



# Cisco Secure Network Analytics

管理対象アプライアンスの SSL/TLS 証明書 7.5.0



---

# 目次

はじめに	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
期限が切れる前に証明書を置き換える	8
ネットワーク設定の変更	8
Manager フェールオーバー	9
アプライアンスのアイデンティティ証明書	9
認証	9
証明書の要件	9
サブジェクト代替名 (SAN)	11
証明書のテスト	11
自己署名証明書	11
認証局によって署名された証明書 (チェーンの長さ = 2)	12
認証局によって署名された証明書 (チェーンの長さ > 2)	12
クライアント アイデンティティ証明書	12
証明書の要件	12
PEM チェーンファイルの要件	13
信頼ストアの要件	14
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)	14
追加の証明書の設定	14
[集中管理 (Central Management)] を開く	15
[アプライアンスステータス (Appliance Status)] が [接続済み (Connected)] であることの確認	15
概要	16
TLS バージョンの変更	18
証明書の確認	19
証明書の保存	20
シスコのバンドルのダウンロード	21
証明書期限切れの通知を受け取る	22
システムアラーム	22
電子メール通知	22

---

以前に有効にされた電子メール通知 .....	22
最近有効にされた電子メール通知 .....	22
カスタム電子メール通知の作成 .....	23
1. アクションの作成 .....	23
2. ルールの作成 .....	25
電子メール通知の無効化 .....	26
電子メール通知の有効化 .....	28
<b>期限切れになっていない、または期限切れの証明書の置換(概要) .....</b>	<b>29</b>
<b>期限切れになっていないシスコのデフォルト証明書の置換(証明書の更新) .....</b>	<b>30</b>
要件 .....	30
すべてのアプライアンスまたは選択したアプライアンスでの証明書の更新 .....	30
概要 .....	31
1. アプライアンスのステータスの確認 .....	31
2. 証明書の生成 .....	32
3. [集中管理(Central Management)] の確認 .....	35
4. 信頼ストアの確認 .....	36
<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>37</b>
要件 .....	37
1. アプライアンスのステータスの確認 .....	37
2. アプライアンスの手順の選択 .....	38
<b>Manager と管理対象アプライアンス .....</b>	<b>38</b>
概要 .....	39
1. Data Store データベースを停止する .....	39
2. Central Management からのアプライアンスの削除 .....	39
3. アプライアンス アイデンティティ証明書の再生成 .....	40
4. [集中管理(Central Management)] への Manager の登録 .....	42
5. 信頼ストアからの期限切れ証明書の削除 .....	43
6. Central Management へのアプライアンスの追加 .....	44
アプライアンスの設定順序 .....	44
7. Data Store データベースの開始 .....	46
8. 信頼ストアからの期限切れ証明書の削除 .....	46
9. Manager フェールオーバーペアの設定 .....	47
<b>Manager 以外の個別のアプライアンス .....</b>	<b>47</b>
概要 .....	47
1. Data Store データベースを停止する .....	48

---

2. アプライアンスの削除と証明書の再生成 .....	48
3. 信頼ストアからの期限切れ証明書の削除 .....	50
4. Central Management へのアプライアンスの追加 .....	51
5. Data Store データベースの開始 .....	52
<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>53</b>
証明書の要件 .....	53
環境に応じた手順の選択 .....	53
Central Management での CSR の生成 .....	53
概要 .....	53
1. 証明書署名要求の生成 .....	53
2. ルート CA 証明書を信頼ストアに追加する .....	54
信頼ストアの要件 .....	55
3. Data Store データベースを停止する .....	57
4. アプライアンス アイデンティティ証明書の置換 .....	57
5. デスクトップ クライアントで証明書を信頼する .....	58
[集中管理 (Central Management)] での CSR の省略 .....	58
概要 .....	58
1. 信頼ストアへの必要な証明書の追加 .....	58
信頼ストアの要件 .....	59
2. Data Store データベースを停止する .....	61
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 クライアントで証明書を信頼する .....	62
<b>信頼ストアの証明書の確認 .....</b>	<b>63</b>
信頼ストアからの証明書の削除 .....	63
信頼ストア の場所 .....	64
<b>ホスト名またはネットワークドメイン名の変更 .....</b>	<b>66</b>
最新の設定の確認 .....	66
ホスト名またはネットワークドメイン名の変更 .....	66
要件 .....	66
アプライアンスの手順の選択 .....	67
Manager .....	67
概要 .....	67
1. Data Store データベースを停止する .....	67
2. Central Management からのアプライアンスの削除 .....	68
3. Manager のホスト名またはネットワークドメイン名の変更 .....	69

---

4. [集中管理 (Central Management)] への Manager の登録	69
5. Central Management へのアプライアンスの追加	70
アプライアンスの設定順序	70
6. Data Store データベースの開始	72
7. 信頼ストアからの古い Manager 証明書の削除	72
8. Manager フェールオーバーペアの設定	72
Manager 以外のアプライアンス	73
概要	73
1. Data Store データベースを停止する	73
2. Central Management からのアプライアンスの削除	74
3. 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	74
4. [集中管理 (Central Management)] へのアプライアンスの追加	74
5. Data Store データベースの開始	75
<b>ネットワーク インターフェイスの変更</b>	<b>76</b>
最新の設定の確認	76
[集中管理 (Central Management)] でのネットワーク インターフェイスの変更	76
アプライアンスの IP アドレスの変更	77
要件	77
アプライアンスの手順の選択	77
Manager	78
概要	78
1. Central Management からのアプライアンスの削除	78
2. Manager IP アドレスの変更	79
3. [集中管理 (Central Management)] への Manager の登録	79
4. Central Management へのアプライアンスの追加	80
アプライアンスの設定順序	80
5. 信頼ストアからの古い Manager 証明書の削除	82
6. Manager フェールオーバーペアの設定	82
Manager 以外のアプライアンス	83
概要	83
1. Central Management からのアプライアンスの削除	83
2. アプライアンスの IP アドレスの変更	84
3. [集中管理 (Central Management)] へのアプライアンスの追加	84
<b>SSL/TLS クライアントアイデンティティの追加</b>	<b>85</b>
追加の証明書の設定	85

---

---

証明書の要件 .....	85
環境に応じた手順の選択 .....	85
Central Management での CSR の生成 .....	86
概要 .....	86
1. 証明書署名要求の生成 .....	86
2. 信頼ストアへの証明書の追加 .....	87
3. クライアントアイデンティティ証明書の追加 .....	87
Central Management での CSR の省略 .....	88
概要 .....	88
1. 信頼ストアへの証明書の追加 .....	88
2. クライアントアイデンティティ証明書の追加 .....	89
<b>クライアントアイデンティティ証明書の削除 .....</b>	<b>90</b>
<b>トラブルシューティング .....</b>	<b>91</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。 .....	91
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。 .....	91
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。 .....	91
[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 .....	92
<b>サポートへの問い合わせ .....</b>	<b>93</b>
<b>変更履歴 .....</b>	<b>94</b>

## はじめに

Cisco Secure Network Analytics (旧 Stealthwatch) v7.5.0 アプライアンス (旧 Stealthwatch Management Console (SMC)) の SSL/TLS 証明書関連の設定を変更するには、このガイドを使用します。

- Cisco Secure Network Analytics Manager
- Cisco Secure Network Analytics Flow Collector
- Cisco Secure Network Analytics Flow Sensor
- Cisco Secure Network Analytics UDP Director
- Cisco Secure Network Analytics データノード

詳細については、「[概要](#)」を参照してください。

## DoDIN およびコモンクライテリアへの準拠

米国国防総省情報ネットワーク (DoDIN) またはコモンクライテリア (CC) に準拠するように Secure Network Analytics を設定するには、『DoDIN 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すべての Secure Network Analytics 製品に対し「アプライアンス」という用語を使用しています。

「**クラスタ**」は、Manager が管理する Secure Network Analytics アプライアンスのグループです。

アプライアンス アイデンティティ証明書はリーフ証明書です。

## 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 [集中管理 (Central Management)] から削除し、[集中管理 (Central Management)] に再度追加する順序と手順に従ってください。

**Manager:** Manager で期限切れのアプライアンス アイデンティティ証明書をシスコ自己署名アプライアンス アイデンティティ証明書と置き換える場合は、すべてのアプライアンスを (表示されている順序で) [集中管理 (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。

**Manager 以外のアプライアンス:** たとえば、Manager 以外の個別のアプライアンス (Flow Collector、Flow Sensor、UDP Director、または Data Node) 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シスコ自己署名アプライアンス アイデンティティ証明書と置き換える場合、必要な操作は、各アプライアンスを [集中管理 (Central Management)] から削除し、変更後に [集中管理 (Central Management)] に再度追加するだけで済みます。

- **Data Store:** このガイドに含まれる多くの手順では、Data Store データベースを停止する必要があります。データベースを停止せずに、3 つ以上の Data Node がある状況で操作する場合は、[シスコサポート](#) に連絡してサポートを求めてください。

## 期限が切れる前に証明書を置き換える

- ⚠️ アプライアンス アイデンティティ証明書は、期限切れになる前に必ず置き換えてください。有効期限を確認するには、「[証明書の確認](#)」の手順に従います。

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は、次の手順で置き換えることができます。

- **シスコの証明書 (証明書の更新):** すべてまたは選択したアプライアンスで新しいシスコ自己署名アプライアンス アイデンティティ証明書を生成するには、「[期限切れになっていないシスコのデフォルト証明書の置換 \(証明書の更新\)](#)」を参照してください。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。
- **カスタム証明書:** 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、「[アプライアンスのアイデンティティ証明書](#)」記載の要件と、「[SSL/TLS アプライアンス アイデンティティ証明書の置換](#)」記載の手順を参照してください。

証明書の有効期限がすでに切れている場合は、「[期限切れになったシスコのデフォルト証明書の置換](#)」記載の手順を参照するか、カスタム証明書に置き換えてください。

## ネットワーク設定の変更

ネットワーク設定 ([ホスト名](#)、[ネットワークドメイン名](#)、または [eth0 IP アドレス](#)) を変更すると、新しいアプライアンス アイデンティティ証明書を生成するように求められることがあります。画面に表示される指示に従って、証明書の再生成が必要かどうか、または証明書を保持するを選択できるかどうかを確認してください。

- ⚠️ **カスタム証明書を使用している場合は、誤って証明書を上書きした場合に備えて、ネットワーク設定 (ホスト名、ネットワークドメイン名、または eth0 IP アドレス) を変更する前に、証明書を保存します。シスコ自己署名アプライアンス 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、次の手順に従います：[SSL/TLS アプライアンス アイデンティティ 証明書の置換](#)。

⚠ このガイドを使用して Data Node の eth0 ネットワークインターフェイスを変更することは避けてください。Data Node の eth0 IP アドレスを変更する場合は、[シスコサポート](#)に連絡して専門家のサポートを求めてください。

## Manager フェールオーバー

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

## アプライアンスのアイデンティティ証明書

各 Secure Network Analytics アプライアンスは固有の自己署名アプライアンス アイデンティティ証明書と一緒にインストールされます。

### 認証

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

### 証明書の要件

Secure Network Analytics アプライアンスの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、以下の手順に従います。

- 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。
- **[集中管理(Central Management)] でCSRを生成**:[集中管理(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(「[\[集中管理\(Central Management\)\] でCSRを生成](#)」の列を参照)。
- **[集中管理(Central Management)] でCSRをスキップする**:[集中管理(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(「[\[集中管理\(Central Management\)\] でCSRをスキップ](#)」の列を参照)。
- **証明書要件の検証とテスト**:[集中管理(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	CSR の作成 (Central Management で操作)	CSR のスキップ (Central Management で操作)
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 *	RSA キーの長さ 使用可能: 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	必要な RSA キーの長さ: 2048ビット(非推奨)以上 または 必要な ECDSA キーカーブ: 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。 <ul style="list-style-type: none"> <li>• 信頼ストア内の他の証明書 と比較される一意のサブ ジェクト名(日付、識別子、 文字列など)</li> </ul> または <ul style="list-style-type: none"> <li>• 権限キー識別子とサブジェ クトキー識別子。これらの</li> </ul>	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。 <ul style="list-style-type: none"> <li>• 一意のサブジェクト名(日 付、識別子、文字列など)</li> </ul> または <ul style="list-style-type: none"> <li>• 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 用する場合は、置き換える</li> </ul>

要件	CSR の作成 (Central Management で操作)	CSR のスキップ (Central Management で操作)
	キー識別子を使用する場合は、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、デフォルトのアプライアンスアイデンティティ証明書には含まれていません。	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、デフォルトのアプライアンス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。

\*[集中管理(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。

## サブジェクト代替名(SAN)

アプライアンスのネットワーク IP モード設定により、シスコ自己署名証明書の SAN が決定されます。[CSRを生成する](#)場合は次のようになります。

- IPv4:IPv4 SAN
- IPv6:IP SAN は使用不可
- デュアルスタック:IPv4 SAN

ネットワーク IP モードの詳細については、『[System Configuration Guide](#)』[英語]を参照してください。

## 証明書のテスト

アプライアンス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 [集中管理(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 [集中管理(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> <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>
```

## 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。
- [集中管理(Central Management)] でCSRを生成:** [集中管理(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(「[集中管理(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	CSR の作成 (Central Management で操作)	CSR のスキップ (Central Management で操作)
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> 。	PKCS#12(p12、.pfx、pks)
キー*	使用可能な RSA キーの長さ: 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	必要な RSA キーの長さ: 2048 ビット(非推奨)以上  または 必要な ECDSA キーカーブ: NIST P-256、P-384、または P-521

要件	CSR の作成 (Central Management で操作)	CSR のスキップ (Central Management で操作)
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 Manager 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します。チェーンファイルには、ルート証明書と中間証明書が含まれています。

チェーンファイルが次の要件を満たしていることを確認してください。

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

次に例を示します。

```

— BEGIN CERTIFICATE —
中間証明書 #3
— END CERTIFICATE —
— BEGIN CERTIFICATE —
中間証明書 #2
— END CERTIFICATE —
— BEGIN CERTIFICATE —
中間証明書 #1
— END CERTIFICATE —

```

— BEGIN CERTIFICATE —

**ルート CA 証明書**

— END CERTIFICATE —

**⚠** ファイルにアイデンティティ証明書を含めないでください。

## 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。

- **カスタム証明書:** 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場合は、必要な証明書を必要な信頼ストアにアップロードする必要があります。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。
- **ファイルに複数の証明書が含まれている場合は、**各証明書を信頼ストアに個別にアップロードします。チェーン全体を1つのファイルとしてアップロードしないでください。
- **フレンドリ名:** 証明書を信頼ストアに追加する場合は、各フレンドリ名が一意であることを確認します。フレンドリ名を重複させないでください。

## ワイルドカード証明書(クライアントアイデンティティのみ)

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

## 追加の証明書の設定

このガイドでは、アプライアンスアイデンティティとクライアントアイデンティティの設定について説明します。証明書、およびサーバー ID 検証の要件を必要とする Secure Network Analytics が追加の設定が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 (Help)] の手順に従います。[**?** (ヘルプ) アイコンをクリックします。[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。
- **シスコ ISE または Cisco ISE-PIC:** 次の手順を実行します: [ISE および ISE-PIC コンフィギュレーションガイド](#)。
- **LDAP:** [ヘルプ (Help)] の手順に従います。**?** (ヘルプ) アイコンをクリックします。[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 (Help)] の手順に従います。**?** (ヘルプ) アイコンをクリックします。[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:** 次の手順を実行します: [システムコンフィギュレーションガイド](#)。
- **応答管理に対する SMTP の設定:** ヘルプの手順に従います。**?** (ヘルプ) アイコンをクリックします。[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、次を参照してください: [コンフィギュレーションガイド](#)。



## [集中管理 (Central Management)] を開く

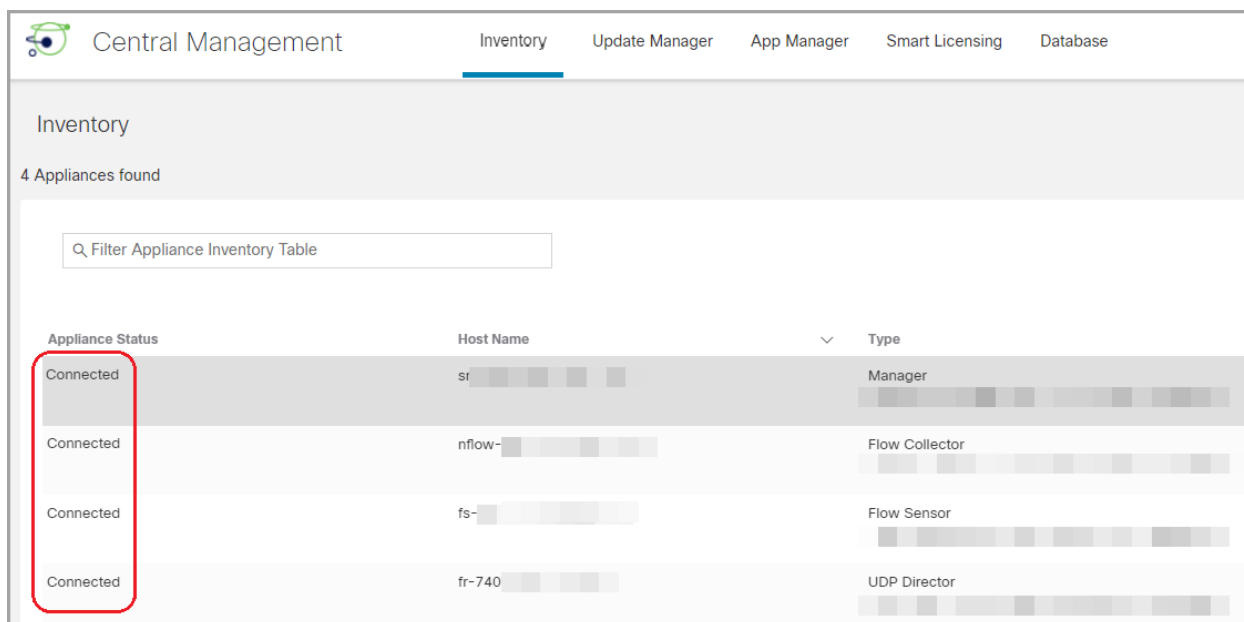
このガイドでは、主に Central Management を使用します。

1. Manager 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。

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

一度に1つのアプライアンスを設定します。Central Management にアプライアンスを追加するか設定を変更すると、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。



The screenshot shows the Central Management web interface. The top navigation bar includes 'Central Management', 'Inventory', 'Update Manager', 'App Manager', 'Smart Licensing', and 'Database'. The 'Inventory' page displays '4 Appliances found' and a search filter 'Filter Appliance Inventory Table'. Below is a table with columns 'Appliance Status', 'Host Name', and 'Type'. The 'Appliance Status' column for all four rows is highlighted with a red box, showing 'Connected'.

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

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

タスク	注意
<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>	シスコのバンドル情報を確認します。
<a href="#">証明書期限切れの通知を受け取る</a>	期限切れ間近の証明書に関する電子メール通知を設定します。
<a href="#">期限切れになっていない、または期限切れの証明書の置換</a>	<p>既存の証明書の有効期限が切れていない(およびアプライアンスのホスト情報が保持されている)場合に、新しいシスコ自己署名アプライアンスアイデンティティ証明書を生成するには、「<a href="#">期限切れになっていないシスコのデフォルト証明書の置換(証明書の更新)</a>」を参照してください。</p> <p>期限切れになっていない証明書または期限切れの証明書を置き換えるための追加オプションを確認するには、「<a href="#">期限切れになっていない、または期限切れの証明書の置換(概要)</a>」を参照してください。</p>
<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す。手順に従って、アプライアンスアイデンティティ証明書を認証局からのカスタム証明書に置き換えます。
<a href="#">ホスト名の変更</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アプライアンスホスト名を変更します。</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="#">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>	

## TLS バージョンの変更

アプライアンスの TLS バージョンサポートを選択するには、次の手順を使用します。システム内でさまざまなモードを選択できます。次がサポートされています。

- TLS 1.2 および 1.3 (デフォルト)
- TLS 1.3 のみ (Data Store ではサポートされていません)

アプライアンスの TLS バージョンを変更するには、次の手順を実行します。

1. アプライアンスコンソール (SystemConfig) に sysadmin としてログインします。
2. [セキュリティ (Security)] を選択します。
3. [TLSバージョン (TLS Version)] を選択します。
4. TLS バージョンを選択するには、バージョンを選択してクリックします (またはキーボードのスペースキーを押します)。[\*] は選択したバージョンを示します。

 Data Store が展開されている場合は、[TLS v1.3のみ (TLS v1.3 only)] を使用しないでください。

5. [OK] をクリックします。アプライアンスが再起動します。
6. [Central Management](#) を開きます。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。

## 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。フレンドリ名、発行された情報、期限日などの詳細を確認できます。

1. [Central Management を開きます](#)。
2. アプライアンスの … (省略符号)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。
6. **期限日**: [有効期限(Valid To)] 列を確認します。

## 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 アドレスまたはホスト名の後のパスを `/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。

## 証明書期限切れの通知を受け取る

アプライアンス アイデンティティ証明書が期限切れ間近になると、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、**電子メール通知**を受信することもできます。

### 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。

### 以前に有効に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。



Manager 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 アイデンティティ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。「[電子メール通知の無効化](#)」を参照してください。

### 最近有効に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。

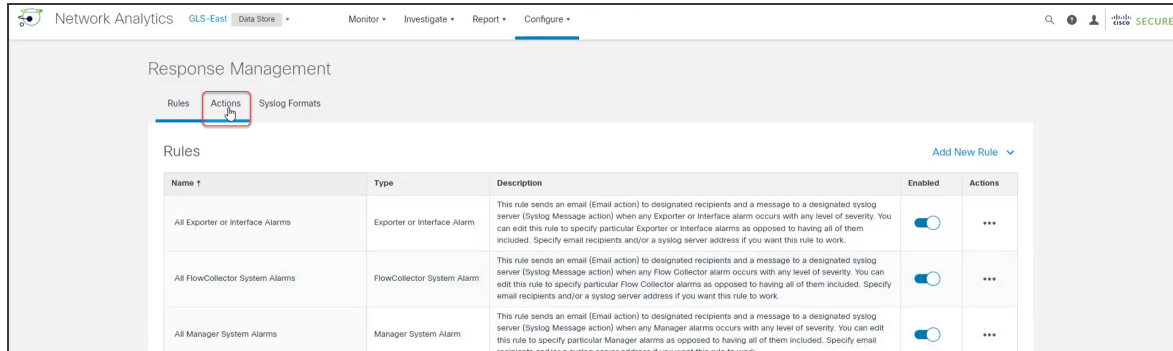
## カスタム電子メール通知の作成

「1. アクションの作成」を開始して、新しいアクションを作成します。それから「2. ルールの作成」に進み、作成したアクションにルールを割り当てます。

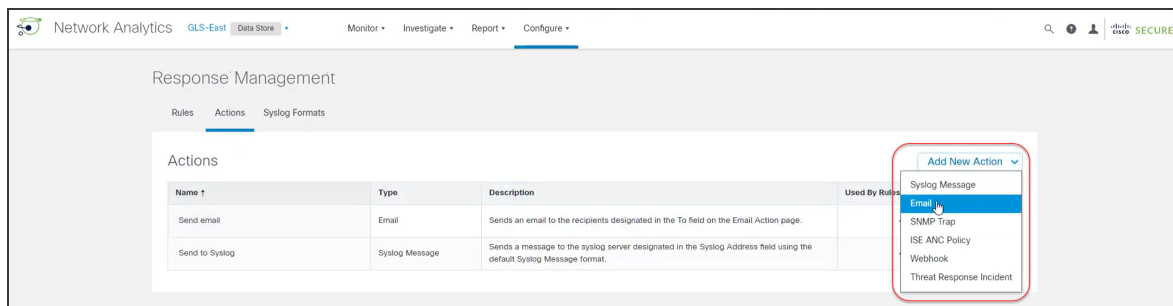
### 1. アクションの作成

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。

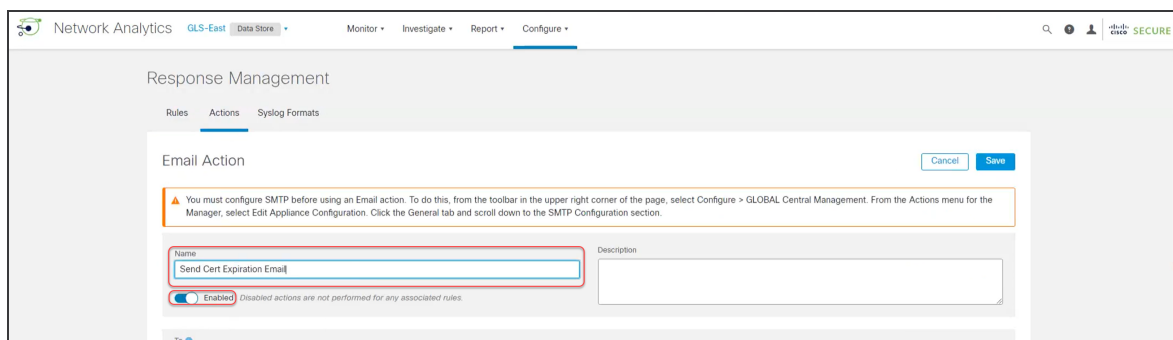
1. メインメニューで、[設定 (Configuration)] > [応答の管理 (Response Management)] を選択します。
2. [アクション (Actions)] タブをクリックします。



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。

- [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 the Subject and Body fields, which are also empty. At the bottom left of the form, there 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 a list of email addresses. The first address is 'ame@Company.com'. The second address, 'Name@Company.com', is highlighted with a red rectangular border and has a small plus sign (+) to its right, indicating it is being added to the list.

- 追加後、緑色で強調表示されます。

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

- [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 variables listed are: alarm\_category\_name, alarm\_id, alarm\_note, alarm\_severity\_id, alarm\_severity\_name, and alarm\_status. The variable 'alarm\_severity\_name' is highlighted with a red rectangular border. Each variable has a brief description below it.

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。

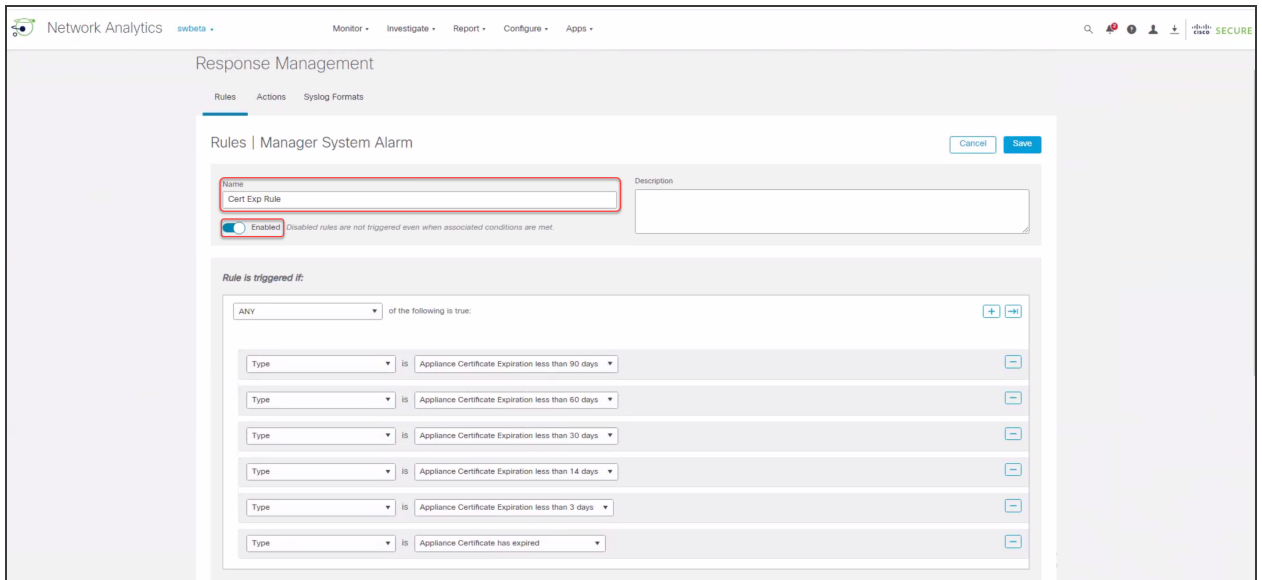
## 2. ルールの作成

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. [ルール (Rule)] 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。

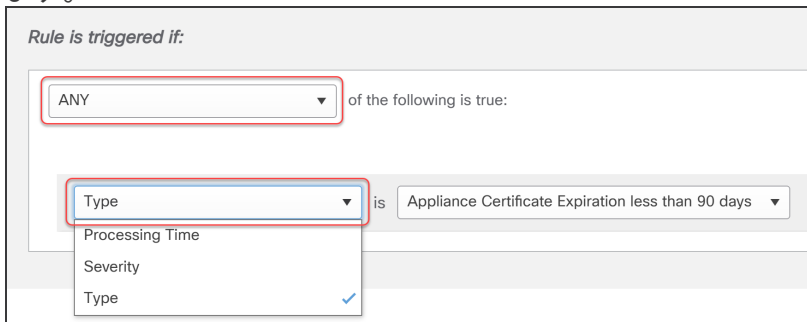
Associated Actions				
Execute the following actions when the alarm becomes <i>active</i> :				
Name ↑	Type	Description	Used By Rules	Assigned
Send Cert Expiration Email	Email		0	<input checked="" type="checkbox"/>
Send email	Email	Sends an email to the recipients designated in the To field on the Email 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 <i>inactive</i> :				
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。

- [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。



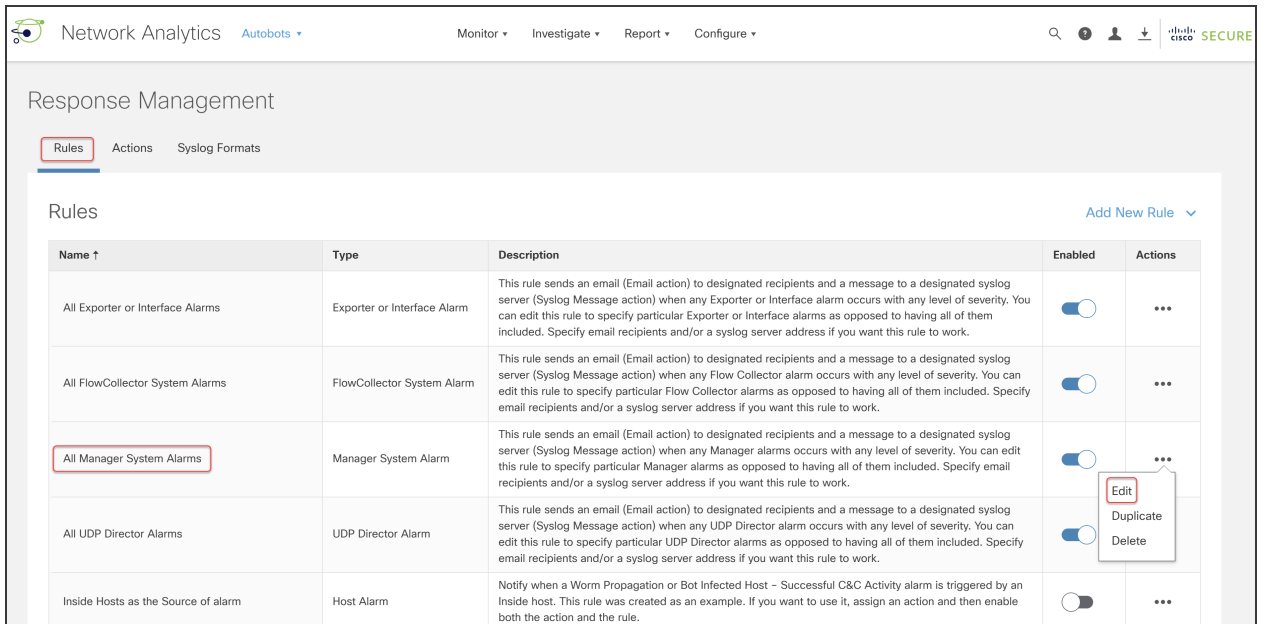
- [タイプ (Type)] を選択し、リストをスクロールして、受信する各メール通知を選択します。
- [+] (プラス) アイコンをクリックしてタイプを追加します。タイプを削除するには、[-] (マイナス) アイコンをクリックします。
- [保存 (Save)] をクリックします。

## 電子メール通知の無効化

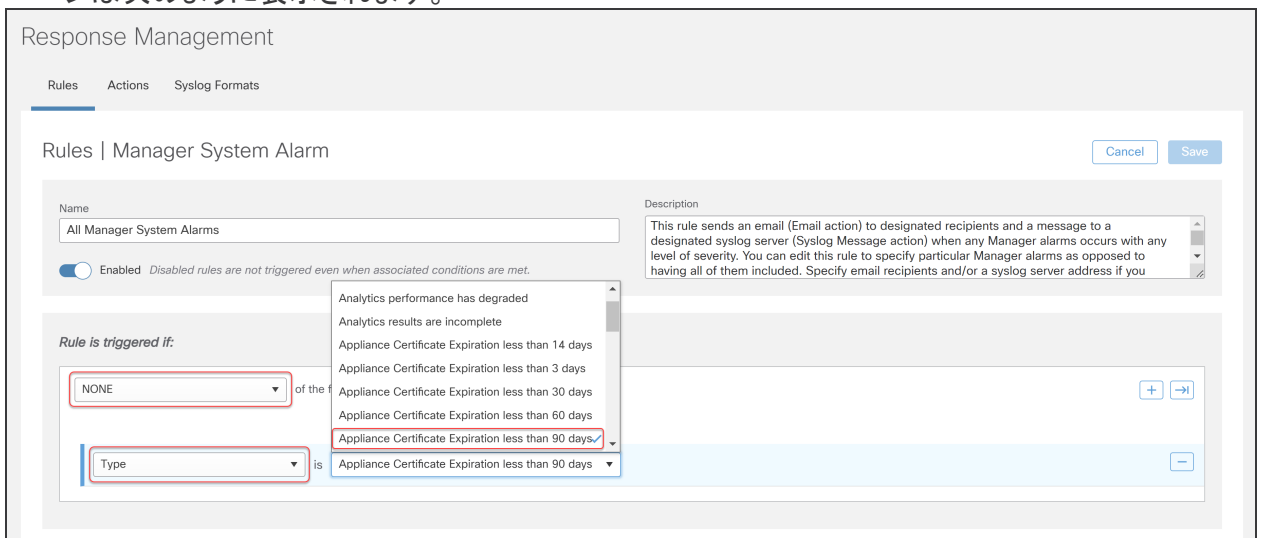
次の手順を使用して、1 つ以上の電子メール通知を無効にします。

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





ページは次のように表示されます。



- [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。
- [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。
- [+](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。
- [保存 (Save)] をクリックします。

## 電子メール通知の有効化

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。

## 期限切れになっていない、または期限切れの証明書の置換(概要)

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。アプライアンス アイデンティティ証明書の置換方法を選択します。

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証明書の置換(証明書の更新)</a>」を参照してください。</p> <p>証明書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>証明書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>現在の証明書を認証局からのカスタム証明書に置き換え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>

## 期限切れになっていないシスコのデフォルト証明書の置換(証明書の更新)

各 Secure Network Analytics アプライアンスは固有のシスコ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。既存のアプライアンス アイデンティティ証明書が期限切れになっていない場合、次の手順を実行して、新しいシスコ自己署名アプライアンス アイデンティティ証明書を生成します。

- **ホスト情報:** アプライアンスのホスト情報 (IPアドレス、ホスト名、ドメイン名) は保持されます。有効期限に加えてホスト情報を変更する必要がある場合は、(このセクションの手順ではなく)「[ネットワーク インターフェイスの変更](#)」または「[ホスト名またはネットワークドメイン名の変更](#)」の手順を実行します。
- **カスタム証明書:** アプライアンス アイデンティティ証明書は、この証明書更新手順でシスコの自己署名アプライアンス アイデンティティ証明書に自動的に置き換えられます。既存の証明書をカスタム アプライアンス アイデンティティ証明書に置き換えるには、「[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](#)」を参照し、以下を確認します。

- **ユーザー:** Manager アプライアンスコンソール ([システム設定 (System Configuration)]) の sysadmin アクセス権と、Manager Web ログイン用の管理者アクセス権が必要です。
- **集中管理:** このプロセスの進行中は、[集中管理 (Central Management)] で設定を変更したり、アプライアンスを追加/削除したりしないでください。
- **データ収集:** アプライアンスとデータベースを再起動し、データ収集を一時的に停止します。
- **フェールオーバー:** [証明書の更新 (Certificate Refresh)] メニューは、セカンダリ Manager では使用できません。Manager がフェールオーバー ペアとして設定されている場合は、プライマリ Manager にログインして、セカンダリ Manager 証明書を更新します。

### すべてのアプライアンスまたは選択したアプライアンスでの証明書の更新

Manager およびインベントリ内の他の管理対象アプライアンスの新しいシスコ自己署名アプライアンス アイデンティティ証明書を生成するには、次の手順に従います。リスト内のすべてのアプライアンス (デフォルト) または選択した個々のアプライアンスの証明書を生成できます。

証明書は順番に生成されるため、多数のアプライアンスを選択すると、このプロセスに時間がかかることがあります。

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。



既存の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には、「[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. 証明書の生成
3. [集中管理(Central Management)] の確認
4. 信頼ストアの確認



設定の変更が保留中、または設定チャネルがダウンしている場合は、アプライアンスを再起動しないでください。

## 1. アプライアンスのステータスの確認

新しい証明書を生成する前に、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。

1. プライマリ Manager 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[コンフィギュレーションチャネルのダウン(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。



Manager が[接続済み(Connected)]と表示されていない場合、アプライアンスの証明書を生成できません。あるアプライアンスのステータスが[接続済み(Connected)]と表示されない場合、そのアプライアンスの新しい証明書を生成できません。

Inventory

3 Appliances found

Q Filter Appliance Inventory Table

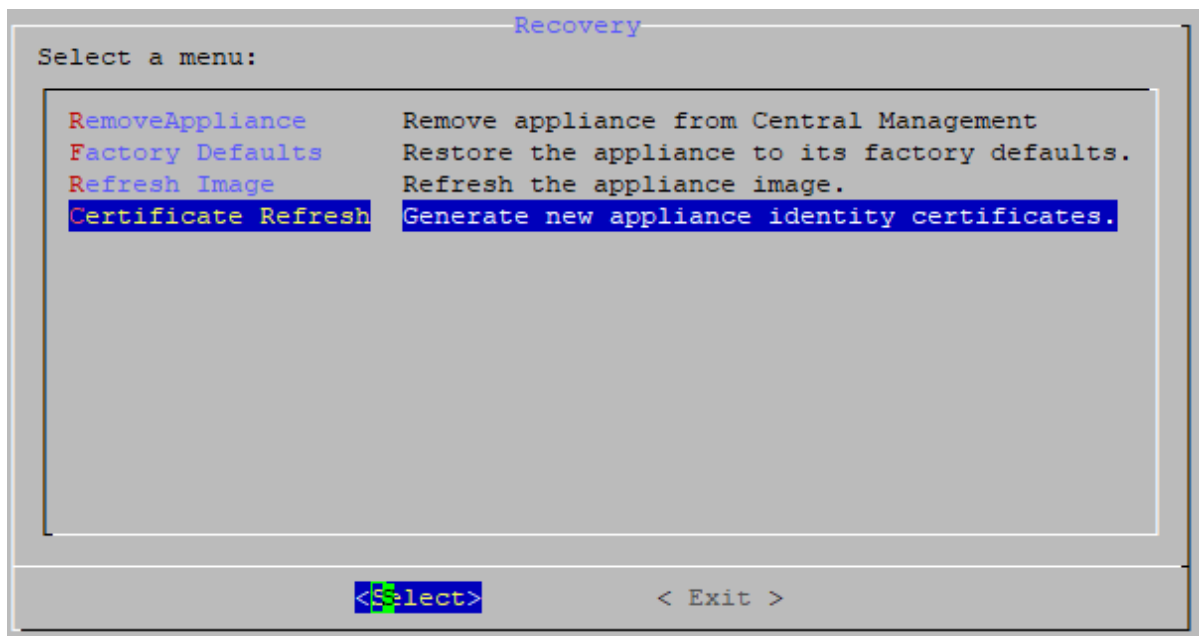
APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Config Changes Pending	fs-	Flow Sensor FSVE-KVM-		
Connected	nflow-	Flow Collector FCNFVE-KVM-		
Connected		Manager -VE-KVM-		

## 2. 証明書の生成

新しいシスコ自己署名アプライアンスアイデンティティ証明書を生成するには、次の手順を使用します。

**!** このプロセスの進行中は、[集中管理(Central Management)]で設定を変更したり、アプライアンスを追加/削除したりしないでください。アプライアンスとデータベースを再起動し、データの収集を一時的に停止します。

1. プライマリ Manager 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. [システム設定(System Configuration)] が開きます。
3. メインメニューから [リカバリ(Recovery)] を選択します。
4. [証明書の更新(Certificate Refresh)] を選択します。画面に表示される指示に従って操作します。



5. 1 ~ 5 年の有効期間を入力します。[OK] をクリックします。

Enter a certificate validity period between 1 and 5 years.

5

< OK > <Cancel>

6. アプライアンスのリストと証明書の有効期限の日付を確認します。リスト内のすべてのアプライアンスまたは選択した個々のアプライアンスの証明書を生成できます。
  - [\*] は、アプライアンスが選択されていることを示します。デフォルトでは、すべてのアプライアンスが選択されています。
  - アプライアンスの選択を解除するには、アプライアンスを選択し、クリックして(またはキーボードのスペースキーを押して)[\*]を削除します。
  - [OK] をクリックして、選択したアプライアンスの証明書を生成します。

You can generate new identity certificates for all appliances or individual appliances. We've selected all appliances by default. To deselect an appliance, select it and click it (or press the space key on your keyboard) to remove the \*. Click OK to confirm.

[*]	sdbn-7	2028-09-17
[*]	nflow-7	2028-09-17
[*]	smc-	2028-09-17

< OK > <Cancel>



7. 画面に表示される指示に従って操作します。
8. 証明書の更新の進行状況を確認するには、統計(失敗、スキップ、完了、および選択済み)を確認します。

**システム設定ログ:** 詳細については、次のいずれかの場所にある system\_config.log を確認してください。

- /lancopel/var/logs/system\_config.log
- [アプライアンス管理 (Appliance Admin)] にログインします。[サポート (Support)] > [ファイルの参照 (Browse Files)] > [ログ (logs)] > [system\_config.log] の順に選択します。

```

We are generating new appliance identity certificates:

sdbn-7 [REDACTED] : COMPLETED
nflow [REDACTED] : RUNNING
smc- [REDACTED] : WAITING

Failed: 0 | Skipped: 0 | Completed: 1 | Selected: 3
For details, review the system_config.log.

After this process is completed, review your Central Management
inventory, and confirm all appliances are shown as Connected.

Also, check each appliance trust store, confirm the new appliance
identity certificates are shown, and delete the old certificates.
    
```

9. すべてのアプライアンスに完了と表示され、成功メッセージが表示されるまで、[システム設定 (System Configuration)] を開いたままにします。
  - SSH が終了し、選択したアプライアンスが再起動します。
  - 証明書の更新プロセスが失敗した場合は、エラーメッセージを確認し、[\[システム設定ログ \(System Config Log\)\]](#) で詳細を確認してください。

You've successfully completed the certificate refresh process for all selected appliances. We are waiting for this appliance to restart.

After this process is completed, review your Central Management inventory, and confirm all appliances are shown as Connected.

Also, check each appliance trust store, confirm the new appliance identity certificates are shown, and delete the old certificates.

### 3. [集中管理(Central Management)] の確認

1. プライマリ Manager 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 [コンフィギュレーション 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。

The screenshot shows the 'Inventory' page in the Central Management interface. It displays a table with 3 appliances found. The 'Appliance Status' column is highlighted with a red box, showing 'Connected' for all three entries.

Appliance Status	Host Name	Type	IP Address	Actions
Connected	nflow-0-1	Flow Collector FCNFVE-Data Store	10.0.0.1	...
Connected	sdbn-7-1	Data Node DNODEVE-K1	10.0.0.2	...
Connected	smc-0-1	Manager SMCVE-	10.0.0.0	...

## 4. 信頼ストアの確認

1. [集中管理(Central Management)]の[インベントリ(Inventory)]ページで、Managerの[⋮(省略符号)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. スクロールして[信頼ストア(Trust Store)]リスト全体を確認します。
  - 新しい証明書が表示されていることを確認します。
  - 古い証明書を削除します。



新しい証明書は削除しないでください。

Friendly Name	Issued To	Issued By	Valid From	Valid To	Serial Number	Key Length	Actions
cn- r1- n Cwl	smc- id 1	smc-2	2023-09-15 16:12:21	2028-09-15 16:12:21	C- C	2 8192 bits	Delete
nflow-742	nflow- 1. em	nflow-74	2023-09-15 16:13:23	2028-09-15 16:13:23	e b	5 8192 bits	Delete
sdbn-7-	sdbn-74 1. la	sdbn-	2023-09-15 16:10:56	2028-09-15 16:10:56		33 8192 bits	Delete

6 Certificates

5. [設定の適用(Apply settings)]をクリックします。
6. [集中管理(Central Management)]の[インベントリ(Inventory)]に戻ります。
7. リスト内の次のアプライアンスの[⋮(省略符号)アイコン]をクリックします。手順2～5を繰り返して、[集中管理(Central Management)]の[インベントリ(Inventory)]に含まれる各アプライアンスの信頼ストアを確認します。

# 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。既存のアプライアンス アイデンティティ証明書が**期限切れ**になった場合、次の手順を実行して、有効期限を変更し、新しいシスコ自己署名アプライアンス アイデンティティ証明書を生成します。

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



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

## 要件

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

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

## 1. アプライアンスのステータスの確認

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

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	1.5	
Config Channel Down		Manager DVE-KVM	1.4	

## 2. アプライアンスの手順の選択

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

### Manager と管理対象アプライアンス

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

**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、この期間は手順を進める過程で変更できます。

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

アプライアンス アイデンティティ証明書は、この手順の一環として自動的に置き換えられます。

- ⚠ カスタム証明書を使用するアプライアンスの場合、アプライアンスでカスタム アプライアンス アイデンティティ証明書を使用するこの手順はサポートされていません。この手順を実行すると、カスタム証明書はシスコ自己署名アプライアンス アイデンティティ証明書に置き換えられます。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には、「[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. **Data Store データベースを停止する**
2. **Central Management からのアプライアンスの削除**
3. **アプライアンス アイデンティティ証明書の再生成**
4. **[集中管理(Central Management)] への Manager の登録**
5. **信頼ストアからの期限切れ証明書の削除**
6. **Central Management へのアプライアンスの追加**
7. **Data Store データベースの開始**
8. **信頼ストアからの期限切れ証明書の削除**
9. **Manager フェールオーバーペアの設定**

### 1. Data Store データベースを停止する

データベースを停止せずに、3 つ以上の Data Node がある状況で操作する場合は、[シスコ サポート](#) に連絡してサポートを求めてください。

**i** 展開に Data Node がない場合は、「**2. Central Management からのアプライアンスの削除**」に進みます。

1. 次の URL にアクセスしてください: Central Management > データストア > [データベースコントロール(Database Control)]。
2. まず、[データベースステータス(Database Status)] 列に移動し、データベースが次のように表示されていることを確認します:[アップ(Up)]。
3. データベースの [アクション(Actions)] 列の [... (省略符号)アイコン] をクリックします。
4. [停止(Stop)] を選択します。
5. データベースのステータスが次のように表示されていることを確認します:[ダウン(Down)]。

### 2. Central Management からのアプライアンスの削除

**i** Manager の証明書のみを変更する場合でも、すべてのアプライアンスを [集中管理(Central Management)] から削除する必要があります。Manager 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、「**Manager 以外の個別のアプライアンス**」を参照してください。

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 Manager を除く)を [集中管理(Central Management)] から削除します。

- [インベントリ (Inventory)] タブで、アプライアンスの [⋮ (省略符号) アイコン] をクリックします。
- [このアプライアンスの削除 (Remove This Appliance)] を選択します。
- **コンフィギュレーションチャネルのダウン**: アプライアンスのステータスが [コンフィギュレーションチャネルのダウン (Config Channel Down)] と表示されている場合は、アプライアンスコンソールにログインします。メインメニューから、[リカバリ (Recovery)] > [アプライアンスの削除 (RemoveAppliance)] を選択します。

Inventory

1 Appliances found

Filter Appliance Inventory Table

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

**!** 最後に [集中管理 (Central Management)] から Manager を削除します。

4. [集中管理 (Central Management)] からプライマリ Manager を削除します。
  - [インベントリ (Inventory)] タブで、プライマリ Manager の [⋮ (省略符号) 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、Manager 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。

### 3. アプライアンス アイデンティティ証明書の再生成

Manager およびその他のアプライアンスでアプライアンス アイデンティティ証明書を再生成するには、次の手順を使用します。

**!** Manager ではない他のアプライアンスでアイデンティティ証明書を変更する必要がある場合は、最後にプライマリ Manager でこの手順を実行します。

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。画面に表示される指示に従って、[システム設定 (System Configuration)] を開きます。

**Manager:** Manager にログインし、すべての [システム設定 (System Configuration)] メニューをロードできなかったというエラーが表示された場合は、[OK] をクリックします。







**Manager のフェールオーバー:** 2 つの Manager がある場合、プライマリ Manager でこの手順を実行するだけで十分です。以下の手順で、セカンダリ Manager を登録します。「[6. Central Management へのアプライアンスの追加](#)」で、セカンダリ SMC を登録します。

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

1. Manager アプライアンスコンソールに sysadmin としてログインします。
2. [リカバリ (Recovery)] を選択します。
3. [アプライアンスの追加 (Add Appliance)] を選択します。
4. Manager の IP アドレス、ユーザー名およびパスワードを入力します。
5. 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。Manager アプライアンスのステータスが以下のように表示されていることを確認します: [接続済み (Connected)]。

The screenshot shows the 'Inventory' section of a management console. It displays '1 Appliances found' and a table with the following columns: APPLIANCE STATUS, HOST NAME, TYPE, IP ADDRESS, and ACTIONS. The 'APPLIANCE STATUS' column contains the value 'Connected', which is highlighted with a red box. The 'TYPE' column shows 'Manager' and 'VE-KVM-'. There is a search filter 'Filter Appliance Inventory Table' and a search icon.

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

## 5. 信頼ストアからの期限切れ証明書の削除

Manager が 2 つある場合は、プライマリ Manager でこの手順を実行するだけで十分です (セカンダリ Manager は工場出荷時のデフォルトにリセットされたため)。

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

1. [集中管理 (Central Management)] の [インベントリ (Inventory)] で、Manager の [⋮ (省略符号) 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。Manager と Manager 以外のその他のアプライアンスのすべての期限切れ証明書 (アイデンティティ、ルート、および中間証明書) を見つけます。
5. [削除 (Delete)] をクリックして古い証明書それぞれを削除します。
6. [設定の適用 (Apply settings)] をクリックします。画面に表示される指示に従って操作します。
7. [集中管理 (Central Management)] の [インベントリ (Inventory)] ページで、Manager 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。

## 6. Central Management へのアプライアンスの追加

アプライアンスコンソール (SystemConfig) を使用して、他のアプライアンスを [集中管理 (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。
- [集中管理 (Central Management)]: Manager IP アドレス、Manager パスワード、および Secure Network Analytics ドメインが必要です。
- **順序**: 「[アプライアンスの設定順序](#)」に従います。
- **アクセス**: Central Management にアクセスするには管理者権限が必要です。

### アプライアンスの設定順序

次の順序でアプライアンスを設定し、各アプライアンスの詳細を書き留めます。

	アプライアンス	詳細
1.	UDP Director (別名 FlowReplicators)	
2.	Flow Collector 5000 シリーズ データベース	エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [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.	Data Node	
7.	セカンダリ Manager (使用する場合)	セカンダリ Manager の設定を開始する前に、プライマリ Manager が [接続済み (Connected)] として表示されていることを確認します。  セカンダリ Manager は、自身を Central Manager として選択します。すべてのアプライアンスの設定後にフェールオーバーを設定します。「 <a href="#">9. Manager フェールオーバーペアの設定</a> 」を参照してください。

アプライアンスコンソール(SystemConfig)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。

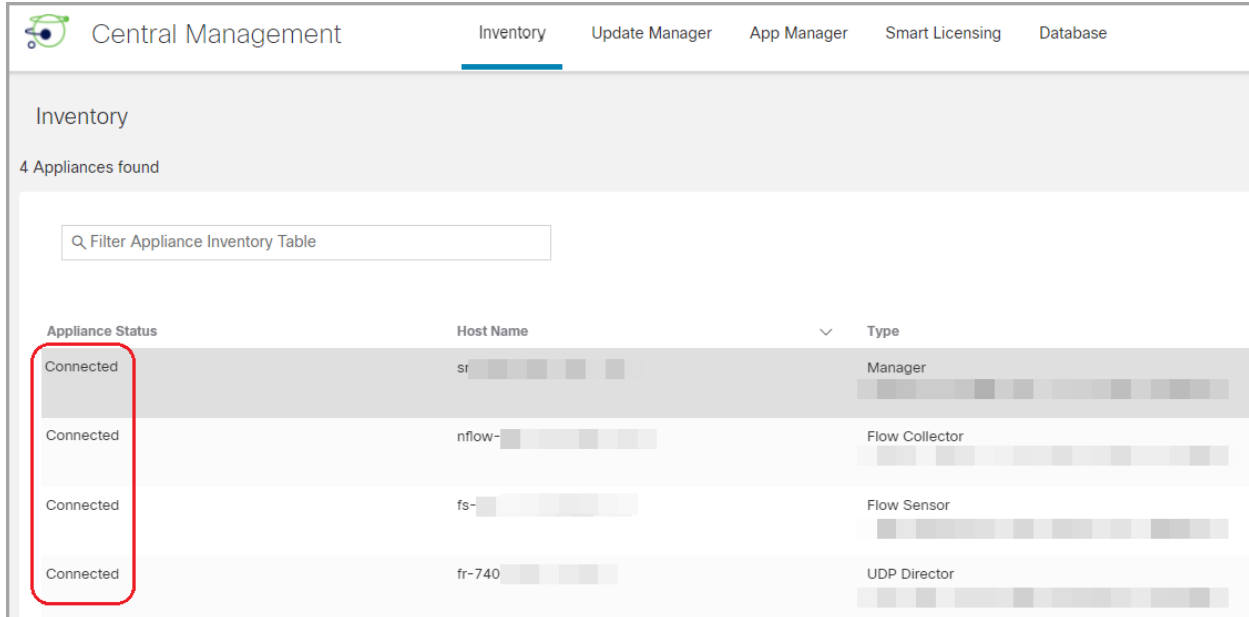
1. アプライアンスコンソールに sysadmin としてログインします。

**セカンダリ Manager のみ:** セカンダリ Manager がある場合は、sysadmin としてログインします。初回セットアップの指示に従います([システムコンフィギュレーションガイド](#)の手順を参照してください)。Manager は、自身を Central Manager として選択します。すべてのアプライアンスが [集中管理 (Central Management)] に接続された後に、フェールオーバーを設定します。

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

2. [リカバリ (Recovery)] を選択します。
3. [アプライアンスの追加 (Add Appliance)] を選択します。
4. Manager の IP アドレスと管理者パスワードを入力します。[OK] をクリックします。
5. 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以下のように表示されていることを確認します: [接続済み (Connected)]。

**!** 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 Manager 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 [集中管理 (Central Management)] に追加します ([設定の順序と詳細を使用](#))。



- 手順 1 ~ 5 を繰り返して各アプライアンスを [集中管理 (Central Management)] に追加します。

## 7. Data Store データベースの開始

**i** 展開に Data Node がない場合は、「[8. 信頼ストアからの期限切れ証明書の削除](#)」に進みます。

- [集中管理 (Central Management)] で以下を選択します: データストア > [データベースコントロール (Database Control)]。
- まず、[データベースステータス (Database Status)] 列に移動し、データベースが次のように表示されていることを確認します: [ダウン (Down)]。
- データベースの [アクション (Actions)] 列の [... (省略符号) アイコン] をクリックします。
- [開始 (Start)] を選択します。
- データベースのステータスが次のように表示されていることを確認します: [アップ (Up)]。

## 8. 信頼ストアからの期限切れ証明書の削除

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

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

- [集中管理 (Central Management)] の [インベントリ (Inventory)] で、アプライアンスの [... (省略符号) アイコン] をクリックします。
- [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。
- [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、Manager、およびその他のアプライアンスのすべての期限切れ証明書 (アイデンティティ、ルート、および中間証明書) を見つけます。
5. [削除 (Delete)] をクリックして古い証明書それぞれを削除します。
6. [設定の適用 (Apply settings)] をクリックします。画面に表示される指示に従って操作します。
7. [集中管理 (Central Management)] の [インベントリ (Inventory)] ページで、アプライアンスと Manager 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、UDP Director、および Data Node で手順 1 ~ 7 を繰り返します。

## 9. Manager フェールオーバーペアの設定

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

### Manager 以外の個別のアプライアンス

次の手順に従って、Manager 以外の個別のアプライアンス (Flow Collector、Flow Sensor、UDP Director、または Data Node) 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、この期間は手順を進める過程で変更できます。

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。この手順を実行すると、カスタム証明書はシスコ自己署名アプライアンス アイデンティティ証明書に置き換えられます。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には、「[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. [Data Store データベースを停止する](#)
2. [アプライアンスの削除と証明書の再生成](#)
3. [信頼ストアからの期限切れ証明書の削除](#)
4. [Central Management へのアプライアンスの追加](#)
5. [Data Store データベースの開始](#)



Manager 証明書の有効期限を変更する必要がある場合は、「[Manager と管理対象アプライアンス](#)」を参照してください。









## 4. Central Management へのアプライアンスの追加

アプライアンスを [集中管理 (Central Management)] に追加すると、IP アドレス、ホスト名などは保持されます。

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

- [集中管理 (Central Management)]: Manager IP アドレス、Manager パスワード、および Secure Network Analytics ドメインが必要です。
  - **順序**: 2 つ以上のアプライアンスを Central Management に追加する場合は、「[アプライアンスの設定順序](#)」に従います。
  - **アクセス**: Central Management にアクセスするには管理者権限が必要です。
1. アプライアンスコンソールに sysadmin としてログインします。
  2. [リカバリ (Recovery)] を選択します。
  3. [アプライアンスの追加 (Add Appliance)] を選択します。
  4. Manager の IP アドレスと管理者パスワードを入力します。[OK] をクリックします。
  5. 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。

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

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


## 5. Data Store データベースの開始

**i** 展開に Data Node がない場合は、このセクションをスキップできます。

1. [集中管理 (Central Management)] で以下を選択します: データストア > [データベースコントロール (Database Control)]。
2. まず、[データベースステータス (Database Status)] 列に移動し、データベースが次のように表示されていることを確認します: [ダウン (Down)]。
3. データベースの [アクション (Actions)] 列の [⋯ (省略符号) アイコン] をクリックします。
4. [開始 (Start)] を選択します。
5. データベースのステータスが次のように表示されていることを確認します: [アップ (Up)]。

# 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「[アプライアンスのアイデンティティ証明書](#)」を参照してください。

## 環境に応じた手順の選択

Central Management で証明書署名要求 (CSR) を生成するか、すでに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、「[\[集中管理 \(Central Management\)\] 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. [ルート CA 証明書を信頼ストアに追加する](#)
3. [Data Store データベースを停止する](#)
4. [アプライアンス アイデンティティ証明書の置換](#)
5. [デスクトップ クライアントで証明書を信頼する](#)

### 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 (Inventory)] ページで、アプライアンスの [… (省略符号) 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。

**i** CSRを生成する必要がない場合は、「[\[集中管理\(Central Management\)\]でのCSRの省略](#)」に進みます。

7. 認証局でサポートされる RSA キーの長さを選択します。
8. [CSRの生成(Generate a CSR)] セクションのフィールド(任意)に入力します。
9. [CSRの生成(Generate a 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. ルート CA 証明書を信頼ストアに追加する

1. [Central Management を開きます](#)。
2. [インベントリ(Inventory)] タブで、アプライアンスの [⋮ (省略符号)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-	121-	121-					
1.lanc	1.lanc	1.lanc			39		
m	m	m					

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



**!** 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。

7. [ファイルの選択 (Choose File)] をクリックします。新しいルート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。
9. 各アプライアンスの信頼ストアで手順 1 ~ 8 を繰り返します。

## 信頼ストアの要件

このテーブルを使用して、アプライアンスの信頼ストアにルート CA 証明書を追加します。

アプライアンス アイデンティティ証明書	詳細	信頼ストア
Manager/ Central Manager	Manager 信頼ストアと [集中管理 (Central Management)] 内の各アプライアンスの信頼ストアに Manager ルート証明書を追加します。	<ul style="list-style-type: none"> <li>• プライマリ Manager</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>• Data Node</li> <li>• セカンダリ Manager (フェールオーバーのみ)</li> </ul>
セカンダリ Manager (フェールオーバーのみ)	<p>Manager がフェールオーバー用に設定されている場合にセカンダリ Manager アイデンティティ証明書を置き換えるには、新しいセカンダリ Manager ルート証明書をセカンダリ Manager 信頼ストア、プライマリ Manager 信頼ストア、および [集中管理 (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>• Data Node</li> <li>• セカンダリ Manager (フェールオーバーのみ)</li> <li>• プライマリ Manager</li> </ul>

Flow Collector	<p>Flow Collector のルート証明書を、Flow Collector の信頼ストアと Manager の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 エンジンのルート証明書を Flow Collector データベースの信頼ストアに追加します。</li> <li>Flow Collector データベースのルート証明書を 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 Manager (フェールオーバーのみ)</li> <li>プライマリ Manager</li> </ul>
フローセンサー	<p>Flow Sensor のルート証明書を Flow Sensor の信頼ストアと Manager の信頼ストアに追加します。</p>	<ul style="list-style-type: none"> <li>フローセンサー</li> <li>セカンダリ Manager (フェールオーバーのみ)</li> <li>プライマリ Manager</li> </ul>
UDP Director	<p>UDP Director のルート証明書を UDP Director の信頼ストアと Manager の信頼ストアに追加します。</p>	<ul style="list-style-type: none"> <li>UDP Director</li> <li>セカンダリ Manager (フェールオーバーのみ)</li> <li>プライマリ Manager</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 のルート証明書をプライマリ UDP Director の信頼ストアに追加します。</li> <li>プライマリ UDP Director のルート証明書をセカンダリ UDP Director の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 Manager (フェールオーバーのみ)</li> <li>プライマリ Manager</li> </ul>
データノード	<p>Data Node のルート証明書を Data Node の信頼ストアと Manager の信頼ストアに追加します。</p>	<ul style="list-style-type: none"> <li>プライマリ Manager</li> <li>データノード</li> <li>セカンダリ Manager (フェールオーバーのみ)</li> </ul>

### 3. Data Store データベースを停止する

データベースを停止せずに、3 つ以上の Data Node がある状況で操作する場合は、[シスコ サポート](#) に連絡してサポートを求めてください。

**i** 展開に Data Node がない場合は、「[4. アプライアンス アイデンティティ証明書の置換](#)」に進みます。

1. 次の URL にアクセスしてください: Central Management > データストア > [データベースコントロール (Database Control)]。
2. まず、[データベースステータス (Database Status)] 列に移動し、データベースが次のように表示されていることを確認します: [アップ (Up)]。
3. データベースの [アクション (Actions)] 列の [⋮ (省略符号) アイコン] をクリックします。
4. [停止 (Stop)] を選択します。
5. データベースのステータスが次のように表示されていることを確認します: [ダウン (Down)]。

### 4. 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、アプライアンスの再起動を管理できる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 (Inventory)] ページで、アプライアンスの [⋮ (省略符号) 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、UDP Director、または Data Node 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)] を選択します。
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 (リーフ) 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てい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。

## 5. デスクトップ クライアントで証明書を信頼する

デスクトップクライアントを使用する場合は、次の手順を実行します。デスクトップクライアントは、Data Store のない展開でのみ使用できます。

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

1. Manager に管理者としてログインします (https://<IPAddress>)。
2.  (ダウンロード) 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。

## [集中管理 (Central Management)] での CSR の省略

「[アプライアンスのアイデンティティ証明書](#)」の要件を満たす証明書がすでにある場合は、次の手順を実行して、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. [信頼ストアへの必要な証明書の追加](#)
2. [Data Store データベースを停止する](#)
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で証明書を信頼する](#)

### 1. 信頼ストアへの必要な証明書の追加

開始する前に、「[信頼ストアの要件](#)」で必要な証明書についての情報を確認してください。

1. [Central Management を開きます](#)。
2. [インベントリ (Inventory)] タブで、アプライアンスの [ (省略符号) 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
	nmxm fs-7 nzq1o 1.la mi0yz m wnimzd	fs-7 1.la m	2020-11-20 17:51:53	2025-11-20 17:51:53		8192 bits	Delete
	9- 121- 1.lanc m	121- 1.lanc m	2020-11-20 17:42:20	2025-11-20 17:42:20	39	8192 bits	Delete

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。

**!** 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。
- [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。
- 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

このテーブルを使用して、アプライアンスの信頼ストアに必要な証明書を追加します。必要な証明書は、以下によって決まります。

- 自己署名:** 自己署名証明書がある場合は、信頼ストアに追加します。
- チェーン/ルート:** チェーン証明書がある場合は、ルート証明書を信頼ストアに追加するだけで済みます。

アプライアンス アイデンティティ証明書	詳細	信頼ストア
Manager/ Central Manager	Manager 信頼ストアと [集中管理 (Central Management)] 内の各アプライアンスの信頼ストアに必要な証明書を追加します。	<ul style="list-style-type: none"> <li>プライマリ Manager</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>Data Node</li> <li>セカンダリ Manager (フェールオーバーのみ)</li> </ul>

<p>セカンダリ Manager (フェールオーバーのみ)</p>	<p>Manager がフェールオーバー用に設定されている場合にセカンダリ Manager アイデンティティ証明書を置き換えるには、必要な証明書をセカンダリ Manager 信頼ストア、プライマリ Manager 信頼ストア、および [集中管理 (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>• Data Node</li> <li>• セカンダリ Manager (フェールオーバーのみ)</li> <li>• プライマリ Manager</li> </ul>
<p>Flow Collector</p>	<p>必要な証明書を、Flow Collector の信頼ストアと Manager の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>• 必要なエンジン証明書を Flow Collector データベースの信頼ストアに追加します。</li> <li>• 必要な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 Manager (フェールオーバーのみ)</li> <li>• プライマリ Manager</li> </ul>
<p>フローセンサー</p>	<p>必要な証明書を、Flow Sensor の信頼ストアと Manager の信頼ストアに追加します。</p>	<ul style="list-style-type: none"> <li>• フローセンサー</li> <li>• セカンダリ Manager (フェールオーバーのみ)</li> <li>• プライマリ Manager</li> </ul>
<p>UDP Director</p>	<p>必要な証明書を、UDP Director の信頼ストアと Manager の信頼ストアに追加します。</p>	<ul style="list-style-type: none"> <li>• UDP Director</li> <li>• セカンダリ Manager (フェールオーバーのみ)</li> <li>• プライマリ Manager</li> </ul>

高可用性ペアの UDP Director	必要な証明書を、プライマリ UDP Director の信頼ストアとセカンダリ UDP Director の信頼ストアと Manager の信頼ストアに追加します。	<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 Manager (フェールオーバーのみ)</li> <li>プライマリ Manager</li> </ul>
データノード	必要な証明書を Data Node の信頼ストアと Manager の信頼ストアに追加します。	<ul style="list-style-type: none"> <li>プライマリ Manager</li> <li>データノード</li> <li>セカンダリ Manager (フェールオーバーのみ)</li> </ul>

## 2. Data Store データベースを停止する

データベースを停止せずに、3 つ以上の Data Node がある状況で操作する場合は、[シスコ サポート](#) に連絡してサポートを求めてください。

**i** 展開に Data Node がない場合は、「[3. アプライアンス アイデンティティ証明書の置換](#)」に進みます。

- 次の URL にアクセスしてください: Central Management > データストア > [データベースコントロール (Database Control)]。
- まず、[データベースステータス (Database Status)] 列に移動し、データベースが次のように表示されていることを確認します: [アップ (Up)]。
- データベースの [アクション (Actions)] 列の [... (省略符号) アイコン] をクリックします。
- [停止 (Stop)] を選択します。
- データベースのステータスが次のように表示されていることを確認します: [ダウン (Down)]。

## 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。

- [Central Management を開きます](#)。
- [インベントリ (Inventory)] タブで、アプライアンスの [... (省略符号) 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、UDP Director、または Data Node から開始します。最後に Manager を更新します。
- [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。
- [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。
- [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)]を選択します。[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。

また、証明書ファイル形式に応じて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(リーフ)を含めないでください。


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てい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。

#### 4. デスクトップ クライアントで証明書を信頼する

デスクトップクライアントを使用する場合は、次の手順を実行します。デスクトップクライアントは、Data Store のない展開でのみ使用できます。

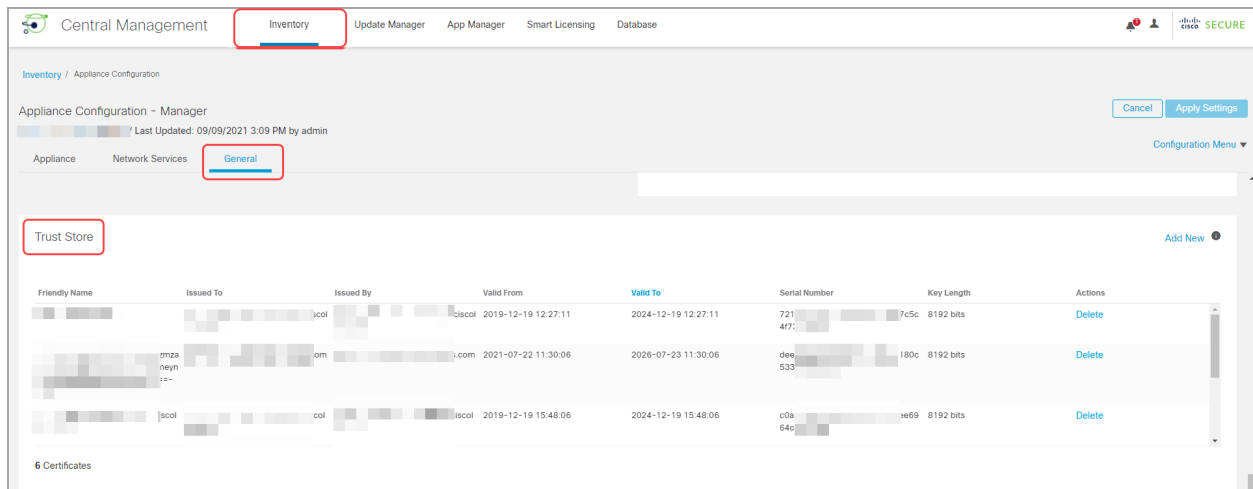
デスクトップ クライアントは、ローカルコンピュータにインストールされたデフォルトの信頼ストアに保存されている証明書だけを信頼します。

1. Manager に管理者としてログインします(https://<IPAddress>)。
2.  (ダウンロード)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 … (省略符号) 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、新しい証明書を追加して「[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。

Trust Store							Add New
FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
[Redacted]	nmxm fs-7 nzq1o 1.la mi0yz m wnmzd	fs-7 1.la m	2020-11-20 17:51:53	2025-11-20 17:51:53	[Redacted]	8192 bits	Delete
[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

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

証明書が保存されている場所を確認するには、「信頼ストア」列を参照してください。

アプライアンス アイデンティティ証明書	信頼ストア
マネージャ Central Manager	<ul style="list-style-type: none"> <li>プライマリ Manager</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>Data Node</li> <li>セカンダリ Manager (フェールオーバーのみ)</li> </ul>
セカンダリ Manager (フェールオーバーのみ)	<ul style="list-style-type: none"> <li>Flow Collector</li> <li>Flow Collector Databases (5000 シリーズのみ)</li> <li>Flow Sensor</li> <li>UDP Director</li> <li>Data Node</li> <li>セカンダリ Manager (フェールオーバーのみ)</li> <li>プライマリ Manager</li> </ul> <p><b>Manager フェールオーバー:</b> Manager フェールオーバーの関係を削除する場合は、すべてのアプライアンスの信頼ストアからセカンダリ Manager 証明書を削除します。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 Manager (フェールオーバーのみ)</li> <li>• プライマリ Manager</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 Manager (フェールオーバーのみ)</li> <li>• プライマリ Manager</li> </ul>
UDP Director	<ul style="list-style-type: none"> <li>• UDP Director</li> <li>• セカンダリ Manager (フェールオーバーのみ)</li> <li>• プライマリ Manager</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 Manager (フェールオーバーのみ)</li> <li>• プライマリ Manager</li> </ul>
データノード	<ul style="list-style-type: none"> <li>• プライマリ Manager</li> <li>• データノード</li> <li>• セカンダリ Manager (フェールオーバーのみ)</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、初回セットアップ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。
- **カスタム証明書を使用している場合は**、誤って証明書を上書きした場合に備えて、ネットワーク設定 (ホスト名、ネットワークドメイン名、または eth0 IP アドレス) を変更する前に、証明書を保存します。シスコ自己署名アプライアンス 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、次の手順に従います: [SSL/TLS アプライアンス アイデンティティ証明書の置換](#)。

## 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 **… (省略符号)** 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 [集中管理 (Central Management)] から一時的に削除します。

また、画面に表示される指示に従って、証明書の再生成が必要かどうか、または証明書を保持することを選択できるかどうかを確認してください。

**!** カスタム証明書を使用している場合は、誤って証明書を上書きした場合に備えて、ネットワーク設定 (ホスト名、ネットワークドメイン名、または IP アドレス) を変更する前に、証明書を保存します。シスコ自己署名アプライアンス 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、次の手順に従います: [SSL/TLS アプライアンス アイデンティティ証明書の置換](#)。

## 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。
- **Flow Collector 5000 シリーズ データベース**: 複数のデータベースとエンジンのペアがある場合は、[集中管理 (Central Management)] で識別できるように、データベースとエンジンの各ペアに名前を付けます (例: database1 and engine1、database2 and engine2)。
- **Manager のフェールオーバー**: Manager がフェールオーバーペアとして設定されている場合は、Manager の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

- Manager: **Manager**
- Flow Collector、Flow Sensor、UDP Director、または Data Node: **Manager 以外のアプライアンス**

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

## Manager

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

**Manager のフェールオーバー:** Manager がフェールオーバーペアとして設定されている場合は、Manager の設定を変更する前に、フェールオーバーの関係を削除します。[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。

**!** カスタム証明書を使用している場合は、誤って証明書を上書きした場合に備えて、ネットワーク設定 (ホスト名、ネットワークドメイン名、または eth0 IP アドレス) を変更する前に、証明書を保存します。シスコ自己署名アプライアンス 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、次の手順に従います: [SSL/TLS アプライアンス アイデンティティ証明書の置換](#)。

## 概要

全体的な手順は次のとおりです。

1. [Data Store データベースを停止する](#)
2. [Central Management からのアプライアンスの削除](#)
3. [Manager のホスト名またはネットワークドメイン名の変更](#)
4. [\[集中管理 \(Central Management\)\] への Manager の登録](#)
5. [Central Management へのアプライアンスの追加](#)
6. [Data Store データベースの開始](#)
7. [信頼ストアからの古い Manager 証明書の削除](#)
8. [Manager フェールオーバーペアの設定](#)

### 1. Data Store データベースを停止する

データベースを停止せずに、3 つ以上の Data Node がある状況で操作する場合は、[シスコ サポート](#) に連絡してサポートを求めてください。

**i** 展開に Data Node がない場合は、「[2. Central Management からのアプライアンスの削除](#)」に進みます。

1. 次の URL にアクセスしてください: Central Management > データストア > [データベースコントロール (Database Control)]。
2. まず、[データベースステータス (Database Status)] 列に移動し、データベースが次のように表示されていることを確認します: [アップ (Up)]。
3. データベースの [アクション (Actions)] 列の [⋮ (省略符号) アイコン] をクリックします。
4. [停止 (Stop)] を選択します。
5. データベースのステータスが次のように表示されていることを確認します: [ダウン (Down)]。

## 2. 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 Manager を除く) を [集中管理 (Central Management)] から削除します。
  - [インベントリ (Inventory)] タブで、アプライアンスの [⋮ (省略符号) 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。
  - **構成チャンネルのダウン**: 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、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。
4. Manager のアプライアンスステータスが [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. [集中管理 (Central Management)] からプライマリ Manager を削除します。
  - [インベントリ (Inventory)] タブで、プライマリ Manager の [⋮ (省略符号) 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。
  - **構成チャンネルのダウン**: 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、Manager アプライアンスコンソールにログイン



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。

### 3. Manager の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、Manager のホスト名またはネットワークドメイン名を変更します。

**Manager のフェールオーバー:** 2 つの Manager がある場合、プライマリ Manager でこの手順を実行するだけで十分です。以下の手順で、セカンダリ Manager を登録します。「[5. Central Management へのアプライアンスの追加](#)」に進みます。

1. Manager アプライアンスコンソール(SystemConfig)に sysadmin としてログインします。
2. [ネットワーク(Network)] を選択します。
3. [管理(Management)] を選択します。
4. アプライアンスのネットワーク IP モードを選択するか、変更せずそのままにします。
5. [ホスト名(Host Name)] フィールドと [ドメイン(Domain)] フィールドを選択します。新しい情報を入力します。



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。

6. 画面に表示される指示に従って、変更を確認します。

### 4. [集中管理(Central Management)] への Manager の登録

1. Manager アプライアンスコンソールに sysadmin としてログインします。
2. [リカバリ(Recovery)] を選択します。
3. [アプライアンスの追加(Add Appliance)] を選択します。
4. Manager の IP アドレス、ユーザー名およびパスワードを入力します。
5. 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。Manager アプライアンスのステータスが以下のように表示されていることを確認します：[接続済み(Connected)]。

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

## 5. Central Management へのアプライアンスの追加

各アプライアンスコンソール(SystemConfig)を使用して、他のアプライアンスを[集中管理(Central Management)]に追加します。

- 一度に1つ: 一度に1つのアプライアンスを設定します。お使いのクラスタ内で次のアプライアンスの設定を開始する前に、[集中管理(Central Management)]でアプライアンスのステータスが[接続済み(Connected)]であることを確認します。
- [集中管理(Central Management)]: Manager IP アドレス、Manager の admin パスワード、および Secure Network Analytics ドメインが必要です。
- 順序: 「[アプライアンスの設定順序](#)」に従います。
- アクセス: Central Management にアクセスするには管理者権限が必要です。

### アプライアンスの設定順序

次の順序でアプライアンスを設定し、各アプライアンスの詳細を書き留めます。

順序	アプライアンス	詳細
1.	UDP Director (別名 FlowReplicators)	
2.	Flow Collector 5000 シリーズ データベース	エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [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.	Data Node	
7.	セカンダリ Manager (使用する場合)	セカンダリ Manager の設定を開始する前に、プライマリ Manager が [接続済み(Connected)] として表示されていることを確認します。  セカンダリ Manager は、自身を Central Manager として選択します。すべてのアプライアンスの設定後にフェールオーバーを設定します。手順については、「 <a href="#">8. Manager フェールオーバーペアの設定</a> 」を参照してください。

1. アプライアンスコンソールに sysadmin としてログインします。

**セカンダリ Manager のみ:** セカンダリ Manager がある場合は、sysadmin としてログインします。初回セットアップの指示に従います ([システムコンフィギュレーションガイド](#) の手順を参照してください)。Manager は、自身を Central Manager として選択します。すべてのアプライアンスが [集中管理 (Central Management)] に接続された後に、フェールオーバーを設定します。

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

2. [リカバリ (Recovery)] を選択します。
3. [アプライアンスの追加 (Add Appliance)] を選択します。
4. Manager の IP アドレスと管理者パスワードを入力します。[OK] をクリックします。
5. 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以下のように表示されていることを確認します: [接続済み (Connected)]。

**!** 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 Manager 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 [集中管理 (Central Management)] に追加します ([設定の順序と詳細を使用](#))。

The screenshot shows the 'Central Management' web interface. The 'Inventory' tab is active, displaying '4 Appliances found'. Below this is a search filter box and a table of appliances. The table has columns for 'Appliance Status', 'Host Name', and 'Type'. All four appliances listed have a status of 'Connected'.

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

6. 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。

## 6. Data Store データベースの開始

**i** 展開に Data Node がない場合は、「[7. 信頼ストアからの古い Manager 証明書の削除](#)」に進みます。

1. [集中管理 (Central Management)] で以下を選択します: データストア > [データベースコントロール (Database Control)]。
2. まず、[データベースステータス (Database Status)] 列に移動し、データベースが次のように表示されていることを確認します: [ダウン (Down)]。
3. データベースの [アクション (Actions)] 列の [... (省略符号) アイコン] をクリックします。
4. [開始 (Start)] を選択します。
5. データベースのステータスが次のように表示されていることを確認します: [アップ (Up)]。

## 7. 信頼ストアからの古い Manager 証明書の削除

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

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

1. アプライアンスの ... (省略符号) 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 Manager 証明書 (アイデンティティ、中間、ルート) を見つけます。
5. [削除 (Delete)] をクリックして古い証明書それぞれを削除します。
6. [設定の適用 (Apply settings)] をクリックします。画面に表示される指示に従って操作します。
7. [集中管理 (Central Management)] のインベントリで、アプライアンスと Manager 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、UDP Director、および Data Node で手順 1 ~ 7 を繰り返します。

## 8. Manager フェールオーバーペアの設定

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

## Manager 以外のアプライアンス

次の手順に従って、Manager 以外のアプライアンス (Flow Collector、Flow Sensor、UDP Director、または Data Node) のホスト名とネットワークドメイン名を変更します。



カスタム証明書を使用している場合は、誤って証明書を上書きした場合に備えて、ネットワーク設定 (ホスト名、ネットワークドメイン名、または eth0 IP アドレス) を変更する前に、証明書を保存します。シスコ自己署名アプライアンス 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、次の手順に従います: [SSL/TLS アプライアンス アイデンティティ証明書の置換](#)。

### 概要

全体的な手順は次のとおりです。

1. [Data Store データベースを停止する](#)
2. [Central Management からのアプライアンスの削除](#)
3. [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](#)
4. [\[集中管理 \(Central Management\)\] へのアプライアンスの追加](#)
5. [Data Store データベースの開始](#)



Manager 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、「[Manager](#)」の指示に従います。

### 1. Data Store データベースを停止する

データベースを停止せずに、3 つ以上の Data Node がある状況で操作する場合は、[シスコ サポート](#) に連絡してサポートを求めてください。



展開に Data Node がない場合は、「[2. Central Management からのアプライアンスの削除](#)」を参照してください。

1. 次の URL にアクセスしてください: Central Management > データストア > [データベースコントロール (Database Control)]。
2. まず、[データベースステータス (Database Status)] 列に移動し、データベースが次のように表示されていることを確認します: [アップ (Up)]。
3. データベースの [アクション (Actions)] 列の [... (省略符号) アイコン] をクリックします。
4. [停止 (Stop)] を選択します。
5. データベースのステータスが次のように表示されていることを確認します: [ダウン (Down)]。


## 2. 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。… (省略符号) アイコンをクリックします。
4. [このアプライアンスの削除 (Remove This Appliance)] を選択します。

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

## 3. 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

1. アプライアンスコンソール (SystemConfig) に sysadmin としてログインします。
2. [ネットワーク (Network)] を選択します。
3. [管理 (Management)] を選択します。
4. アプライアンスのネットワーク IP モードを選択するか、変更せずそのままにします。
5. [ホスト名 (Host Name)] フィールドと [ドメイン (Domain)] フィールドを選択します。新しい情報を入力します。

 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。

6. 画面に表示される指示に従って、変更を確認します。

## 4. [集中管理 (Central Management)] へのアプライアンスの追加


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。

**セカンダリ Manager のみ:** セカンダリ Manager がある場合は、sysadmin としてログインします。初回セットアップの指示に従います ([システムコンフィギュレーションガイド](#) の手順を参照してください)。Manager は、自身を Central Manager として選択します。すべてのアプライアンスが [集中管理 (Central Management)] に接続された後に、フェールオーバーを設定します。


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

2. [リカバリ (Recovery)] を選択します。
3. [アプライアンスの追加 (Add Appliance)] を選択します。
4. Manager の IP アドレスと管理者パスワードを入力します。[OK] をクリックします。

5. 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以下のように表示されていることを確認します:[接続済み(Connected)]。

 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](#)」と「[信頼ストアからの証明書の削除](#)」を参照してください。

## 5. Data Store データベースの開始

 展開に Data Node がない場合は、このセクションをスキップできます。

1. [集中管理 (Central Management)] で以下を選択します: データストア > [データベースコントロール (Database Control)]。
2. まず、[データベースステータス (Database Status)] 列に移動し、データベースが次のように表示されていることを確認します:[ダウン (Down)]。
3. データベースの [アクション (Actions)] 列の [⋮ (省略符号) アイコン] をクリックします。
4. [開始 (Start)] を選択します。
5. データベースのステータスが次のように表示されていることを確認します:[アップ (Up)]。



## 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、初回セットアップ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。[\[集中管理 \(Central Management\)\]](#) で選択した [ネットワーク インターフェイスの変更](#) や、アプライアンスコンソール (SystemConfig) 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。Data Node の eth0 IP アドレスを変更する場合は、[シスコサポート](#) に連絡してサポートを求めてください。
- **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。
- **カスタム証明書を使用している場合は、** 誤って証明書を上書きした場合に備えて、ネットワーク設定 (ホスト名、ネットワークドメイン名、または eth0 IP アドレス) を変更する前に、証明書を保存します。シスコ自己署名アプライアンス 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、次の手順に従います: [SSL/TLS アプライアンス アイデンティティ証明書の置換](#)。



この手順を使用して Data Node の eth0 ネットワーク インターフェイスを変更することは避けてください。Data Node の eth0 IP アドレスを変更する場合は、[シスコ サポート](#) に連絡して専門家のサポートを求めてください。

### 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 … (省略符号) 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。

### [集中管理 (Central Management)] でのネットワーク インターフェイスの変更

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

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


- **eth0:** アプライアンスの IP アドレスを変更するには、「[アプライアンスの IP アドレスの変更](#)」を参照してください。
- **eth2 (Flow Collector 5000 シリーズのみ)** ネットワーク インターフェイス
- Flow Sensor のネットワーク インターフェイス
- UDP Director のネットワーク インターフェイス
- Data Node 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 [集中管理 (Central Management)] から一時的に削除します。

また、画面に表示される指示に従って、証明書の再生成が必要かどうか、または証明書を保持するを選択できるかどうかを確認してください。

 **カスタム証明書を使用している場合は、誤って証明書を上書きした場合に備えて、ネットワーク設定 (ホスト名、ネットワークドメイン名、または IP アドレス) を変更する前に、証明書を保存します。シスコ自己署名アプライアンス 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、次の手順に従います: [SSL/TLS アプライアンス アイデンティティ証明書の置換](#)。**


## 要件

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

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

## アプライアンスの手順の選択

- **Manager:** [Manager](#)
- **Flow Collector、Flow Sensor、UDP Director:** [Manager 以外のアプライアンス](#)

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

## Manager

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

**Manager のフェールオーバー:** Manager がフェールオーバーペアとして設定されている場合は、Manager の設定を変更する前に、フェールオーバーの関係を削除します。[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。

**!** カスタム証明書を使用している場合は、誤って証明書を上書きした場合に備えて、ネットワーク設定 (ホスト名、ネットワークドメイン名、または eth0 IP アドレス) を変更する前に、証明書を保存します。シスコ自己署名アプライアンス 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、次の手順に従います: [SSL/TLS アプライアンス アイデンティティ証明書の置換](#)。

## 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. [Manager IP アドレスの変更](#)
3. [\[集中管理 \(Central Management\)\] への Manager の登録](#)
4. [Central Management へのアプライアンスの追加](#)
5. [信頼ストアからの古い Manager 証明書の削除](#)
6. [Manager フェールオーバーペアの設定](#)

**!** この手順を使用して Data Node の eth0 ネットワーク インターフェイスを変更することは避けてください。Data Node の eth0 IP アドレスを変更する場合は、[シスコサポート](#)に連絡して専門家のサポートを求めてください。

## 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 Manager を除く) を [集中管理 (Central Management)] から削除します。
  - [インベントリ (Inventory)] タブで、アプライアンスの [⋮ (省略符号) アイコン] をクリックします。
  - [このアプライアンスの削除 (Remove This Appliance)] を選択します。
  - **コンフィギュレーションチャネルのダウン:** アプライアンスのステータスが [コンフィギュレーションチャネルのダウン (Config Channel Down)] と表示されている場合は、アプ

イア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. Manager のアプライアンスステータスが [接続済み (Connected)] と表示されていることを確認します。

The screenshot shows the 'Inventory' page with the heading '1 Appliances found'. Below is a search bar and a table with columns: APPLIANCE STATUS, HOST NAME, TYPE, IP ADDRESS, and ACTIONS. The 'APPLIANCE STATUS' column contains the word 'Connected', which is highlighted with a red box. The 'TYPE' column shows 'Manager' and the 'ACTIONS' column has a blue circular icon.

APPLIANCE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Connected		Manager		

5. [集中管理 (Central Management)] からプライマリ Manager を削除します。
  - [インベントリ (Inventory)] タブで、プライマリ Manager の [... (省略符号) 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、Manager 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. Manager IP アドレスの変更

次の手順を実行して、Manager IP アドレス (eth0) を変更します。

**Manager のフェールオーバー:** 2 つの Manager がある場合、プライマリ Manager でこの手順を実行するだけで十分です。以下の手順で、セカンダリ Manager を登録します。「[4. Central Management へのアプライアンスの追加](#)」に進みます。

1. Manager アプライアンスコンソール (SystemConfig) に sysadmin としてログインします。
2. [ネットワーク (Network)] を選択します。
3. [管理 (Management)] を選択します。
4. アプライアンスのネットワーク IP モードを選択するか、変更せずそのままにします。
5. [IP アドレス (IP Address)] フィールドを選択します。新しい情報を入力します。
6. 画面に表示される指示に従って、変更を確認します。

## 3. [集中管理 (Central Management)] への Manager の登録

1. Manager アプライアンスコンソールに sysadmin としてログインします。
2. [リカバリ (Recovery)] を選択します。
3. [アプライアンスの追加 (Add Appliance)] を選択します。
4. Manager の IP アドレス、ユーザー名およびパスワードを入力します。
5. 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。Manager アプライアンスのステータスが以下のように表示されていることを確認します: [接続済み (Connected)]。

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

## 4. Central Management へのアプライアンスの追加

アプライアンスコンソール (SystemConfig) を使用して、他のアプライアンスを [集中管理 (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。
- [集中管理 (Central Management)]: Manager IP アドレス、Manager パスワード、および Secure Network Analytics ドメインが必要です。
- **順序**: 「[アプライアンスの設定順序](#)」に従います。
- **アクセス**: Central Management にアクセスするには管理者権限が必要です。

### アプライアンスの設定順序

次の順序でアプライアンスを設定し、各アプライアンスの詳細を書き留めます。

順序	アプライアンス	詳細
1.	UDP Director (別名 FlowReplicators)	
2.	Flow Collector 5000 シリーズ データベース	エンジンの設定を開始する前に、Flow Collector 5000 シリーズ データベースが [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 Manager (使用する場合)	<p>セカンダリ Manager の設定を開始する前に、プライマリ Manager が [接続済み (Connected)] として表示されていることを確認します。</p> <p>セカンダリ Manager は、自身を Central Manager として選択します。すべてのアプライアンスの設定後にフェールオーバーを設定します。詳細については、「<a href="#">6. Manager フェールオーバーペアの設定</a>」を参照してください。</p>
----	------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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。

**セカンダリ Manager のみ:** セカンダリ Manager がある場合は、sysadmin としてログインします。初回セットアップの指示に従います ([システムコンフィギュレーションガイド](#) の手順を参照してください)。Manager は、自身を Central Manager として選択します。すべてのアプライアンスが [集中管理 (Central Management)] に接続された後に、フェールオーバーを設定します。

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

2. [リカバリ (Recovery)] を選択します。
3. [アプライアンスの追加 (Add Appliance)] を選択します。
4. Manager の IP アドレスと管理者パスワードを入力します。[OK] をクリックします。
5. 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以下のように表示されていることを確認します: [接続済み (Connected)]。

 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 Manager 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 [集中管理 (Central Management)] に追加します ([設定の順序と詳細を使用](#))。



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

6. 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. 信頼ストアからの古い Manager 証明書の削除

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

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

1. アプライアンスの ... (省略符号) 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 Manager 証明書 (アイデンティティ、中間、ルート) を見つけます。
5. [削除 (Delete)] をクリックして古い証明書それぞれを削除します。
6. [設定の適用 (Apply settings)] をクリックします。画面に表示される指示に従って操作します。
7. [集中管理 (Central Management)] の [インベントリ (Inventory)] ページで、アプライアンスと Manager 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. Manager フェールオーバーペアの設定

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



## Manager 以外のアプライアンス

次の手順に従って、Manager 以外のアプライアンスである Flow Collector、Flow Sensor、および UDP Director の IP アドレスを変更します。

また、画面に表示される指示に従って、証明書の再生成が必要かどうか、または証明書を保持することを選択できるかどうかを確認してください。

**!** カスタム証明書を使用している場合は、誤って証明書を上書きした場合に備えて、ネットワーク設定（ホスト名、ネットワークドメイン名、または IP アドレス）を変更する前に、証明書を保存します。シスコ自己署名アプライアンス 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、次の手順に従います：[SSL/TLS アプライアンス アイデンティティ証明書の置換](#)。

### 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](#)
3. [\[集中管理 \(Central Management\)\] へのアプライアンスの追加](#)

**!** この手順を使用して Data Node の eth0 ネットワークインターフェイスを変更することは避けてください。Data Node の eth0 IP アドレスを変更する場合は、[シスコ サポート](#)に連絡して専門家のサポートを求めてください。

**i** Manager の IP アドレスを変更するには、「[Manager](#)」の手順に従います。

### 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。… (省略符号) アイコンをクリックします。
4. [このアプライアンスの削除 (Remove This Appliance)] を選択します。

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

## 2. アプライアンスの IP アドレスの変更

1. アプライアンスコンソール(SystemConfig)に sysadmin としてログインします。
2. [ネットワーク(Network)]を選択します。
3. [管理(Management)]を選択します。
4. アプライアンスのネットワーク IP モードを選択するか、変更せずそのままにします。
5. [IPアドレス(IP Address)]フィールドを選択します。新しい情報を入力します。
6. 画面に表示される指示に従って、変更を確認します。


## 3. [集中管理(Central Management)] へのアプライアンスの追加

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。

**セカンダリ Manager のみ:** セカンダリ Manager がある場合は、sysadmin としてログインします。初回セットアップの指示に従います ([システムコンフィギュレーションガイド](#) の手順を参照してください)。Manager は、自身を Central Manager として選択します。すべてのアプライアンスが [集中管理(Central Management)] に接続された後に、フェールオーバーを設定します。

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

2. [リカバリ(Recovery)]を選択します。
3. [アプライアンスの追加(Add Appliance)]を選択します。
4. Manager の IP アドレスと管理者パスワードを入力します。[OK] をクリックします。
5. 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以下のように表示されていることを確認します:[接続済み(Connected)]。

 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](#)」と「[信頼ストアからの証明書の削除](#)」を参照してください。

## SSL/TLS クライアント アイデンティティの追加

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

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

### 追加の証明書の設定

このガイドでは、アプライアンス アイデンティティとクライアント アイデンティティの設定について説明します。証明書、およびサーバー ID 検証の要件を必要とする Secure Network Analytics が追加の設定が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 (Help)] の手順に従います。[**?** (ヘルプ) アイコンをクリックします。[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。
- **シスコ ISE または Cisco ISE-PIC:** 次の手順を実行します: [ISE および ISE-PIC コンフィギュレーションガイド](#)。
- **LDAP:** [ヘルプ (Help)] の手順に従います。**?** (ヘルプ) アイコンをクリックします。[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 (Help)] の手順に従います。**?** (ヘルプ) アイコンをクリックします。[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:** 次の手順を実行します: [システムコンフィギュレーションガイド](#)。
- **応答管理に対する SMTP の設定:** ヘルプの手順に従います。**?** (ヘルプ) アイコンをクリックします。[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、次を参照してください: [コンフィギュレーションガイド](#)。

### 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、Manager 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、Manager の [… (省略符号) 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。

**i** 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。

**i** 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 a 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、Manager の [⋮ (省略符号) 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
[Redacted]	fs-7- 1.la	fs-7- 1.la	2020-11-20 17:51:53	2025-11-20 17:51:53	3	8192 bits	Delete
[Redacted]	121- 1.lanc m	121- 1.lanc m	2020-11-20 17:42:20	2025-11-20 17:42:20	39	8192 bits	Delete

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、Manager の [⋮ (省略符号) 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てい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がある場合は、次の手順に従って Manager 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、Manager の [\*\*\* (省略符号) 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
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					
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-					
1.lanc		1.lanc			39		
m		m					

- [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。
- [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。
- [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

- [Central Management](#) を開きます。
- [インベントリ (Inventory)] タブで、Manager の [\*\*\* (省略符号) アイコン] をクリックします。
- [アプライアンス構成の編集 (Edit Appliance Configuration)] を選択します。
- [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。
- [新規追加 (Add New)] をクリックします。
- 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)] を選択します。[次へ (Next)] をクリックします。

**i** CSR を生成する必要がある場合は、「[Central Management での CSR の生成](#)」に進みます。

- [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。
- [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。
- [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。
- [設定の適用 (Apply settings)] をクリックします。
- 追加の [SSL/TLS クライアントアイデンティティ](#) のリストを確認します。新しい証明書が表示されてい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 … (省略符号) 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。

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

**!** 続行する前に、会社のポリシーを確認します。

## アプライアンスアイデンティティ証明書が無効なのはなぜですか。

アプライアンスアイデンティティ証明書を認証局からのカスタム証明書に置き換えた場合は、[要件](#)を満たしていることを確認します。

また、新しいアプライアンスアイデンティティ証明書が[必要な信頼ストア](#)に保存されていることを確認します。

手順については、「[SSL/TLS アプライアンスアイデンティティ証明書の置換](#)」を参照してください。

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

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

1. アプライアンスコンソールに sysadmin としてログインします。
  - **最初:** 複数のアプライアンスを削除する場合は、最初に Flow Collector、Flow Sensor、UDP Director、および Data Node 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 Manager にログインします。

**!** 最後に [集中管理 (Central Management)] から Manager を削除します。

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

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



## 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 12 月 13 日	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は、以下の URL でご確認いただけます。

[https://www.cisco.com/c/ja\\_jp/about/legal/trademarks.html](https://www.cisco.com/c/ja_jp/about/legal/trademarks.html)。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)