



# Cisco Secure Network Analytics

管理対象アプライアンスの SSL/TLS 証明書 v7.4.2



---

# 目次

はじめに .....	7
Data Store .....	7
DoDIN およびコモンクライテリアへの準拠 .....	7
対象読者 .....	7
用語 .....	7
計画時間 .....	7
ベストプラクティス .....	7
アプライアンス アイデンティティ証明書 .....	8
認証 (Authentication) .....	8
証明書の要件 .....	8
証明書のテスト .....	10
自己署名証明書 .....	10
認証局によって署名された証明書 (チェーンの長さ = 2) .....	10
認証局によって署名された証明書 (チェーンの長さ > 2) .....	10
アプライアンス セットアップ ツール .....	11
マネージャ フェールオーバー .....	11
クライアント アイデンティティ証明書 .....	11
証明書の要件 .....	11
PEM チェーンファイルの要件 .....	12
信頼ストアの要件 .....	13
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) .....	13
追加の証明書の設定 .....	13
証明書の要件を開く .....	14
[アプライアンスステータス (Appliance Status)] が [接続済み (Connected)] であることを確認 .....	14
概要 .....	16
証明書の確認 .....	18
証明書の保存 .....	19
シスコのバンドルのダウンロード .....	20
更新時の証明書チェック .....	20
期限切れの証明書の通知を受け取る .....	21
システムアラーム .....	21
電子メールの通知 .....	21
以前に有効化されていた電子メール通知 .....	21

最近有効化された電子メール通知 .....	21
カスタム電子メール通知の作成 .....	22
1. アクションの作成 .....	22
2. ルールの作成 .....	24
電子メール通知のディセーブル化 .....	25
電子メール通知のイネーブル化 .....	26
<b>証明書の有効期限の変更(概要) .....</b>	<b>28</b>
<b>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 .....</b>	<b>29</b>
要件 .....	29
目的とするアプライアンスの手順を選択 .....	29
マネージャおよび管理対象アプライアンス .....	29
概要 .....	30
1. アプライアンスのステータスの確認 .....	30
2. Central Management を使用したアプライアンスの削除 .....	31
3. システム設定を使用したアプライアンスの削除 .....	31
4. 証明書の再生成 .....	32
5. Central Management へのマネージャの登録 .....	34
6. Central Management へのアプライアンスの追加 .....	35
アプライアンスの設定順序 .....	35
7. 信頼ストアからの古い証明書の削除 .....	38
8. マネージャフェールオーバーペアの設定 .....	38
個別の非マネージャ アプライアンス .....	38
概要 .....	38
1. Central Management からのアプライアンスの削除 .....	39
2. 証明書の再生成 .....	40
3. マネージャ信頼ストアからの古い証明書の削除 .....	41
4. Central Management へのアプライアンスの追加 .....	42
<b>期限切れになったシスコのデフォルト証明書の置換 .....</b>	<b>43</b>
要件 .....	43
1. アプライアンスのステータスの確認 .....	43
2. アプライアンスの手順の選択 .....	44
マネージャおよび管理対象アプライアンス .....	44
概要 .....	44
1. アプライアンスの削除と証明書の再生成 .....	45
2. Central Management へのマネージャの登録 .....	47

3. マネージャ信頼ストアから期限切れの証明書を削除する	48
4. Central Management へのアプライアンスの追加	49
アプライアンスの設定順序	49
5. 信頼ストアからの期限切れ証明書の削除	52
6. マネージャフェールオーバーペアの設定	52
個別の非マネージャ アプライアンス	52
概要	52
1. アプライアンスの削除と証明書の再生成	53
2. マネージャ信頼ストアから期限切れの証明書を削除する	55
3. Central Management へのアプライアンスの追加	55
<b>SSL/TLS アプライアンス アイデンティティ証明書の置換</b>	<b>57</b>
証明書の要件	57
環境に応じた手順の選択	57
Central Management での CSR の生成	57
概要	57
1. 証明書署名要求の生成	57
2. 信頼ストアへの証明書の追加	58
信頼ストアの要件	59
3. アプライアンス アイデンティティ証明書の置換	61
4. デスクトップ クライアント の証明書を信頼する	62
Central Management での CSR の省略	62
概要	62
1. 信頼ストアへの証明書の追加	62
信頼ストアの要件	63
2. アプライアンス アイデンティティ証明書の置換	65
3. デスクトップ クライアント の証明書を信頼する	66
<b>信頼ストアの証明書の確認</b>	<b>67</b>
信頼ストアからの証明書の削除	67
信頼ストアの場所	68
<b>ホスト名またはネットワークドメイン名の変更</b>	<b>70</b>
最新の設定の確認	70
ホスト名またはネットワークドメイン名の変更	70
要件	70
アプライアンスの手順の選択	70
マネージャ	71

概要 .....	71
1. Central Management からのアプライアンスの削除 .....	71
2. 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します。 .....	72
3. Central Management へのアプライアンスの追加 .....	73
アプライアンスの設定順序 .....	73
4. 信頼ストアからの古いマネージャ証明書の削除 .....	76
5. マネージャフェールオーバーペアの設定 .....	76
非マネージャ アプライアンス .....	76
概要 .....	76
1. Central Management からのアプライアンスの削除 .....	77
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 .....	77
<b>ネットワーク インターフェイスの変更 .....</b>	<b>79</b>
最新の設定の確認 .....	79
Central Management でのネットワーク インターフェイスの変更 .....	79
アプライアンスの IP アドレスの変更 .....	80
要件 .....	80
アプライアンスの手順の選択 .....	80
マネージャ .....	80
概要 .....	81
1. Central Management からのアプライアンスの削除 .....	81
2. マネージャ IPアドレスの変更 .....	82
3. Central Management へのアプライアンスの追加 .....	83
アプライアンスの設定順序 .....	83
4. 信頼ストアからの古いマネージャ証明書の削除 .....	85
5. マネージャフェールオーバーペアの設定 .....	86
非マネージャ アプライアンス .....	86
概要 .....	86
1. Central Management からのアプライアンスの削除 .....	86
2. アプライアンスの IP アドレスの変更 .....	86
<b>SSL/TLS クライアントアイデンティティの追加 .....</b>	<b>88</b>
追加の証明書の設定 .....	88
証明書の要件 .....	88
環境に応じた手順の選択 .....	88
Central Management での CSR の生成 .....	88
概要 .....	89

---

1. 証明書署名要求の生成 .....	89
2. 信頼ストアへの証明書の追加 .....	89
3. クライアントアイデンティティ証明書の追加 .....	90
Central Management での CSR の省略 .....	91
概要 .....	91
1. 信頼ストアへの証明書の追加 .....	91
2. クライアントアイデンティティ証明書の追加 .....	92
<b>クライアントアイデンティティ証明書の削除 .....</b>	<b>93</b>
<b>トラブルシューティング .....</b>	<b>94</b>
ログインする前に証明書を選択する必要がありますか。 .....	94
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。 .....	94
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。 .....	94
[アプライアンスステータス (Appliance Status)] に [接続済み (Connected)] ではなく [初期化 中 (Initializing)] と表示される .....	95
<b>サポートへの問い合わせ .....</b>	<b>96</b>
<b>変更履歴 .....</b>	<b>97</b>

## はじめに

このガイドを使用して、Cisco Secure Network Analytics (旧称 Stealthwatch) v7.4.2 アプライアンスの SSL/TLS 証明書関連の設定を変更します。

- Cisco Secure Network Analytics Manager (旧 Stealthwatch 管理コンソールまたは SMC)
- 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。

## Data Store

このガイドには Cisco Secure Network Analytics データストア 情報が含まれていません。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。

## 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 Military Unique Deployment Guide*』または『*Common Criteria Administrative Guide*』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、あらゆる Secure Network Analytics 製品に対して「**アプライアンス**」という用語を使用します。

「**クラスタ**」は Secure Network Analytics によって管理されるアプライアンスマネージャのグループです。

## 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の設定を開始する前に、[アプライアンスステータス (Appliance Status)] が [接続済み (Connected)] 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。

**マネージャ:**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 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 (Authentication)

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 アプライアンス アイデンティティ証明書をカスタム証明書に置き換えるには、次のガイドラインに従ってください。

- 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:** Central Management で CSR を生成する場合、記載された要件で(\*) が付けられた項目が CSR に含まれます(「[Central Management で CSR を生成](#)」の列を参照)。
- **Central Management で CSR をスキップする:** Central Management 以外で CSR を生成する場合、生成した CSR がこの表に記載された要件を満たしていることを確認してください(「[Central Management で CSR をスキップする](#)」の列を参照)。
- **証明書要件の検証とテスト:** Central Management で CSR を生成するか、CSR をスキップするかにかかわらず、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前に、証明書がこの表の要件を満たしていることを確認してください。また、[証明書のテスト](#)を参照して、証明書をテストします。



要件	Central Management での CSR の生成	Central Management での CSR の省略
ファイル形式 *	PEM(.cer、.crt、.pem)または PKCS#12(.p12、.pfx、.pks) PEMを使用する場合は、「 <b>PEM チェーンファイルの要件</b> 」を参照してください。	PKCS#12(p12、.pfx、pks)
キー *	使用可能な RSA キー長： 2048ビット(非推奨)、4096ビット、 または 8192ビット  ECDSA カーブ： 使用不可	RSA キー長の要件： 2048ビット(非推奨)以上 または ECDSA キーカーブの要件： NIST P-256、P-384、または P-521
共通名またはサブジェクト代替名 *	CSR は、共通名および/またはサブジェクトの別名が FQDN と一致することを要求します。	共通名またはサブジェクトの別名が FQDN と一致することを確認します。
署名者	アプライアンス アイデンティティ証明書は、自己署名するか、認証局 (CA) の署名を受けることができます。	アプライアンス アイデンティティ証明書は、自己署名するか、認証局 (CA) の署名を受けることができます。
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。
固有の ID (自己署名)	自己署名アプライアンス アイデンティティ証明書が使用していることを確認します。  • 一意のサブジェクト名 (日付、識別子、文字列など)  または  • 一意の権限キー識別子とサブジェクトキー識別子。これらのキー識別子を使用す	自己署名アプライアンス アイデンティティ証明書が使用していることを確認します。  • 一意のサブジェクト名 (日付、識別子、文字列など)  または  • 一意の権限キー識別子とサブジェクトキー識別子。これらのキー識別子を使

要件	Central Management での CSR の生成	Central Management での CSR の省略
	る場合は、置き換える証明書にキー識別子が含まれていることを確認してください。これらのキー識別子は、デフォルトのアプリケーション アイデンティティ証明書には含まれていません。	用する場合は、置き換える証明書にキー識別子が含まれていることを確認してください。これらのキー識別子は、デフォルトのアプリケーション アイデンティティ証明書には含まれていません。
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。

\* Central Management で CSR を生成する場合、記載されている要件で(\*)が付いている項目が CSR に含まれます。

## 証明書のテスト

アプリケーション アプリケーション証明書を置き換える前に、証明書をテストして、それらがシステム要件を満たしていることを確認します。

個別のファイルに編成された中間 CA 証明書とルート CA 証明書を使用して、新しいアイデンティティ証明書をテストします。

- **PEM(.cer、.crt、.pem)ファイル**: openssl を使用して .cer、.crt、または .pem ファイルを生成し、証明書を Central Management にアップロードしている場合は、証明書のテストを終了した後に CA 証明書を 1 つの証明書チェーンファイルに結合します。詳細については、「[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)ファイル**: openssl を使用して .p12、.pfx、または .pks ファイルを生成し、証明書を Central Management にアップロードしている場合は、証明書のテストが終了した後、CA 証明書を 1 つのファイル(-certfile 引数で指定)に結合します。

## 自己署名証明書

CA 署名付き証明書が保存されているラップトップまたは openssl を備えた任意のサーバーで次のコマンドを実行します。

```
openssl verify -CAfile<identity-cert-file>
```

## 認証局によって署名された証明書(チェーンの長さ=2)

CA 署名付き証明書が保存されているラップトップまたは openssl を備えた任意のサーバーで次のコマンドを実行します。

```
openssl verify -CAfile<root-ca-cert-file><identity-cert-file>
```

## 認証局によって署名された証明書(チェーンの長さ>2)

CA 署名付き証明書が保存されているラップトップまたは openssl を備えた任意のサーバーで次のコマンドを実行します。

```
openssl verify -CAfile <root-ca-cert-file> -untrusted <intermediate-ca-certs-file> <identity-cert-file>
```

## 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

マネージャ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

次のガイドラインを使用して、クライアント アイデンティティ証明書を Manager に追加します。

- 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**: Central Management で CSR を生成する場合、記載された要件で(\*) が付けられた項目が CSR に含まれます(「**Central Management で CSR を生成**」の列を参照)。
- **Central Management で CSR をスキップする**: Central Management 以外で CSR を生成する場合、生成した CSR がこの表に記載された要件を満たしていることを確認してください(「**Central Management で CSR をスキップする**」の列を参照)。
- **証明書要件の確認**: Central Management で CSR を生成するか、CSR をスキップするかにかかわらず、証明書を Manager に追加する前に、この表の要件を満たしていることを確認してください。

要件	Central Management での CSR の生成	Central Management での CSR の省略
ファイル形式*	PEM(.cer、.crt、.pem)または PKCS#12 (.p12、.pfx、.pks) PEM を使用する場合は、「 <a href="#">PEM チェーンファイルの要件</a> 」を参照してください。	PKCS#12(p12、.pfx、pks)
キー*		RSA キー長の要件:

要件	Central Management での CSR の生成	Central Management での CSR の省略
	使用可能な RSA キー長: 2048 ビット (非推奨)、4096 ビット、または 8192 ビット  ECDSA カーブ: 使用不可	2048 ビット (非推奨) 以上  または ECDSA キーカーブの要件: NIST P-256、P-384、または P-521
署名者	クライアント アイデンティティ証明書は、自己署名するか、認証局 (CA) の署名を受けることができます。	クライアント アイデンティティ証明書は、自己署名するか、認証局 (CA) の署名を受けることができます。
認証 (拡張キーの使用状況)*	CSR 要求クライアント (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。

\* Central Management で CSR を生成する場合、記載されている要件で (\*) が付いている項目が CSR に含まれます。

## 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 (Root CA Certificate)]  
 — 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。

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ワイルドカード証明書をインストールすると、その有効期限が切れるまではワイルドカード証明書が使用できます。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、およびサーバーアイデンティティ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。❓([ヘルプ (Help)]) アイコン > [ヘルプ (Help)] を選択します。[監査ログの宛先 (Audit Log Destination)] を検索します。
- **Cisco ISE または Cisco ISE-Pic:** 『[ISE-PIC Configuration Guide](#)』の手順に従います。
- **LDAP:** ヘルプの手順に従います。❓([ヘルプ (Help)]) アイコン > [ヘルプ (Help)] を選択します。「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。❓([ヘルプ (Help)]) アイコン > [ヘルプ (Help)] を選択します。「パケットアナライザ」を検索します。
- **SAML SSO:** 『[System Configuration Guide](#)』の手順に従います。
- **応答管理に対する SMTP の設定:** ヘルプの指示に従ってください。❓([ヘルプ (Help)]) アイコン > [ヘルプ (Help)] を選択します。「SMTP 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。

## 証明書の要件を開く

このガイドでは、主に Central Management を使用します。

1. 管理者としてマネージャにログインします : <https://<IPAddress>>
2. メインメニューから [構成 (Configure)] > [グローバル集中管理 (GLOBAL Central Management)] を選択します。

## [アプライアンスステータス (Appliance Status)] が [接続済み (Connected)] であることを確認

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設定を変更すると、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ンネル保留中 (Config Channel Pending)] から [接続済み (Connected)] 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について、アプライアンスのステータスが [接続済み (Connected)] と表示されていることを確認します。

Central Management

Inventory Update Manager App Manager Smart Licensing Database

### Inventory


4 Appliances found

Q Filter Appliance Inventory Table

Appliance Status	Host Name	Type
Connected	sr	Manager
Connected	nflow-	Flow Collector
Connected	fs-	Flow Sensor
Connected	fr-740	UDP Director

## 概要

証明書は、Secure Network Analytics のいくつかの設定変更に関係します。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
<a href="#">証明書の確認</a>	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。
<a href="#">証明書の保存</a>	アプライアンス アイデンティティ証明書を保存します。
<a href="#">シスコのバンドルのダウンロード</a>	
<a href="#">証明書の有効期限の変更</a>	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、「 <a href="#">SSL/TLS アプライアンス アイデンティティ証明書の置換</a> 」を参照してください。
<a href="#">アプライアンス アイデンティティ証明書の置換</a>	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せん。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。
<a href="#">ホスト名の変更</a>	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 <a href="#">シスコサポート</a> にお問い合わせください。



<a href="#">ネットワークドメイン名の変更</a>	<p>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。</p> <p>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<a href="#">シスコサポート</a>にお問い合わせください。</p>
<a href="#">IP アドレス(eth0)の変更</a>	<p>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。</p> <p>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<a href="#">シスコサポート</a>にお問い合わせください。</p>
<a href="#">クライアント アイデンティティ証明書</a>	<p>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。</p>
<a href="#">トラブルシューティング</a>	

---

## 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役立ちます。

**i** 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。

# 期限切れの証明書の通知を受け取る

Secure Network Analytics の v7.4.2 リリースでは、アプライアンスが識別されると、証明書の有効期限が近づいているときにダッシュボードに **システムアラーム**が表示されます。さらに、**電子メールの通知**を受信するオプションもあります。

## システムアラーム

アプライアンス アイデンティティ証明書の有効期限が切れている場合、次のシステムアラームがダッシュボードに表示され始めます。

- アプライアンス証明書の有効期限が 90 日未満
- アプライアンス証明書の有効期限が 60 日未満
- アプライアンス証明書の有効期限が 30 日未満
- アプライアンス証明書の有効期限が 14 日未満
- アプライアンス証明書の有効期限が 3 日未満
- アプライアンス証明書の有効期限切れ

これらのシステムアラームはデフォルトで有効になっており、必要なアプライアンス アイデンティティ証明書を置き換えるまで表示され続けます。アプライアンス アイデンティティ証明書の置き換えの詳細については、「[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。

## 電子メールの通知

電子メール通知は、応答管理を通じて設定されます。電子メール通知の詳細については、[応答管理: アクションタイプのヘルプトピック](#)を参照してください。

## 以前に有効化されていた電子メール通知

Manager システムアラームの電子メール通知がすでに有効になっている場合は、他のシステムアラームの電子メール通知に加えて、デフォルトで [すべての (all)] アプライアンス アイデンティティ証明書の有効期限の電子メール通知の受信が開始されます。

**i** マネージャシステムアラームの電子メール通知が別のユーザーによって、または別の目的ですでに設定されている場合は、すでに設定されている電子メール通知が元に戻されないよう、[カスタム電子メール通知の作成](#)をお勧めします。

受信する電子メール通知を制限するには、次のオプションがあります。

- 期限切れのアプライアンス識別証明書専用の電子メール通知を設定します。「[カスタム電子メール通知の作成](#)」を参照してください。
- 受け取りたくない電子メール通知を無効にします。「[電子メール通知のディセーブル化](#)」を参照してください。

## 最近有効化された電子メール通知

Manager システムアラームの電子メール通知を新たに有効にする場合は、どの電子メール通知を受信するかを必ず指定してください。受信したい電子メール通知のみを受信できるように、[カスタム電子メール通知の作成](#)をお勧めします。

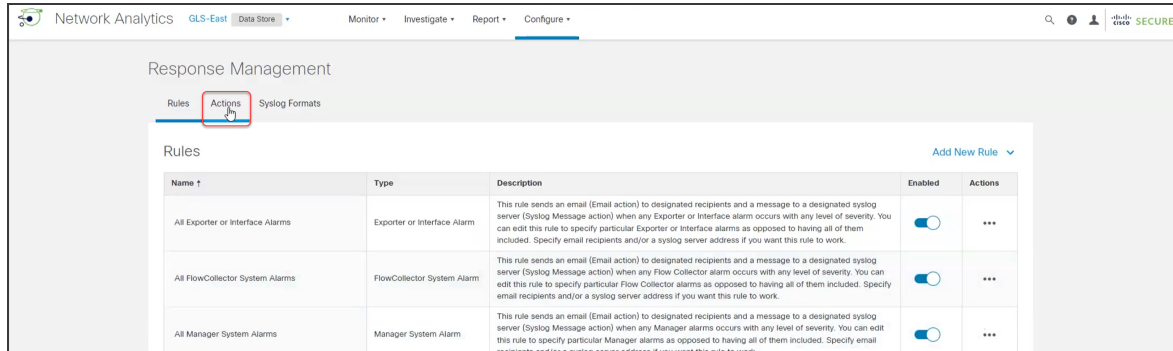
## カスタム電子メール通知の作成

以下から始めます: **1. アクションの作成**を作成し、以下に進みます: **2. ルールの作成**を作成して、作成したアクションにルールを割り当てます。

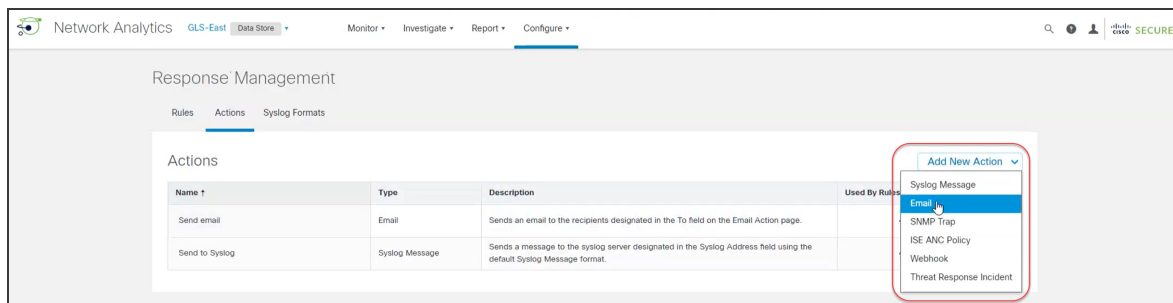
### 1. アクションの作成

次の手順を使用して、証明書の有効期限の電子メール通知の新しいアクションを作成します。

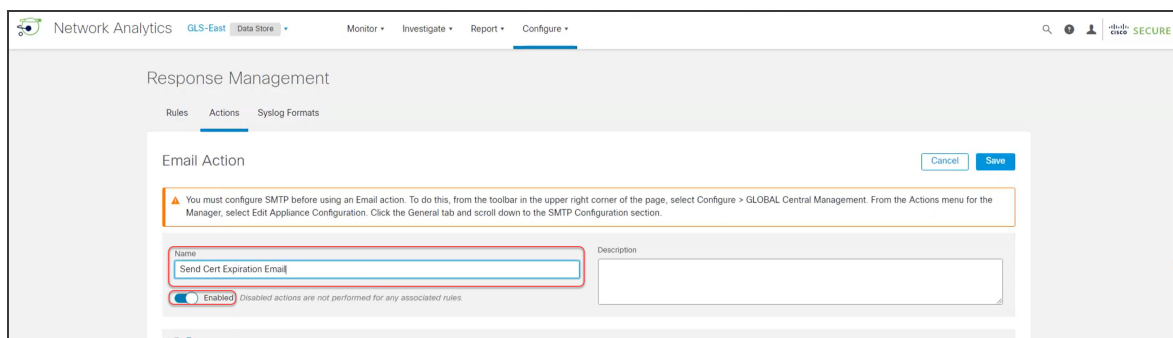
1. メインメニューで、[設定 (Configuration)] [応答の管理 (Response Management)] を選択します。
2. [Actions] タブをクリックします。



3. [アクション (Actions)] 領域で、[新しいアクションの追加 (Add New Actions)] メニューから [電子メール (Email)] を選択します。



4. [名前 (Name)] フィールドに名前を入力します。たとえば、「証明書の有効期限メールを送信」などです。[説明 (Description)] フィールドに説明を追加することもできます。



**i** [有効済み (Enabled)] ボタンがオンになっていることを確認します。

5. [宛先 (To)] フィールドに、アプライアンス アイデンティティ証明書の有効期限が切れたときに通知を受ける必要があるすべての人の電子メールアドレス(および/またはリストエイリアス)を入力します。

The screenshot shows an email configuration form with three main sections: 'To', 'Subject', and 'Body'. The 'To' field is currently empty and is highlighted with a red rectangular border. Below the 'To' field are two buttons: '+ Alarm Variables' and 'Preview'.

- [宛先 (To)] フィールドをクリックして、選択内容が [宛先 (To)] フィールドに追加されていることを確認します。

The screenshot shows the 'To' field with the text 'ame@Company.com' already entered. A new email address 'Name@Company.com' is being added, indicated by a red box around the text and a small plus sign (+) to its right.

- 追加後、緑色で強調表示されます。

The screenshot shows the 'To' field with 'Name@Company.com' added and highlighted in green. A small 'x' icon is visible to the right of the address, indicating it can be removed.

6. [本文 (Body)] 領域の下部にある [+アラーム変数(+Alarm Variable)] をクリックし、電子メール通知の管理に役立つ各変数を選択します。次に例を示します。

- alarm\_severity\_name
- alarm\_status
- alarm\_category\_name

The screenshot shows the 'Body' field with a list of alarm variables. The variable 'alarm\_severity\_name' is highlighted with a blue background and a red border. The list includes:
 

- alarm\_category\_name: String name of the category (e.g., Anomaly).
- alarm\_id: Unique ID assigned to each alarm (e.g., 3Y-13Y1-QJJ2-YYA9-U).
- alarm\_note: Any note attached to this alarm.
- alarm\_severity\_id: Numeric ID of the alarm severity (e.g., 4).
- alarm\_severity\_name: String name of the alarm severity (e.g., Major).
- alarm\_status: Status of the alarm event. Options are ACTIVE or INACTIVE.

7. 選択内容をコピーして、[件名 (Subject)] フィールドに貼り付けます。
8. [プレビュー (Preview)] をクリックして、メール通知がどのように表示されるかのサンプルを確認します。
  - [アクションのテスト (Test Action)] をクリックし、電子メール通知をテストします。
  - 必要に応じて、[編集 (Edit)] をクリックして変更を加えます。

**i** プレビューを閉じるには、[編集 (Edit)] または [本文 (Body)] 領域の任意の場所をクリックします。

9. [保存 (Save)] をクリックします。

## 2. ルールの作成

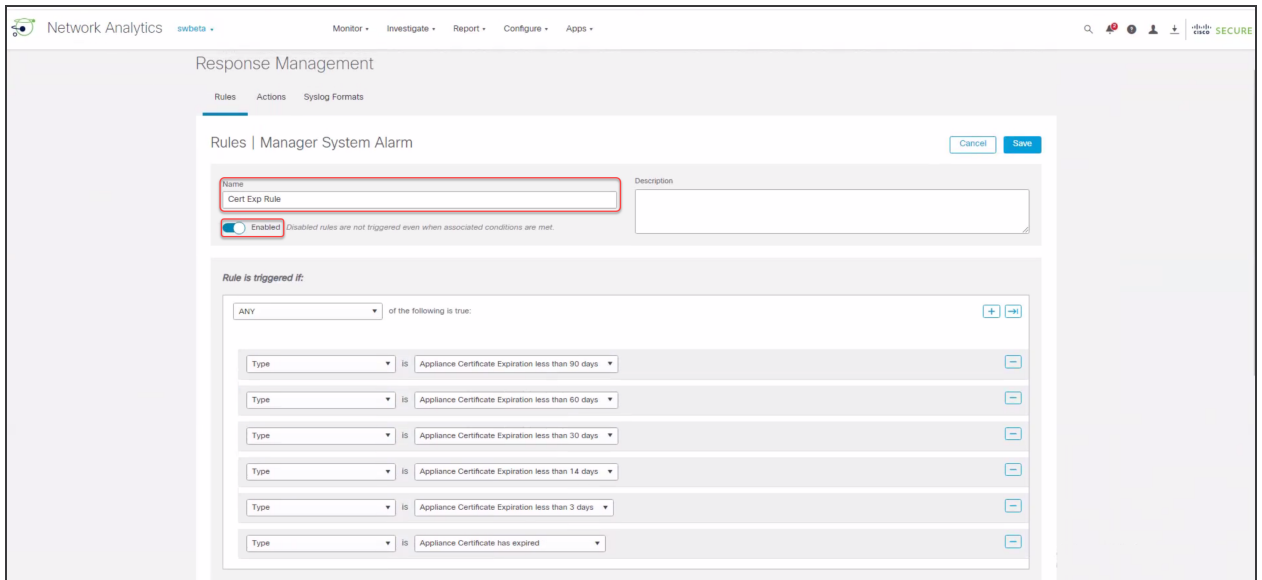
次の手順を使用して、作成したアクションを割り当てるための新しいルールを作成します。

1. [Rules] タブをクリックします。
2. [ルール (Rule)] テーブルの [すべてのマネージャシステムアラーム (All Manager System Alarms)] 行を見つけて、[アクション (Actions)] 列の ([省略記号 (Ellipsis)]) アイコンをクリックします。
3. [複製 (Duplicate)] を選択します。
4. [関連付けられたアクション (Associated Actions)] 領域を見つけて、[アクティブ (Active)] なテーブルと [非アクティブ (Inactive)] なテーブルの両方で作成したアクションの [割り当て済み (Assigned)] 列をオンにします。

Associated Actions				
Execute the following actions when the alarm becomes active:				
Name ↑	Type	Description	Used By Rules	Assigned
Send Cert Expiration Email	Email		0	<input checked="" type="checkbox"/>
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	<input type="checkbox"/>
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	<input type="checkbox"/>
Execute the following actions when the alarm becomes inactive:				
Name ↑	Type	Description	Used By Rules	Assigned
Send Cert Expiration Email	Email		0	<input checked="" type="checkbox"/>
Send email	Email	Sends an email to the recipients designated in the To field on the Email Action page.	4	<input type="checkbox"/>
Send to Syslog	Syslog Message	Sends a message to the syslog server designated in the Syslog Address field using the default Syslog Message format.	4	<input type="checkbox"/>

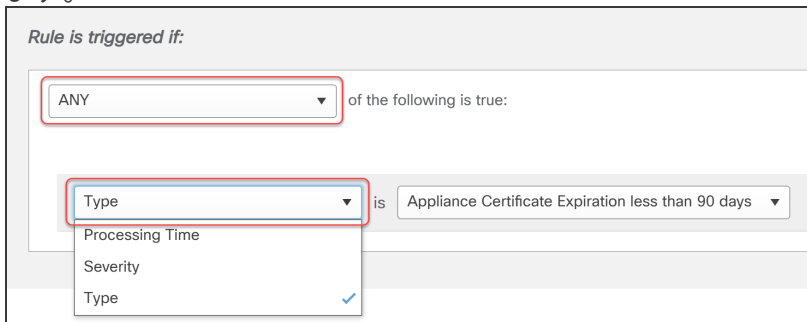
5. [アクティブ (Active)] なテーブルと非アクティブなテーブルの両方で作成したアクションの [割り当て済み (Assigned)] 列をオンに切り替えます。
6. [ルール | マネージャシステムアラーム (Rules | Manager System Alarm)] 領域から [名前 (Name)] フィールドを見つけ、たとえば、「Cert Exp Rule」のように名前を入力します。[説明 (Description)] フィールドに説明を追加することもできます。





**i** [有効済み(Enabled)] ボタンがオンになっていることを確認します。

7. [ルールは次の場合にトリガーされます (Rule is triggered if)] 領域で、[任意 (ANY)] を選択します。

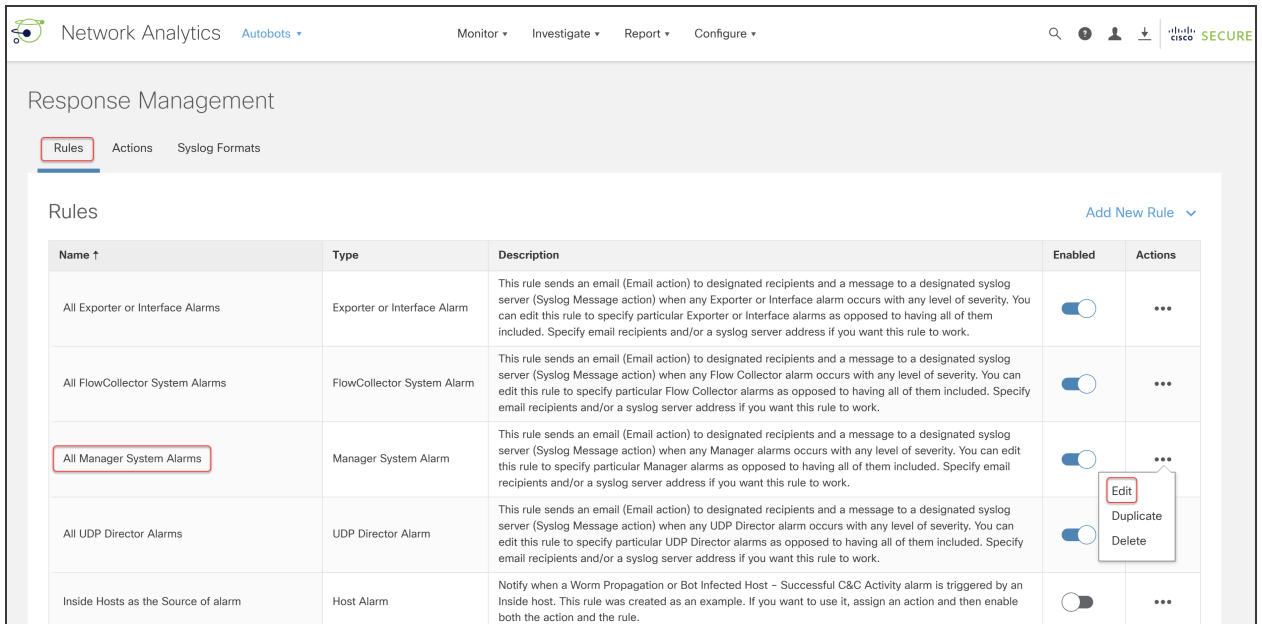


8. [タイプ (Type)] を選択し、リストをスクロールして、受信する各メール通知を選択します。
9. [+](プラス) アイコンをクリックしてタイプを追加します。タイプを削除するには、[-](マイナス) アイコンをクリックします。
10. [保存 (Save)] をクリックします。

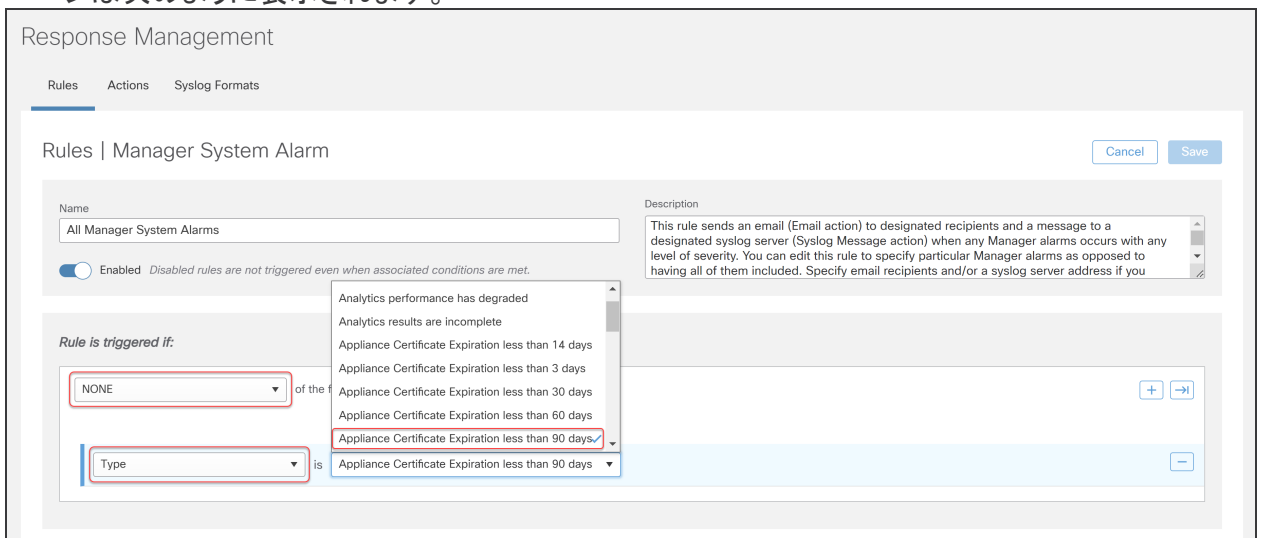
## 電子メール通知のディセーブル化

次の手順を使用して、1 つ以上の電子メール通知を無効にします。

1. メインメニューで、[設定 (Configuration)] [応答の管理 (Response Management)] を選択します。
2. [ルール (Rule)] テーブルの [すべてのマネージャシステムアラーム (All Manager System Alarms)] 行を見つけて、[アクション (Actions)] 列の ([省略記号 (Ellipsis)]) アイコンをクリックします。
3. [編集 (Edit)] を選択します。



ページは次のように表示されます。



4. [ルールは次の場合にトリガーされます (Rule is triggered if)] 領域で、[なし(NONE)] を選択します。
5. [タイプ (Type)] を選択し、リストをスクロールして、無効にする電子メール通知を選択します。
6. [+] (プラス) アイコンをクリックし、手順 5 を繰り返して、追加の電子メール通知を無効にします。
7. [保存 (Save)] をクリックします。

## 電子メール通知のイネーブル化

電子メール通知を有効にするには、次の手順を使用します。

1. メインメニューで、[設定 (Configuration)] [応答の管理 (Response Management)] を選択します。

2. [ルール (Rule)] テーブルの [すべてのマネージャシステムアラーム (All Manager System Alarms)] 行を見つけて、[アクション (Actions)] 列の ([省略記号 (Ellipsis)]) アイコンをクリックします。
3. [編集 (Edit)] を選択します。
4. [ルールは次の場合にトリガーされます (Rule is triggered if)] 領域で、再度有効にする電子メール通知を選択します。

Rule is triggered if:

NONE of the following is true: + ->

Type is Appliance Certificate Expiration less than 60 days -

Type is Appliance Certificate Expiration less than 30 days -

5. [-] (マイナス) アイコンをクリックして、無効になっている電子メール通知を削除します。
6. [保存 (Save)] をクリックします。

## 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	<p>手順については、「<a href="#">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</a>」を参照してください。</p> <p>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、「<a href="#">ネットワーク インターフェイスの変更</a>」または「<a href="#">ホスト名またはネットワークドメイン名の変更</a>」の手順に従います。</p>
期限切れのシスコのデフォルト証明書	<p>手順については、「<a href="#">期限切れになったシスコのデフォルト証明書の置換</a>」を参照してください。</p> <p>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、「<a href="#">ネットワーク インターフェイスの変更</a>」または「<a href="#">ホスト名またはネットワークドメイン名の変更</a>」の手順に従います。</p>
カスタム SSL/TLS 証明書	<p>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、「<a href="#">SSL/TLS アプライアンスアイデンティティ証明書の置換</a>」を参照してください。</p>



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、(このセクションの指示ではなく)「[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](#)」の手順に従います。
- **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。

**i** 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、次の要件を確認してください。

- **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**: マネージャ証明書と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関係を削除してください。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 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ことが含まれています。

## 目的とするアプライアンスの手順を選択

- **マネージャおよび管理対象アプライアンス**: [マネージャおよび管理対象アプライアンス](#)を使用して、マネージャおよびクラスタ内の他の管理対象アプライアンスの証明書の有効期間を変更します。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。
- **個別の非マネージャアプライアンス**: [個別の非マネージャアプライアンス](#)を使用して、個別の非マネージャアプライアンス (Flow Collector、Flow Sensor または UDP ディレクタ) の証明書の有効期間を変更します。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対象アプライアンス

以下の手順に従って、クラスタ内のマネージャおよびその他の管理対象アプライアンスの証明書の有効期間を変更します。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**: マネージャ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関係を削除してください。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 クラスタから削除されます。手順には、セカンダリ マネージャ工場出荷時のデフォルトにリセットすることが含まれます。

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。



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](#)



マネージャのみを変更する必要がある場合でも、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、「[個別の非マネージャアプライアンス](#)」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、それらのアプライアンスが [接続済み (Connected)] 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. メインメニューから [構成 (Configure)] > [グローバル集中管理 (GLOBAL Central Management)] を選択します。
3. [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 [接続済み (Connected)] 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 [構成チャネルのダウン (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、[接続済み (Connected)] 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](#)を使用して中央管理からアプライアンスを削除します。次に、以下に記載されている手順を完了します：[3. システム設定を使用したアプライアンスの削除](#)を使用してアプライアンスを削除します。

Inventory

3 Appliances found

Q Filter Appliance Inventory Table

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Changes Pending	fs-	Flow Sensor FSVE-KVM-		
Connected	nflow-	Flow Collector FCNFVE-KVM-		
Connected		Manager /E-KVM-		

## 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。

**!** マネージャを Central Management から削除します。

- 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 [接続済み (Connected)] に移行します。

- マネージャ アプライアンスのステータスが [接続済み (Connected)] と表示され、Central Management には他のアプライアンスが存在しないことも確認します。

Inventory

1 Appliances found

Q Filter Appliance Inventory Table

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager /E-KVM-		

- プライマリ マネージャを中央管理から削除します。
  - … ([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。

## 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

**i** 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 [接続済み (Connected)] と表示された場合は、この手順を省略できます。以下に進みます: **4. 証明書の再生成**

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。

**⚠** マネージャを Central Management から削除します。

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。

```

lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqRecoveryqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x Select a menu:
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x x RemoveAppliance Remove appliance from Central Management x x
x x Factory Defaults Restore the appliance to its factory defaults. x x
x x Refresh Image Refresh the appliance image. x x
x x
x x
x x
x x
x x
x x
x x
x x
x x
x x
x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj
x
x
x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
x
x
x
x
lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj

```

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。







Inventory				
1 Appliances found				
Q Filter Appliance Inventory Table				
APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager		
	/E-KVM-			

## 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。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 [接続済み (Connected)] になっていることを確認します。
- **一元管理**: マネージャ IP アドレス、パスワード、および Secure Network Analytics ドメイン。
- **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 Flow Replicator)	
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 [接続済み (Connected)] と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 [接続済み (Connected)] と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 [接続済み (Connected)] と表示されていることを確認します。
6.	セカンダリ マネージャ (使用されている場合)	セカンダリ マネージャ設定を開始する前に、プライマリ マネージャが [接続済み (Connected)] として表示されていることを確認してください。

	二次マネージャ自身を中央マネージャとして選択します。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。「 <a href="#">8. マネージャフェールオーバーペアの設定</a> 」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。
  - **接続済み:** 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 [接続済み (Connected)] になってい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、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、それ自体を中央マネージャとして選択します。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、フェールオーバーを設定します。「[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。画面上のプロンプトに従って、プライマリ マネージャアプライアンス アイデンティティ証明書を信頼し、マネージャ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。

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 [接続済み (Connected)] 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 [接続済み (Connected)] 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 [接続済み (Connected)] 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 [設定の順序と詳細](#) を使用して Central Management に追加します。


The screenshot shows the 'Inventory' page in the Central Management interface. At the top, there are navigation tabs: 'Inventory', 'Update Manager', 'App Manager', 'Smart Licensing', and 'Database'. Below the tabs, the page title is 'Inventory' and it states '4 Appliances found'. There is a search bar labeled 'Filter Appliance Inventory Table'. Below the search bar is a table with the following columns: 'Appliance Status', 'Host Name', and 'Type'. The table contains four rows, all with a status of 'Connected'. The first row is a 'Manager' with host name 'sr'. The second row is a 'Flow Collector' with host name 'nflow-'. The third row is a 'Flow Sensor' with host name 'fs-'. The fourth row is a 'UDP Director' with host name 'fr-740'. A red box highlights the 'Connected' status in the first row.

Appliance Status	Host Name	Type
Connected	sr	Manager
Connected	nflow-	Flow Collector
Connected	fs-	Flow Sensor
Connected	fr-740	UDP Director

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が保存される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から期限切れの証明書 (アイデンティティ、ルート、中間証明書) をすべて見つけます。
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 のインベントリページで、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 [接続済み (Connected)] 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

マネージャをフェールオーバーペアとして再設定するには、『[Failover Configuration Guide](#)』の手順に従ってください。

## 個別の非マネージャアプライアンス

この手順に従って、マネージャ以外の個別のアプライアンス (Flow Collector、Flow Sensor、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. [マネージャ信頼ストアからの古い証明書の削除](#)
4. [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間を変更する必要がある場合は、「**マネージャおよび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. アプライアンスに管理者としてログインします : <https://<IPAddress>>
2. メインメニューから [構成 (Configure)] > [グローバル集中管理 (GLOBAL Central Management)] を選択します。
3. [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 [接続済み (Connected)] 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 [接続済み (Connected)] 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 [接続済み (Connected)] として表示されない場合は、解決されるまで数分間待ちます。
4. 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。

**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 [接続済み (Connected)] に移行します。

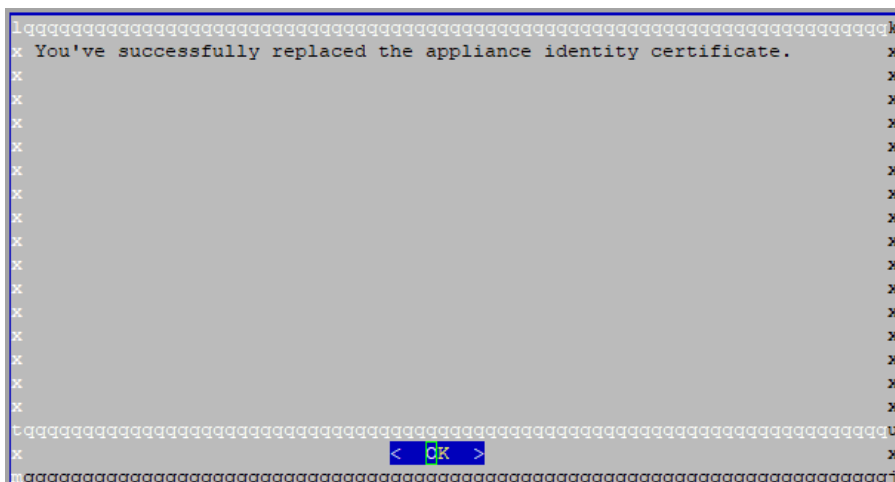
5. マネージャアプライアンスのステータスは接続済みと表示されます。
6. アプライアンスコンソールに sysadmin としてログインします。
7. **SystemConfig** と入力します。Enter を押します。
8. メインメニューから [リカバリ (Recovery)] を選択します。
9. [アプライアンスの削除 (RemoveAppliance)] を選択します。画面に表示される指示に従ってアプライアンスを削除します。  
メニューが表示されない場合、アプライアンスはすでに Central Management から削除されて





**i** [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。以下を参照します：**1. Central Management からのアプライアンスの削除**

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. マネージャ信頼ストアからの古い証明書の削除

次の手順を使用して、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. 管理者としてマネージャにログインします：<https://<IPAddress>>
2. メインメニューから [構成 (Configure)] > [グローバル集中管理 (GLOBAL Central Management)] を選択します。
3. マネージャ アプライアンスのステータスは接続済みと表示されます。
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 のインベントリページで、マネージャ アプライアンスのステータスが [接続済み (Connected)] 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。

- 一元管理: マネージャ IP アドレス、パスワード、および Secure Network Analytics ドメイン。
  - 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。
    - 画面上のプロンプトに従って、プライマリ マネージャ アプライアンス アイデンティティ 証明書を信頼し、マネージャ 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。


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 [接続済み (Connected)] 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 [接続済み (Connected)] に変化します。アプライアンスが [接続済み (Connected)] に変化しない場合は、信頼ストアに古い証明書が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](#) および [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、(このセクションの指示ではなく)「[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](#)」の手順に従います。
- **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まだ切れていない場合は、「[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、次の要件を確認してください。

- **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**: マネージャ証明書と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関係を削除してください。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 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ことが含まれています。

## 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. メインメニューから [構成 (Configure)] > [グローバル集中管理 (GLOBAL Central Management)] を選択します。
3. [インベントリ (Inventory)] タブで、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 [構成チャンネルのダウン (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。

Inventory

2 Appliances found

Filter Appliance Inventory Table

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Channel Down	nflow-	Flow Collector FCNFVE-KVM-1	1.1.1.5	
Config Channel Down		Manager DVE-KVM	1.1.1.4	

## 2. アプライアンスの手順の選択

- マネージャおよび管理対象アプライアンス:** [マネージャおよび管理対象アプライアンス](#)を使用して、マネージャおよびクラスタ内の他の管理対象アプライアンスの証明書の有効期間を変更します。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。
- 個別の非マネージャアプライアンス:** [個別の非マネージャアプライアンス](#)を使用して、個別の非マネージャアプライアンス(Flow Collector、Flow Sensor および UDP ディレクタ)の証明書の有効期間を変更します。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対象アプライアンス

以下の手順に従って、クラスタ内のマネージャおよびその他の管理対象アプライアンスの証明書の有効期間を変更します。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:** マネージャ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関係を削除してください。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ことが含まれています。

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期限切れの証明書を削除する](#)
4. [Central Management へのアプライアンスの追加](#)

## 5. 信頼ストアからの期限切れ証明書の削除

## 6. マネージャフェールオーバーペアの設定

### 1. アプライアンスの削除と証明書の再生成

以下の手順に従って、クラスタ内のマネージャおよびその他の管理対象アプライアンスの証明書の有効期間を変更します。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。



マネージャのみを変更する必要がある場合でも、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、「[個別の非マネージャアプライアンス](#)」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:** 最後にマネージャでこれらの手順を完了します。
- **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。



マネージャを Central Management から削除します。

1. **アプライアンスを Central Management から削除:** 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 を完了した後、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 を完了した後、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。  
 マネージャ: マネージャにログインした場合すべてのシステム構成メニューを読み込めなかつ



```

lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x  Select a menu:                                     x
x  lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk x
x  x  Factory Defaults    Restore the appliance to its factory defaults.  x x
x  x  Refresh Image      Refresh the appliance image.             x x
x  x  Expired Identity    Generate a new appliance identity certificate. x x
x  x                                                             x x
x  x                                                             x x
x  x                                                             x x
x  x                                                             x x
x  x                                                             x x
x  x                                                             x x
x  x                                                             x x
x  mgqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqj x
x                                                             x
x                                                             x
x                                                             x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqquu
x                                <Select>                < Exit >                            x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqvqj
  
```

- 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。

```

lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk
x  You've successfully replaced the appliance identity certificate.  x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
x                                                             x
tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqquu
x                                                             x
x                                < OK >                            x
mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqvqj
  
```

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

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するには、次の手順に従います。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 フェイルオーバー: 2つある場合、この手順はプライマリでのみ実行する必要があります。セカンダリ マネージャを以下で登録します: [4. Central Management へのアプライアンスの追加](#)

**!** 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. 管理者としてマネージャにログインします: `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。画面の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。
  - これにより、マネージャに Central Management が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、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は接続済みと表示されます。

Inventory				
1 Appliances found				
Q Filter Appliance Inventory Table				
APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager /E-KVM-		

### 3. マネージャ信頼ストアから期限切れの証明書を削除する

2つのマネージャがある場合は、プライマリ マネージャでのみこの手順を完了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ました)。

**!** 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。マネージャおよび他の非マネージャ アプライアンス アイデンティティ証明書、ルート証明書、中間証明書) からの期限切れの証明書をすべて見つけます。
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 のインベントリページで、マネージャ アプライアンスのステータスが [接続済み (Connected)] 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。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 [接続済み (Connected)] になっていることを確認します。
- **一元管理:** マネージャ IP アドレス、パスワード、および Secure Network Analytics ドメイン。
- **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 Flow Replicator)	
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 [接続済み (Connected)] と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 [接続済み (Connected)] と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 [接続済み (Connected)] と表示されていることを確認します。

6.	セカンダリ マネージャ (使用されている場合)	セカンダリ マネージャ設定を開始する前に、プライマリ マネージャが [接続済み (Connected)] として表示されていることを確認してください。  二次マネージャ自身を中央マネージャとして選択します。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。「 <a href="#">6. マネージャフェールオーバーペアの設定</a> 」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。
  - **接続済み:** 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 [接続済み (Connected)] になってい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、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、それ自体を中央マネージャとして選択します。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。「[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。画面上のプロンプトに従って、プライマリ マネージャアプライアンスアイデンティティ証明書を信頼し、マネージャ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。

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 [接続済み (Connected)] 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 [接続済み (Connected)] 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 [接続済み (Connected)] 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 [設定の順序と詳細](#) を使用して Central Management に追加します。


The screenshot shows the 'Inventory' section of the Central Management interface. It displays a table with 4 appliances found, all with a status of 'Connected'. The table has columns for Appliance Status, Host Name, and Type. A red box highlights the 'Connected' status for all four appliances.

Appliance Status	Host Name	Type
Connected	sr- [redacted]	Manager
Connected	nflow- [redacted]	Flow Collector
Connected	fs- [redacted]	Flow Sensor
Connected	fr-740 [redacted]	UDP Director

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が保存される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から期限切れの証明書(アイデンティティ、ルート、中間証明書)をすべて見つけます。
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 のインベントリページで、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 [接続済み(Connected)] 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


マネージャをフェールオーバーペアとして再設定するには、『[Failover Configuration Guide](#)』の手順に従ってください。

### 個別の非マネージャアプライアンス

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期限切れの証明書を削除する](#)

### 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間を変更する必要がある場合は、「**マネージャおよび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. **アプライアンスを Central Management から削除**: 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。

```

lqaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaRecoveryaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaak
x Select a menu: x
x lqaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaak x
x x RemoveAppliance Remove appliance from Central Management x x
x x Factory Defaults Restore the appliance to its factory defaults. x x
x x Refresh Image Refresh the appliance image. x x
x x x x
x x x x
x x x x
x x x x
x x x x
x x x x
x x x x
x maaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa] x
x x
x x
x x
taaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaau
x x <Select> < Exit > x
maaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa]

```


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。



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期限切れの証明書を削除する

次の手順を使用して、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. 管理者としてマネージャにログインします : `https://<IPAddress>`
2. マネージャアプライアンスのステータスは接続済みと表示されます。
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 のインベントリページで、マネージャアプライアンスのステータスが [接続済み (Connected)] 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。

- 一元管理: マネージャ IP アドレス、パスワード、および Secure Network Analytics ドメイン。
  - 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。
    - 画面上のプロンプトに従って、プライマリ マネージャアプライアンス アイデンティティ証明書を信頼し、マネージャ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。

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 [接続済み (Connected)] 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 [接続済み (Connected)] に変化します。アプライアンスが [接続済み (Connected)] に変化しない場合は、信頼ストアに古い証明書が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](#) および [信頼ストアからの証明書の削除](#)」を参照してください。

Central Management | Inventory | Update Manager | App Manager | Smart Licensing | Database

Inventory

4 Appliances found


Filter Appliance Inventory Table

Appliance Status	Host Name	Type
Connected	sr	Manager
Connected	nflow-	Flow Collector
Connected	fs-	Flow Sensor
Connected	fr-740	UDP Director



# 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。次の手順を使用して、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

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 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、既存のアプライアンス アイデンティティ証明書を新しい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する](#)の証明書を信頼する

### 1. 証明書署名要求の生成

次の手順に従って、証明書署名要求 (CSR) を準備します。

1. [Central Management を開きます](#)。
2. インベントリ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を生成する必要がある場合は、「[Central Management での CSR の省略](#)」に進みません。

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、またはアイデンティティ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、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. インベントリタブ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 Collectors
- フローセンサーs
- UDP Director
- マネージャs

**!** 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。

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
[Redacted]	fs-7	fs-7	2020-11-20 17:51:53	2025-11-20 17:51:53	[Redacted]	8192 bits	Delete
[Redacted]	1.la	1.la	[Redacted]	[Redacted]	3	[Redacted]	Delete
[Redacted]	m	m	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	m	m	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	121-	121-	2020-11-20 17:42:20	2025-11-20 17:42:20	[Redacted]	8192 bits	Delete
[Redacted]	1.lanc	1.lanc	[Redacted]	[Redacted]	39	[Redacted]	Delete
[Redacted]	m	m	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]

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** 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。

アプライアンスの 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/ 中央管理者	マネージャ証明書をマネージャ信頼ストアと 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。	<ul style="list-style-type: none"> <li>• プライマリ マネージャ</li> <li>• Flow Collector</li> <li>• Flow Collector データベース (5000 シリーズのみ)</li> <li>• Flow Sensor</li> </ul>


		<ul style="list-style-type: none"> <li>• UDP Director</li> <li>• セカンダリ マネージャ (フェールオーバーのみ)</li> </ul>
セカンダリ マネージャ (フェールオーバーのみ)	<p>マネージャがフェールオーバー用に設定されており、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場合は、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。</p> <p>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、<a href="#">フェールオーバーコンフィギュレーションガイド</a> [英語] を参照してフェールオーバーを設定します。</p>	<ul style="list-style-type: none"> <li>• Flow Collector</li> <li>• Flow Collector データベース (5000 シリーズのみ)</li> <li>• Flow Sensor</li> <li>• UDP Director</li> <li>• セカンダリ マネージャ (フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul>
Flow Collector	<p>Flow Collector 証明書を Flow Collector 信頼ストアとマネージャ信頼ストアに追加します。</p> <p><b>5000 シリーズのみ:</b></p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>	<ul style="list-style-type: none"> <li>• Flow Collector</li> <li>• Flow Collector データベース (5000 シリーズのみ)</li> <li>• セカンダリ マネージャ (フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul>
Flow Sensor	<p>Flow Sensor 証明書を Flow Sensor 信頼ストアとマネージャ信頼ストアに追加します。</p>	<ul style="list-style-type: none"> <li>• Flow Sensor</li> <li>• セカンダリ マネージャ (フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul>

UDP Director	UDP Director 証明書を UDP Director 信頼ストアとマネージャ信頼ストアに追加します。	<ul style="list-style-type: none"> <li>• UDP Director</li> <li>• セカンダリ マネージャ (フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul>
高可用性ペアの UDP Director	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>	<ul style="list-style-type: none"> <li>• セカンダリ UDP Director (高可用性のみ)</li> <li>• プライマリ UDP Director (高可用性のみ)</li> <li>• セカンダリ マネージャ (フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul>

### 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. インベントリ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、証明書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. [集中管理 (Central Management)] の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 [接続済み (Connected)] 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ることを確認します。

**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、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 [接続済み (Connected)] 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 の証明書を信頼する

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ているデフォルトの信頼ストアに保存されている証明書のみを信頼します。

1. 管理者としてマネージャにログインします : `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 アイデンティティ証明書**の要件を満たす証明書がすでにある場合、次の手順を使用して、現在のアプライアンス アイデンティティ証明書を新しいアプライアンス 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 の証明書を信頼する

#### 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、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. インベントリタブ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 Collectors
- 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。

Trust Store							Add New
FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
nmxm	fs-7	fs-7	2020-11-20 17:51:53	2025-11-20 17:51:53		8192 bits	Delete
nzq1o	1.la	1.la					
rm0yz	m	m			3		
wnmzd							
	9-		2020-11-20 17:42:20	2025-11-20 17:42:20		8192 bits	Delete
	121-	121-					
	1.lanc	1.lanc			39		
	m	m					

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** 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。

アプライアンスの 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	マネージャ証明書をマネージャ	<ul style="list-style-type: none"> <li>• プライマリ マネージャ</li> </ul>

中央管理者	信頼ストアと 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。	<ul style="list-style-type: none"> <li>• Flow Collector</li> <li>• Flow Collector データベース (5000 シリーズのみ)</li> <li>• Flow Sensor</li> <li>• UDP Director</li> <li>• セカンダリ マネージャ (フェールオーバーのみ)</li> </ul>
セカンダリ マネージャ (フェールオーバーのみ)	<p>マネージャがフェールオーバー用に設定されており、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場合は、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。</p> <p>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、<a href="#">フェールオーバーコンフィギュレーションガイド [英語]</a> を参照してフェールオーバーを設定します。</p>	<ul style="list-style-type: none"> <li>• Flow Collector</li> <li>• Flow Collector データベース (5000 シリーズのみ)</li> <li>• Flow Sensor</li> <li>• UDP Director</li> <li>• セカンダリ マネージャ (フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul>
Flow Collector	<p>Flow Collector 証明書を Flow Collector 信頼ストアとマネージャ信頼ストアに追加します。</p> <p><b>5000 シリーズのみ:</b></p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>	<ul style="list-style-type: none"> <li>• Flow Collector</li> <li>• Flow Collector データベース (5000 シリーズのみ)</li> <li>• セカンダリ マネージャ (フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul>



Flow Sensor	Flow Sensor 証明書を Flow Sensor 信頼ストアとマネージャ信頼ストアに追加します。	<ul style="list-style-type: none"> <li>Flow Sensor</li> <li>セカンダリ マネージャ (フェールオーバーのみ)</li> <li>プライマリ マネージャ</li> </ul>
UDP Director	UDP Director 証明書を UDP Director 信頼ストアとマネージャ信頼ストアに追加します。	<ul style="list-style-type: none"> <li>UDP Director</li> <li>セカンダリ マネージャ (フェールオーバーのみ)</li> <li>プライマリ マネージャ</li> </ul>
高可用性ペアの UDP Director	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> </ul>	<ul style="list-style-type: none"> <li>セカンダリ UDP Director (高可用性のみ)</li> <li>プライマリ UDP Director (高可用性のみ)</li> <li>セカンダリ マネージャ (フェールオーバーのみ)</li> <li>プライマリ マネージャ</li> </ul>

## 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. インベントリタブ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。最後にマネージャを更新します。
3. [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。
4. [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 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. [集中管理 (Central Management)] の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 [接続済み (Connected)] 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ることを確認します。

**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 ~ 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 [接続済み (Connected)] 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 の証明書を信頼する

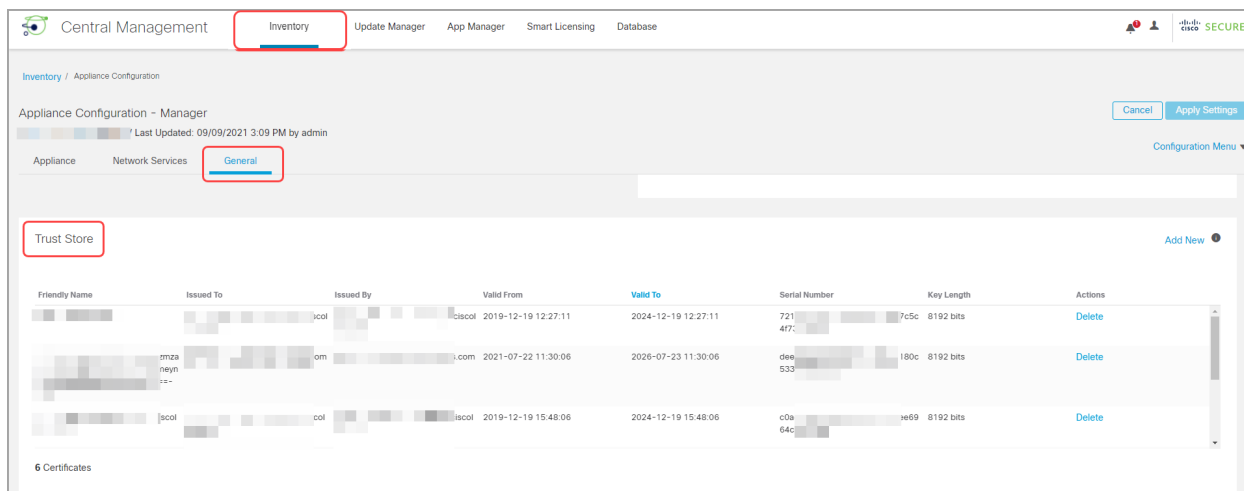
デスクトップ クライアント は、ローカルコンピュータにインストールされているデフォルトの信頼ストアに保存されている証明書のみを信頼します。

1. 管理者としてマネージャにログインします : `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。

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
[Redacted]	nmxm fs-7 nzq1o 1.la	fs-7 1.la	2020-11-20 17:51:53	2025-11-20 17:51:53	[Redacted]	8192 bits	Delete
[Redacted]	mi0yz m wnmzd	m			3		
[Redacted]	9- 121- 1.lanc m	121- 1.lanc m	2020-11-20 17:42:20	2025-11-20 17:42:20	[Redacted]	8192 bits	Delete
[Redacted]					39		

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 のインベントリページで、アプライアンスのステータスが [接続済み (Connected)] 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化されます。

アプライアンスの アイデンティティ証明書	信頼ストア
マネージャ 中央管理者	<ul style="list-style-type: none"> <li>プライマリ マネージャ</li> <li>Flow Collector</li> <li>Flow Collector データベース (5000 シリーズのみ)</li> <li>Flow Sensor</li> <li>UDP Director</li> <li>セカンダリ マネージャ (フェールオーバーのみ)</li> </ul>
セカンダリ マネージャ (フェールオーバーのみ)	<ul style="list-style-type: none"> <li>Flow Collector</li> <li>Flow Collector データベース (5000 シリーズのみ)</li> <li>Flow Sensor</li> <li>UDP Director</li> <li>セカンダリ マネージャ (フェールオーバーのみ)</li> <li>プライマリ マネージャ</li> </ul> <p><b>マネージャフェールオーバー</b> マネージャフェールオーバー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</p>

	<p>す。詳細と手順については、『<a href="#">フェールオーバー コンフィギュレーション ガイド</a>』を参照してください。</p>
Flow Collector	<ul style="list-style-type: none"> <li>• Flow Collector</li> <li>• セカンダリ マネージャ(フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul> <p><b>5000 シリーズのみ:</b></p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
Flow Sensor	<ul style="list-style-type: none"> <li>• Flow Sensor</li> <li>• セカンダリ マネージャ(フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul>
UDP Director	<ul style="list-style-type: none"> <li>• UDP Director</li> <li>• セカンダリ マネージャ(フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul>
高可用性ペアの UDP Director	<ul style="list-style-type: none"> <li>• セカンダリ UDP Director(高可用性のみ)</li> <li>• プライマリ UDP Director(高可用性のみ)</li> <li>• セカンダリ マネージャ(フェールオーバーのみ)</li> <li>• プライマリ マネージャ</li> </ul>

# 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。

- 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。
- マネージャフェールオーバー: マネージャ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。 [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: [非マネージャアプライアンス](#)

**!** マネージャおよび別のアプライアンス (Flow Collector など) のホスト名またはネットワークドメイン名を変更する場合は、マネージャの手順を最初に行います。

## マネージャ

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、次の手順を使用します。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。

**マネージャフェールオーバー:** マネージャがフェールオーバーペアとして設定されている場合は、これらの設定を変更する前にフェールオーバー関係を削除してください。[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を変更します。](#) を変更する
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 [接続済み (Connected)] 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。
  - インベントリタブ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。
  - **構成チャネルのダウン:** アプライアンスのステータスが [構成チャネルのダウン (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 [接続済み (Connected)] と表示されていることを確認します。

Inventory

1 Appliances found

Q Filter Appliance Inventory Table

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager		

5. プライマリ マネージャを Central Management から削除します。
  - [在庫 (Inventory)] タブで、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。
  - **構成チャネルのダウン**: アプライアンスのステータスが [構成チャネルのダウン (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を変更します。

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**: マネージャが 2 つある場合、この手順は プライマリ マネージャでのみ完了する必要があります。セカンダリ マネージャを以下で登録します: [3. Central Management へのアプライアンスの追加](#)

1. 管理者としてマネージャにログインします: `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。

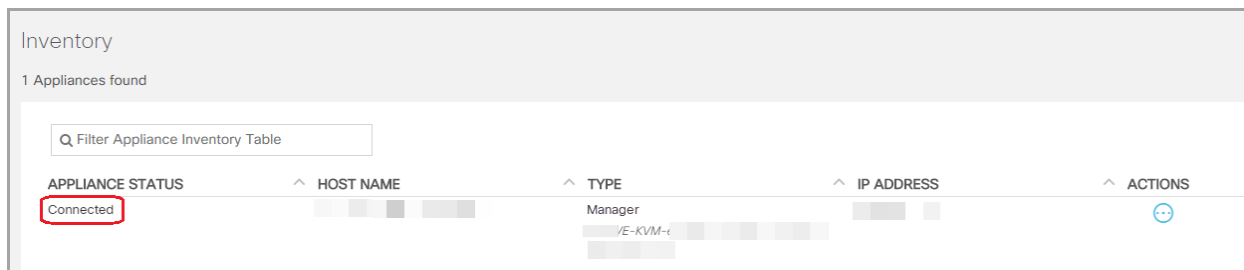
2. [続行/次へ (Continue/Next)] をクリックし、[ホスト名とドメイン (Host Name and Domains)] タブまでスクロールします。
3. フィールドに新しいホスト名またはネットワークドメイン名を入力します。

**!** 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。

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。画面の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。
  - これにより、Central Management がマネージャ上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、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 [接続済み (Connected)] 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。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 [接続済み (Connected)] になってい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 Flow Replicator)	
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 [接続済み (Connected)] と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 [接続済み (Connected)] と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 [接続済み (Connected)] と表示されていることを確認します。
6.	セカンダリ マネージャ (使用されている場合)	セカンダリ マネージャ設定を開始する前に、プライマリ マネージャが [接続済み (Connected)] として表示されていることを確認してください。 セカンダリ マネージャは、それ自体を 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。 <a href="#">5. マネージャフェールオーバーペアの設定</a> を構成します。

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。
  - **接続済み:** 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 [接続済み (Connected)] になってい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、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、それ自体を中央マネージャとして選択します。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。[5. マネージャフェールオーバーペアの設定](#)を構成します。
  - **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。画面上のプロンプトに従って、プライマリ マネージャアプライアンスアイデンティティ証明書を信頼し、マネージャ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。

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 [接続済み (Connected)] 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 [接続済み (Connected)] 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 [接続済み (Connected)] 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 [設定の順序と詳細](#) を使用して Central Management に追加します。


The screenshot shows the 'Central Management' interface with the 'Inventory' tab selected. It displays a table of 4 appliances, all with a 'Connected' status. A red box highlights the 'Connected' status column.

Appliance Status	Host Name	Type
Connected	sr- [redacted]	Manager
Connected	nflow- [redacted]	Flow Collector
Connected	fs- [redacted]	Flow Sensor
Connected	fr-740 [redacted]	UDP Director

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が保存される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、およびルート) 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 [接続済み (Connected)] 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

マネージャをフェールオーバーペアとして再設定するには、『[Failover Configuration Guide](#)』の手順に従ってください。

## 非マネージャアプライアンス

マネージャ以外のアプライアンス (Flow Collector、MadCap:variable name="GlobalVariables.FSFullName" />、および UDP Director) で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、次の手順を使用します。


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](#)

 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 [接続済み (Connected)] 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。

**構成チャネルのダウン:** アプライアンスのステータスが [構成チャネルのダウン (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 (Remove Appliance)] 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 (Remove Appliance)] 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。

 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。

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 マネージャにログインします。
  - アプライアンスが Central Management インベントリに表示されていることを確認します。
  - [アプライアンスステータス (Appliance Status)] が [接続済み (Connected)] 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 [接続済み (Connected)] に変化します。アプライアンスが [接続済み (Connected)] に変化しない場合は、信頼ストアに古い証明書が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](#)および[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 (フロー コレクタ 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:** マネージャがフェールオーバーペアとして設定されている場合は、フェールオーバー関係を削除します。 [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:** [非マネージャ アプライアンス](#)



マネージャおよび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、マネージャの手順を最初に実行します。

## マネージャ

マネージャ IP アドレス (eth0 ネットワーク インターフェイス) を変更するには、次の手順を使用します。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。

**マネージャフェールオーバー:** マネージャがフェールオーバーペアとして設定されている場合は、これらの設定を変更する前にフェールオーバー関係を削除してください。 [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 [接続済み (Connected)] 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。
  - インベントリタブ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。
  - **構成チャネルのダウン**: アプライアンスのステータスが [構成チャネルのダウン (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 [接続済み (Connected)] と表示されていることを確認します。

Inventory				
1 Appliances found				
<input type="text" value="Filter Appliance Inventory Table"/>				
APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager		
		/E-KVM-		

5. プライマリ マネージャを Central Management から削除します。
  - [在庫 (Inventory)] タブで、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。

- **構成チャネルのダウン:** アプライアンスのステータスが [構成チャネルのダウン (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

次の手順に従って、マネージャ 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 に登録します。

**マネージャフェールオーバー:** マネージャが 2 つある場合、この手順はプライマリ マネージャでのみ完了する必要があります。セカンダリ マネージャを以下で登録します: [3. Central Management へのアプライアンスの追加](#)

1. 管理者としてマネージャにログインします: `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。画面の指示に従ってマネージャを再起動します。
6. マネージャ (新しい IP アドレスを使用) にログインします。
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。
  - これにより、Central Management がマネージャ上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、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は接続済みと表示されます。

Inventory				
1 Appliances found				
<input type="text" value="Filter Appliance Inventory Table"/>				
APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager		

### 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。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 [接続済み (Connected)] になってい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 Flow Replicator)	
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 [接続済み (Connected)] と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 [接続済み (Connected)] と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 [接続済み (Connected)] と表示されていることを確認します。
6.	セカンダリ マネージャ (使用されている場合)	セカンダリ マネージャ設定を開始する前に、プライマリ マネージャが [接続済み (Connected)] として表示されていることを確認してください。  セカンダリ マネージャは、それ自体を 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。「 <a href="#">5. マネージャフェールオーバーペアの設定</a> 」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。
  - **接続済み:** 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 [接続済み (Connected)] になってい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、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、それ自体を中央マネージャとして選択します。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。「[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。画面上のプロンプトに従って、プライマリ マネージャ アプライアンス アイデンティティ証明書を信頼し、マネージャ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 [接続済み (Connected)] 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 [接続済み (Connected)] 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 [接続済み (Connected)] 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 [設定の順序と詳細](#) を使用して Central Management に追加します。

The screenshot shows the 'Central Management' interface with the 'Inventory' tab selected. It displays '4 Appliances found' and a search filter. Below is a table with columns for Appliance Status, Host Name, and Type. The 'Appliance Status' column for all four entries is highlighted with a red box and contains the text 'Connected'.

Appliance Status	Host Name	Type
Connected	sr	Manager
Connected	nflow-	Flow Collector
Connected	fs-	Flow Sensor
Connected	fr-740	UDP Director

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が保存される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、およびルート) 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 のインベントリページで、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 [接続済み (Connected)] 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

マネージャをフェールオーバーペアとして再設定するには、『[Failover Configuration Guide](#)』の手順に従ってください。

## 非マネージャ アプライアンス

マネージャ以外のアプライアンス (Flow Collector、MadCap:variable name="GlobalVariables.FSFullName" />、および UDP Director) で IP アドレスを変更するには、次の手順を使用します。

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 [接続済み (Connected)] 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。

**構成チャネルのダウン:** アプライアンスのステータスが [構成チャネルのダウン (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 (Remove Appliance)] 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 (Remove Appliance)] 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。  
アプライアンスが再起動します。
6. 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)。
7. [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。
8. プライマリ マネージャにログインします。
  - アプライアンスが Central Management インベントリに表示されていることを確認します。
  - [アプライアンスステータス (Appliance Status)] が [接続済み (Connected)] 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 [接続済み (Connected)] に変化します。アプライアンスが [接続済み (Connected)] に変化しない場合は、信頼ストアに古い証明書が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](#)および[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、およびサーバーアイデンティティ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。❓ ([ヘルプ (Help)]) アイコン > [ヘルプ (Help)] を選択します。[監査ログの宛先 (Audit Log Destination)] を検索します。
- **Cisco ISE または Cisco ISE-Pic:** 『[ISE-PIC Configuration Guide](#)』の手順に従います。
- **LDAP:** ヘルプの手順に従います。❓ ([ヘルプ (Help)]) アイコン > [ヘルプ (Help)] を選択します。「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。❓ ([ヘルプ (Help)]) アイコン > [ヘルプ (Help)] を選択します。「パケットアナライザ」を検索します。
- **SAML SSO:** 『[System Configuration Guide](#)』の手順に従います。
- **応答管理に対する SMTP の設定:** ヘルプの指示に従ってください。❓ ([ヘルプ (Help)]) アイコン > [ヘルプ (Help)] を選択します。「SMTP 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

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

次の手順に従って、証明書署名要求 (CSR) を準備します。

1. [Central Management](#) を開きます。
2. [インベントリ (Inventory)] タブで、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 を生成する必要がある場合は、「[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、またはクライアントアイデンティティ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. [インベントリ(Inventory)] タブで、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。

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
mmxm	fs-7	fs-7	2020-11-20 17:51:53	2025-11-20 17:51:53		8192 bits	Delete
nzq1o	1.la	1.la					
mi0yz	m	m			3		
wnmzd							
9-			2020-11-20 17:42:20	2025-11-20 17:42:20		8192 bits	Delete
121-	1.lanc	121-			39		
m	m	m					

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. [インベントリ(Inventory)] タブで、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、証明書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まないでください。

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ることを確認します。

## 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](#)の要件を満たす証明書をすでにお持ちの場合は、次のコマンドを使用してそれらを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. [インベントリ (Inventory)] タブで、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。

Trust Store							Add New
FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
mmxm	fs-7	fs-7	2020-11-20 17:51:53	2025-11-20 17:51:53		8192 bits	Delete
nzq1o	1.la	1.la					
mi0yz	m	m			3		
wnmzd							
9-	121-	121-	2020-11-20 17:42:20	2025-11-20 17:42:20		8192 bits	Delete
	1.lanc	1.lanc			39		
	m	m					

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. [インベントリ (Inventory)] タブで、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](#)に移動してください。

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ることを確認します。

## 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、ログインする前に証明書を選択するように求められる場合があります。このダイアログは、Secure Network Analytics にログインできるかどうかには影響しません。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。

**!** マネージャを Central Management から削除します。

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。

```

lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqRecoveryqqqqqqqqqqqqqqqqqqqqqqqqqqqqkk
x Select a menu:                                                                 x
x lqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqk  x
x x RemoveAppliance          Remove appliance from Central Management   x x
x x Factory Defaults       Restore the appliance to its factory defaults.  x x
x x Refresh Image          Refresh the appliance image.                   x x
x x                                                                        x x
x x                                                                        x x
x x                                                                        x x
x x                                                                        x x
x x                                                                        x x
x x                                                                        x x
x x                                                                        x x
x x                                                                        x x
x mqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq] x
x                                                                            x
x                                                                            x
x tqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq]u
x                                                                            x
x <Select>                   < Exit >                                       x
x qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq]  x

```

- 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。

## [アプライアンスステータス (Appliance Status)] に [接続済み (Connected)] ではなく [初期化中 (Initializing)] と表示される

アプライアンスのステータスが [初期化中 (Initializing)] または [構成チャネルのダウン (Config Channel Down)] と表示され、[接続済み (Connected)] 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](mailto: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>



## 変更履歴

マニュアルのバージョン	公開日	説明
1_0	2023 年 3 月	最初のバージョン。

---

## 著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、URL: <https://www.cisco.com/go/trademarks> をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パートナー」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)

