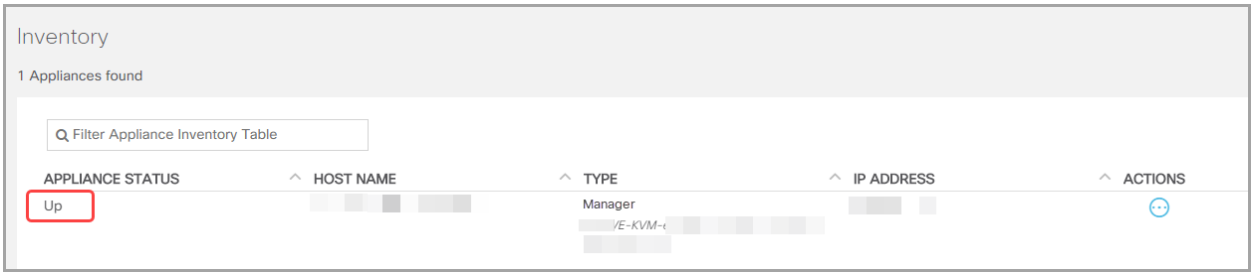
概要

全体的な手順は次のとおりです。

1. **Central Management からのアプライアンスの削除**
2. **マネージャ IP アドレスの変更**
3. **Central Management へのアプライアンスの追加**
4. **信頼ストアからの古い マネージャ 証明書の削除**
5. **マネージャ フェールオーバーペアの設定**

1. Central Management からのアプライアンスの削除

1. Central Management を開きます。
2. [アプライアンスステータス(Appliance Status)] 列を確認します。すべてのアプライアンスが [アップ(Up)] と表示されていることを確認します。
3. すべてのアプライアンス(プライマリ マネージャ を除く)を Central Management から削除します。
   - [Appliance Manager] ページで、アプライアンスの ••• ([省略記号(Ellipsis)]) アイコン をクリックします。
   - [このアプライアンスの削除(Remove This Appliance)] を選択します。
   - **コンフィギュレーションチャネルのダウン**:アプライアンスのステータスが [コンフィギュレーションチャネルのダウン(Config Channel Down)] と表示されている場合は、アプライアンスコンソールにログインします。メインメニューから、[リカバリ(Recovery)] > [アプライアンスの削除(RemoveAppliance)] を選択します。
4. マネージャ 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。



5. Central Management からプライマリ マネージャ を削除します。
   - [Appliance Manager] ページで、プライマリ マネージャ の ••• ([省略記号(Ellipsis)]) アイコン をクリックします。

- [このアプライアンスの削除(Remove This Appliance)]を選択します。
- [コンフィギュレーションチャネルのダウン(Config Channel Down)]:アプライアンスのステータスが[コンフィギュレーションチャネルのダウン(Config Channel Down)]と表示されている場合は、マネージャ アプライアンスコンソールにログインします。メインメニューから、[リカバリ(Recovery)]>[アプライアンスの削除(RemoveAppliance)]を選択します。

2. マネージャ IP アドレスの変更

次の手順を実行して、マネージャ の IP アドレスを変更し、アプライアンス セットアップ ツールを使用して Central Management にそのアドレスを登録します。

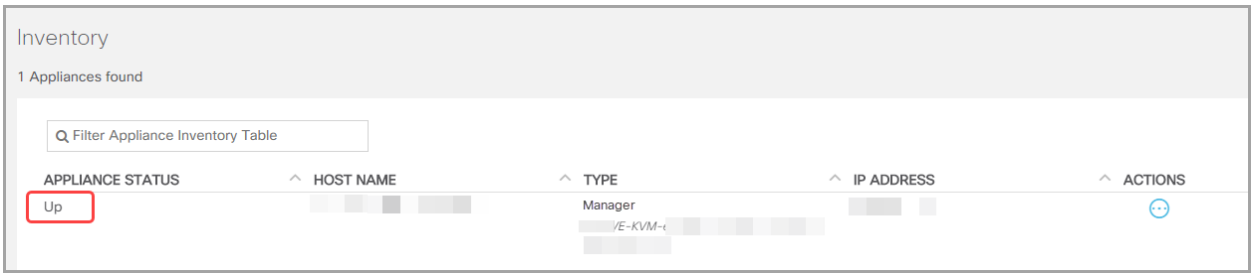
マネージャ フェールオーバー:2 つの Manager がある場合は、プライマリ マネージャ でこの手順を実行するだけです。セカンダリ マネージャ を登録します。「3. Central Management へのアプライアンスの追加」に進みます。

1. マネージャ に管理者としてログインします(https://<IP address>)。

   アプライアンス セットアップ ツール:アプライアンス セットアップ ツールが自動的に開かない場合は、マネージャ にログインします。メインメニューから、[リカバリ(Recovery)]>[アプライアンスの削除(RemoveAppliance)]を選択します。

2. [続行/次へ(Continue/Next)]をクリックし、[管理ネットワーク インターフェイス(Management Network Interface)]タブまでスクロールします。
3. フィールドに新しい IP アドレスを入力します。

   IP アドレスまたはサブネットマスクを変更すると、**ゲートウェイとブロードキャストアドレス**がデフォルトの設定に戻ります。次の手順に進む前に、これらのフィールドがネットワークに対して正しいことを確認してください。
4. [確認と再起動(Review and Restart)]ダイアログが開くまで[次へ(Next)]をクリックします。
5. 新しい設定が正しいことを確認します。[再起動して続行(Restart and Proceed)]をクリックします。画面に表示される指示に従って マネージャ を再起動します。
6. マネージャ にログインします(新しい IP アドレスを使用)。
7. [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。
   - Central Management が マネージャ にインストールされます。
   - マネージャ IP アドレスは自動的に検出されるため、変更できません。
8. アプライアンスのセットアップが完了したら、[Central Management]でインベントリを確認します。マネージャ 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。



3. Central Management へのアプライアンスの追加

アプライアンス セットアップ ツールを使用して、別のアプライアンスを Central Management に追加します。

- **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。
- Central Management：マネージャ IP アドレス、マネージャ パスワード、および Secure Network Analytics ドメインが必要です。
- **順序**：「アプライアンスの設定順序」に従います。
- **アクセス**：Central Management にアクセスするには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.	UDP Director （別名 FlowReplicators）	
2.	Flow Collector 5000 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。
3.	Flow Collector 5000 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。
4.	その他のすべての Flow Collector （NetFlow および sflow）	
5.	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。
6.	Secondary マネージャ （使用する場合）	セカンダリ マネージャ の設定を開始する前に、プライマリ マネージャ が [アップ（Up）] として表示されていることを確認します。 セカンダリ マネージャ 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。手順については、「**5. マネージャ フェールオーバーペアの設定**」を参照してください。

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

   - **アップ**：次のアプライアンスを Central Management に追加する前に、各アプライアンスが［アップ（Up）］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。

2. **セカンダリ マネージャ**：次のログイン情報を入力してログインします。
   - **ユーザー名**：admin
   - **パスワード**：lan411cope

   その他のすべてのアプライアンス：手順 4 に進みます。

3. **セカンダリ マネージャ**：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ー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。

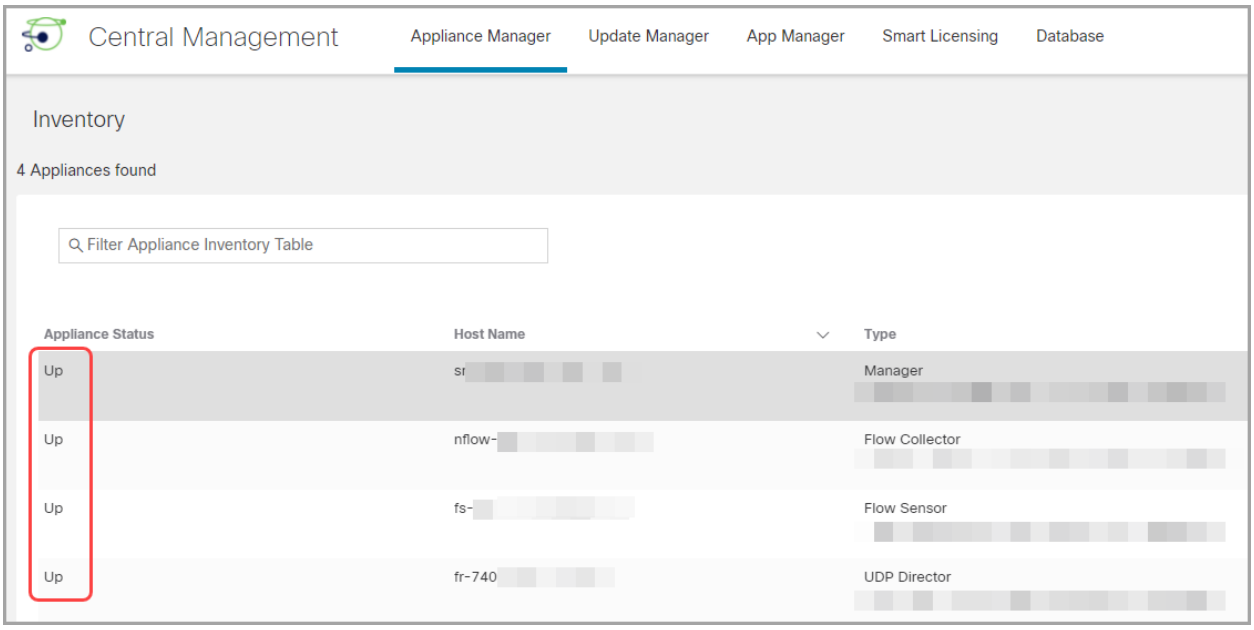
ユーザー	デフォルト パスワード
admin	lan411cope
root	lan1cope
sysadmin	lan1cope

4. ［次へ（Next）］をクリックし、［Central Management］タブまたは［アプライアンスの登録（Register Your Appliance）］タブ（セカンダリ マネージャ のみ）までスクロールします。
5. 次の手順に従って、アプライアンスを Central Management に登録します。
   - **セカンダリ マネージャ**：セカンダリ マネージャ がある場合は、それ自体が Central Manager として選択します。Secure Network Analytics ドメインを選択し、その他の必要な情報を入力します。アプライアンス セットアップ ツールですべてのアプライアンスを設定した後にフェールオーバーを設定します。手順については、「**5. マネージャ フェールオーバーペアの設定**」を参照してください。
   - **その他のすべてのアプライアンス**：プライマリ マネージャ の IP アドレスを入力します。**［保存（Save）］**をクリックします。画面に表示される指示に従って、プライマリ マネージャ アプライアンスのアイデンティティ証明書を信頼し、マネージャ の管理者ユーザー名とパスワードを入力します。Secure Network Analytics ドメインを選択し、その他の必要な情報を入力します。

アプライアンスによっては、メニューが異なる場合があります。たとえば、Flow Sensor を設定する場合は、Flow Collector を選択します。

6. アプライアンスのセットアップが完了したら、[Central Management] でインベントリを確認します。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 [初期化中(Initializing)] または [設定の変更を保留中(Config Changes Pending)] から [アップ(Up)] に変化します。プライマリ マネージャ と各アプライアンスが [アップ(Up)] と表示されていることを確認してから、次のアプライアンスを Central Management に追加します(設定の順序と詳細を使用)。



7. 手順 1 ～ 6 を繰り返して各アプライアンスを Central Management に追加します。

4. 信頼ストアからの古い マネージャ 証明書の削除

マネージャ 以外の各信頼ストアを確認し、古い マネージャ 証明書を削除します。各アプライアンス アイデンティティ証明書の保存場所の詳細については、「**信頼ストアの場所**」を参照してください。

無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。

1. アプライアンスの ••• ([省略記号(Ellipsis)]) アイコン 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. **[全般(General)]** タブを選択します。
4. [信頼ストア(Trust Store)] リストを確認します。すべての古い マネージャ 証明書(アイデンティティ、中間、ルート)を見つけます。
5. [削除(Delete)] をクリックして古い証明書それぞれを削除します。
6. [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。

7. Central Management のインベントリで、アプライアンスと マネージャ アプライアンスのステータスが [アップ(Up)] に戻っていることを確認します。
8. 各 Flow Collector、Flow Sensor、および UDP Director で手順 1 ～ 7 を繰り返します。

5. マネージャ フェールオーバーペアの設定

Manager をフェールオーバーペアとして設定するには、フェールオーバー コンフィギュレーション ガイド [英語] の手順に従います。

マネージャ 以外のアプライアンス

次の手順を実行して、マネージャ 以外のアプライアンス(Flow Collector、フローセンサー、および UDP Director)の IP アドレスを変更します。

> 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シスコ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。

概要

全体的な手順は次のとおりです。

1. **Central Management からのアプライアンスの削除**
2. **アプライアンスの IP アドレスの変更**

> マネージャ IP アドレスを変更するには、**マネージャ**の手順を使用します。

1. Central Management からのアプライアンスの削除

1. Central Management を開きます。
2. [アプライアンスステータス(Appliance Status)] 列を確認します。すべてのアプライアンスが [アップ(Up)] と表示されていることを確認します。
3. 変更するアプライアンスを特定します。••• ([省略記号(Ellipsis)])アイコンをクリックします。
4. [このアプライアンスの削除(Remove This Appliance)] を選択します。

   コンフィギュレーションチャネルのダウン:アプライアンスのステータスが [コンフィギュレーションチャネルのダウン(Config Channel Down)] と表示されている場合は、アプライアンスコンソールにログインします。メインメニューから、[リカバリ(Recovery)] > [アプライアンスの削除(RemoveAppliance)] を選択します。

2. アプライアンスの IP アドレスの変更

アプライアンス セットアップ ツールを使用して設定を変更し、アプライアンスを Central Management に追加します。

1. アプライアンスに管理者としてログインします（https://<IPAddress>）。

   アプライアンス セットアップ ツール：アプライアンス セットアップ ツールが自動的に開かない場合は、アプライアンスコンソールにログインします。メインメニューから、[リカバリ（Recovery）] > [アプライアンスの削除（RemoveAppliance）] を選択します。

2. [続行/次へ（Continue/Next）] をクリックし、[管理ネットワーク インターフェイス（Management Network Interface）] タブまでスクロールします。
3. フィールドに新しい IP アドレスを入力します。

   IP アドレスまたはサブネットマスクを変更すると、**ゲートウェイとブロードキャストアドレス**がデフォルトの設定に戻ります。次の手順に進む前に、これらのフィールドがネットワークに対して正しいことを確認してください。
4. [確認と再起動（Review and Restart）] ダイアログが開くまで [次へ（Next）] をクリックします。
5. 設定の確認[再起動して続行（Restart and Proceed）] をクリックします。
6. アプライアンスが再起動します。
7. アプライアンスにログインします（新しい IP アドレスを使用）。
8. [続行/次へ（Continue/Next）] をクリックしてアプライアンス セットアップ ツールの [Central Management] タブまでスクロールします。
   - プライマリ マネージャ/Central Manager の IP アドレスを入力します。[保存（Save）] をクリックします。
   - 画面上の指示に従い、[Central Management] タブでの変更を完了させます。
9. プライマリ マネージャ/Central Manager にログインします。
   - アプライアンス Manager インベントリに、アプライアンスが表示されていることを確認します。
   - [アプライアンスステータス（Appliance Status）] が [アップ（Up）] と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 [初期化中（Initializing）] または [設定の変更を保留中（Config Changes Pending）] から [アップ（Up）] に変化します。アプライアンスが [アップ（Up）] に変化しない場合は、信頼ストアに古い証明書または重複している証明書が存在する可能性があります。詳細については、「**トラブルシューティング**」と「**信頼ストアからの証明書の削除**」を参照してください。

SSL/TLS クライアント アイデンティティの追加

クライアント アイデンティティは外部サービス間の通信に使用されます。マネージャ で外部サービスを使用する場合は、この手順を実行し、必要に応じてクライアント アイデンティティ証明書を追加します。

> ⚠ 証明書はシステムのセキュリティにとって重要です。証明書を不適切に変更すると、Secure Network Analytics アプライアンスの通信が停止し、データ損失の原因となります。

追加の証明書の設定

このガイドでは、アプライアンス アイデンティティとクライアント アイデンティティの設定について説明します。証明書、およびサーバー ID 検証の要件を必要とする追加の設定が Secure Network Analytics で必要な場合があります。機能のヘルプまたはガイドの手順に従います。

- **監査ログの宛先**:ヘルプの手順に従います。 ([ユーザ(User)])アイコン を選択して [監査ログの宛先(Audit Log Destination)]検索します。
- **シスコISEまたは Cisco ISE-Pic**:『ISE and ISE-PIC Configuration Guide』の手順に従います。
- LDAP:ヘルプの手順に従います。 ([グローバル設定(Global Settings)])アイコン を選択して [LDAP] を検索します。
- パケットアナライザ:ヘルプの手順に従います。 ([グローバル設定(Global Settings)])アイコン 選択して「パケットアナライザ」を検索します。
- SAML SSO:システム コンフィギュレーション ガイド [英語] の手順に従います。
- 応答管理に対する SMTP の設定:ヘルプの手順に従ってください。 ([ユーザ(User)])アイコン を選択して「SMTP の設定」を検索します。

> ℹ その他のコンフィギュレーション ガイドについては、コンフィギュレーション ガイド [英語] を参照してください。

証明書の要件

クライアント アイデンティティ証明書を追加する場合は、認証局の証明書があることを確認します。証明書と信頼ストアの要件については、「はじめに」の「**クライアント アイデンティティ証明書**」を参照してください。

環境に応じた手順の選択

Central Management で**証明書署名要求(CSR)**を生成するか、すでに認証局の証明書がある場合は CSR を省略できます。

- 証明書署名要求を生成するには、「**Central Management での CSR の生成**」に進みます。
- 証明書署名要求を省略するには、「**Central Management での CSR の省略**」に進みます。

Central Management での CSR の生成

Central Management で CSR を生成し、マネージャ にクライアント アイデンティティ証明書を追加するには、次の手順を実行します。

概要

全体的な手順は次のとおりです。

1. **証明書署名要求の生成**
2. **信頼ストアへの証明書の追加**
3. **クライアント アイデンティティ証明書の追加**

1. 証明書署名要求の生成

次の手順を実行して証明書署名要求(CSR)を準備します。

1. Central Management を開きます。
2. [Appliance Manager] ページで、マネージャ の ••• ([省略記号(Ellipsis)])アイコン 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. [追加の SSL/TLS クライアントアイデンティティ(Additional SSL/TLS Client Identities)] セクションに移動します。
5. [新規追加(Add New)] をクリックします。
6. CSR(証明書署名要求)を生成する必要がある場合は、[はい(Yes)] を選択します。[次へ(Next)] をクリックします。

> CSR を生成する必要がない場合は、「**Central Management での CSR の省略**」に進みます。

7. 認証局でサポートされている **RSA キーの長さ**を選択します。

> 使用できる最長のキーの長さを選択します。2048 ビットの使用はお勧めしません。外部サービスで必要とされている場合のみ、2048 ビットを使用します。

8. [CSRの生成(Generate a CSR)] セクションのフィールド(任意)に入力します。
9. [CSR の生成(Generate CSR)] をクリックします。生成プロセスは数分かかることがあります。

   キャンセル:CSR を生成した後、または CA 証明書を待っている間に [キャンセル(Cancel)] をクリックすると、キャンセルされた CSR は無効になります。この場合は新しい CSR を生成します。
10. [CSRのダウンロード(Download CSR)] をクリックします。
11. ダウンロードした CSR を認証局に送信します。

2. 信頼ストアへの証明書の追加

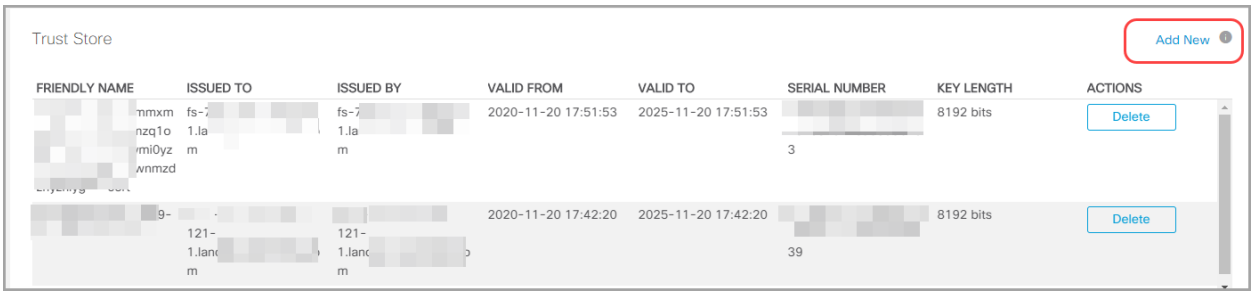
認証局(CA)から証明書を受け取った場合は、必要な信頼ストアにそれらを追加します。

フレンドリ名:新しい証明書に名前を付ける場合、または信頼ストアに追加する場合は、各フレンドリ名が一意であることを確認します。フレンドリ名を重複させないでください。

ファイルに複数の証明書が含まれている場合は、各証明書を信頼ストアに個別にアップロードします。チェーン全体を 1 つのファイルとしてアップロードしないでください。

> ⚠ アプライアンスの信頼ストアに証明書を追加すると、アプライアンスはそのアイデンティティを信頼し、通信できるようになります。

1. Central Management を開きます。
2. [Appliance Manager] ページで、マネージャ の ••• ([省略記号(Ellipsis)])アイコン 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. [全般(General)] タブで、[信頼ストア(Trust Store)] セクションを見つけます。
5. [新規追加(Add New)] をクリックします。



6. [フレンドリ名(Friendly Name)] フィールドに証明書の一意の名前を入力します。
7. [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。
8. [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。

   ファイルに複数の証明書が含まれている場合は、各証明書を信頼ストアに個別にアップロードします。チェーン全体を 1 つのファイルとしてアップロードしないでください。

3. クライアント アイデンティティ証明書の追加

1. Central Management を開きます。
2. [Appliance Manager] ページで、マネージャ の ••• ([省略記号(Ellipsis)])アイコン 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 > [追加の SSL/TLS クライアント アイデンティティ(Additional SSL/TLS Client Identities)] に戻ります。
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。

   また、証明書ファイル形式に次の手順を実行します。

   - **PKCS#12**:[バンドルパスワード(Bundle Password)] フィールドにファイルの復号に必要なパスワードを入力します。パスワードは保存されません。

- **PEM**:[証明書チェーンファイル(Certificate Chain File)]フィールドで、認証局(CA)チェーンファイルを個別にアップロードします([ファイルの選択(Choose File)]をクリックします)。チェーンファイルが正しい順序であり、要件を満たしていることを確認します。詳細については、「はじめに」の「**PEM チェーンファイルの要件**」を参照してください。

> ⚠ ファイルにクライアント アイデンティティ証明書を含めないでください。

7. [クライアント アイデンティティの追加(Add Client Identity)]をクリックします。
8. [設定の適用(Apply settings)]をクリックします。
9. 追加の SSL/TLS クライアント アイデンティティのリストを確認します。新しい証明書が表示されていて、

Central Management での CSR の省略

「**クライアント アイデンティティ証明書**」の要件を満たす認証局からの証明書がある場合は、手順に従って マネージャ に追加します。

概要

全体的な手順は次のとおりです。

1. **信頼ストアへの証明書の追加**
2. **クライアント アイデンティティ証明書の追加**

1. 信頼ストアへの証明書の追加

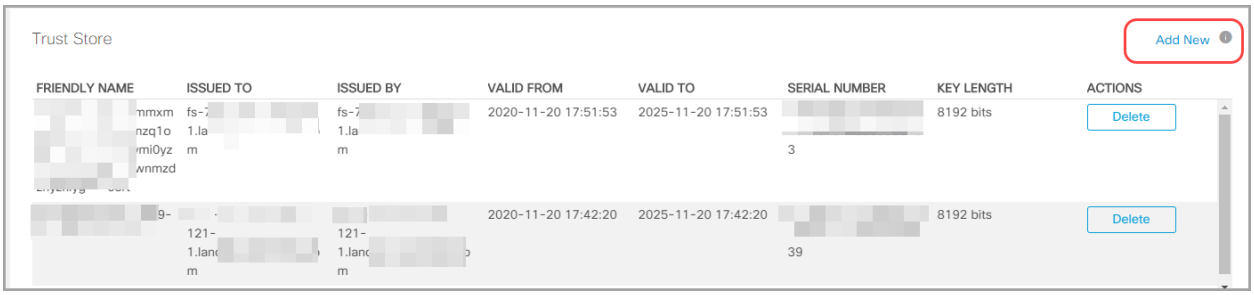
必要な信頼ストアに認証局(CA)証明書を追加します。

フレンドリ名:新しい証明書に名前を付ける場合、または信頼ストアに追加する場合は、各フレンドリ名が一意であることを確認します。フレンドリ名を重複させないでください。

ファイルに複数の証明書が含まれている場合は、各証明書を信頼ストアに個別にアップロードします。チェーン全体を 1 つの証明書としてアップロードしないでください。

> ⚠ アプライアンスの信頼ストアに証明書を追加すると、アプライアンスはそのアイデンティティを信頼し、通信できるようになります。

1. Central Management を開きます。
2. [Appliance Manager] ページで、マネージャ の ••• ([省略記号(Ellipsis)])アイコン 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. [全般(General)]タブで、[信頼ストア(Trust Store)]セクションを見つけます。
5. [新規追加(Add New)]をクリックします。



6. [フレンドリ名（Friendly Name）] フィールドに証明書の一意の名前を入力します。
7. [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。
8. [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。

   ファイルに複数の証明書が含まれている場合は、各証明書を信頼ストアに個別にアップロードします。チェーン全体を 1 つのファイルとしてアップロードしないでください。

2. クライアント アイデンティティ証明書の追加

1. Central Management を開きます。
2. [Appliance Manager] ページで、マネージャ の ••• ([省略記号（Ellipsis）]) アイコン 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. [追加の SSL/TLS クライアントアイデンティティ（Additional SSL/TLS Client Identities）] セクションに移動します。
5. [新規追加（Add New）] をクリックします。
6. CSR（証明書署名要求）を生成する必要がある場合は、[いいえ（No）] を選択し、[次へ（Next）] をクリックします。

> CSR を生成する必要がある場合は、「**Central Management での CSR の生成**」に進みます。

7. [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。
8. [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。
   - **形式**：PKCS#12. 詳細については、「**証明書の要件**」を参照してください。
   - **パスワード**：[バンドルパスワード（Bundle Password）] フィールドにファイルの復号に必要なパスワードを入力します。パスワードは保存されません。
9. [クライアント アイデンティティの追加（Add Client Identity）] をクリックします。
10. [設定の適用（Apply settings）] をクリックします。
11. 追加の SSL/TLS クライアント アイデンティティのリストを確認します。新しい証明書が表示されていて、

クライアント アイデンティティ証明書の削除

1. Central Management を開きます。
2. アプライアンスの ••• ([省略記号(Ellipsis)])アイコン 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。
5. [追加の SSL/TLS クライアント アイデンティティ(Additional SSL/TLS Client Identities)] リストで、削除する証明書を見つけます。
6. [削除(Delete)] をクリックします。

トラブルシューティング

確認のためにトラブルシューティング情報を以下に示します。サポートが必要な場合は、シスコサポートまでお問い合わせください。

> ⚠ 証明書はシステムのセキュリティにとって重要です。証明書を不適切に変更すると、Secure Network Analytics アプライアンスの通信が停止し、データ損失の原因となります。

ログインする前に証明書を選択する必要がありますか。

マネージャ のランディングページを開くと、ログイン前に証明書の選択を求められることがあります。このダイアログは、Secure Network Analytics へのログインには影響しません。証明書をアプライアンス アイデンティティ証明書と同じ認証局を含む証明書がコンピュータに保存した場合にこのプロンプトが表示されることがあります。

> ⚠ 続行する前に、会社のポリシーを確認します。

アプライアンス アイデンティティ証明書が無効なのはなぜですか。

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カスタム証明書に置き換えた場合は、要件を満たしていることを確認します。

また、新しいアプライアンス アイデンティティ証明書が必要な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 アプライアンス アイデンティティ証明書の置換**」を参照してください。

Central Management からアプライアンスを削除しましたが、まだ管理対象になっています。

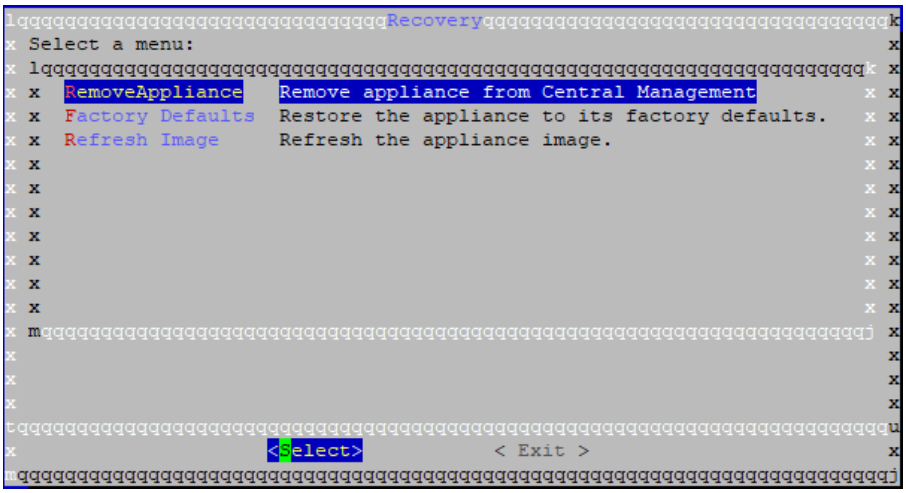
Central Management からアプライアンスを削除しても、システムがまだ管理対象であることを示している場合は、システム設定からアプライアンスを削除します。

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。
   - 最初：複数のアプライアンスを削除する場合は、最初に Flow Collector、Flow Sensor、および UDP Director にログインします。
   - 最後：複数のアプライアンスを削除する場合は、（必要に応じて他のすべてのアプライアンスで手順 1 ～ 5 を完了した後）最後に マネージャ にログインします。

> ⚠ Central Management から最後に マネージャ を削除します。

2. **SystemConfig** と入力します。Enter を押します。
3. メインメニューから [リカバリ（Recovery）] を選択します。
4. [アプライアンスの削除（RemoveAppliance）] を選択します。

   メニューが表示されない場合、アプライアンスはすでに Central Management から削除されています。



5. 画面に表示される指示に従ってアプライアンスを削除します。

[アプライアンスのステータス(Appliance Status)]には[アップ(Up)]ではなく[初期化中(Initializing)]と表示されます。

アプライアンスのステータスが[初期化中(Initializing)]または[コンフィギュレーションチャネルのダウン(Config Channel Down)]と表示され、[アップ(Up)]に戻らない場合は、マネージャ信頼ストアとアプライアンス信頼ストアを確認します。信頼ストアに重複する証明書がないことを確認します。たとえば、同じアプライアンスの信頼ストアに古い証明書と新しい証明書がある場合は競合が発生します。使用した元の手順を参照してください。詳細については、「**信頼ストアからの証明書の削除**」を参照してください。

> ⚠ 無効になった古い証明書のみを削除してください。最新の証明書を削除すると、システムとの通信が切断されます。

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。
- シスコサポートの連絡先
- 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