# Cisco StealthWatch

ISE および ISE-PIC コンフィギュレーション ガイド 7.0

# 目次

# はじめに

## 概要

このドキュメントは、Cisco ISE を使用して Stealthwatch を導入するシスコのエンジニアおよびお客様に、Stealthwatch v7.0 を Cisco ISE pxGrid に接続する際に必要な設定ワークフローの変更情報を提供するものです。

## 技術的な詳細情報

Stealthwatch と Cisco ISE を接続するには、証明書を適切に導入して 2 つのシステム間で信頼できる通信を確立する必要があります。証明書の導入では、さまざまな製品やアプリケーションのインターフェイス（SMC Web アプリケーション、中央管理インターフェイス、Cisco ISE サーバ管理ポータル）を使用する必要があります。

V7.0 以降の Stealthwatch は、Stealthwatch 中央管理で生成された証明書署名要求（CSR）によって作成されたクライアント証明書のみをインポートして、ISE pxGrid ノードに接続します。そのため、証明書の管理ワークフローが以前のバージョンの Stealthwatch とは異なります。

## 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。
- Cisco Stealthwatch サポートのお問い合わせ先：
  - Web でケースを開く場合：http://www.cisco.com/c/en/us/support/index.html
  - 電子メールでケースを開く場合：tac@cisco.com
  - 電話でサポートを受ける場合：800-553-2447（米国）
  - ワールドワイド サポート番号：www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

# 証明書の導入

## オプション 1：ISE 内部認証局を使用した証明書の導入（推奨）

証明書の導入には、ISE 内部認証局（CA）を使用する方法をお勧めします。この方法は、ISE 2.2 以降でのみ使用できます。この方法を実施するには、以下の手順を使用します。

### Stealthwatch pxGrid クライアント証明書の生成

#### Stealthwatch 中央管理でのクライアント証明書の CSR の生成

1. StealthWatch Management Console にログインします。
2. [グローバル設定（Global Settings）] アイコンをクリックしてから、[中央管理（Central Management）] をクリックします。
3. アプライアンス マネージャの [インベントリ（Inventory）] ページで、ISE に接続する SMC の [アクション（Actions）] メニューをクリックします。[アプライアンス設定の編集（Edit Appliance Configuration）] を選択します。
4. [アプライアンス（Appliance）] タブの [追加の SSL/TLS クライアント ID（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。[CSR の生成（Generate a CSR）] フォームが開きます。
6. [RSA キー長（RSA Key Length）] を選択し、[CSR の生成（Generate a CSR）] セクションの残りのフィールドを入力します。
7. [CSR の作成（Generate CSR）] をクリックします。生成プロセスは数分かかることがあります。
8. [CSR のダウンロード（Download CSR）] をクリックし、CSR ファイルをコンピュータに保存します。

## ISE の内部 CA を使用して生成された CSR に基づく証明書の作成

1. ISE 管理インターフェイスにログインします。
2. [管理（Administration）] > [pxGrid サービス（pxGrid Services）] > [証明書（Certificates）] に移動します。[pxGrid 証明書の生成（Generate pxGrid Certificates）] フォームが開きます。

> パスは ISE-PIC とは異なる場合があります。

3. [処理の選択（I want to）] フィールドで、[単一の証明書の生成（証明書署名要求あり）（Generate a single certificate (with certificate signing request)）] を選択します。
4. 前の項で生成した CSR をテキスト エディタで開き、[証明書署名要求の詳細（Certificate Signing Request Details）] フィールドにファイルの内容をコピーします。
5. 必要に応じて、説明を入力します。
6. [証明書のダウンロード形式（Certificate Download Format）] フィールドで、[PKCS12 形式（証明書チェーンを含む。証明書チェーンとキーの両方で 1 つのファイル）（PKCS12 format (including certficate chain; one file for both the certificate chain and key)）] を選択します。
7. [認証パスワード（Certificate Password）] および [パスワードの確認（Confirm password）] フィールドにパスワードを入力します。このパスワードは、[追加の SSL/TLS クライアント ID（Additional SSL/TLS Client Identities）] セクションで証明書を Stealthwatch 中央管理にアップロードする（「**Stealthwatch 中央管理への SMC クライアント証明書の追加**」を参照）ときに要求されます。
8. [作成（Create）] をクリックします。

## Stealthwatch 中央管理への SMC クライアント証明書の追加

1. 上記の項で作成したファイルを解凍して PKCS12 ファイルにアクセスします。

> このファイルをダウンロードするため、ポップアップ メニューをブロック解除することが必要になる場合があります。

2. 中央管理で SMC 設定の [追加の SSL/TLS クライアント ID（Additional SSL/TLS Client Identities）] セクションに移動します。
3. [追加の SSL/TLS クライアント ID（Additional SSL/TLS Client Identities）] セクションには、作成したクライアント証明書をインポートするフォームが含まれています。

4. 証明書のフレンドリ名を指定し、[ファイルの選択（Choose File）] をクリックして証明書ファイルを探します。
5. 前の項で指定したパスワードを入力します。
6. [クライアント ID の追加（Add Client Identity）] をクリックしてシステムに証明書を追加します。
7. [設定を適用（Apply Settings）] をクリックして変更を保存します。

## Stealthwatch 信頼ストアへの Cisco ISE サブ CA 証明書の追加

1. ISE 管理インターフェイスにログインします。
2. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] に移動して [認証局証明書（Certificate Authority Certificates）] をクリックします。
3. **証明書サービス エンドポイント サブ CA** の証明書を見つけてコンピュータにエクスポートします。
4. StealthWatch Management Console にログインします。
5. [グローバル設定（Global Settings）] アイコンをクリックしてから、[中央管理（Central Management）] をクリックします。
6. アプライアンス マネージャの [インベントリ（Inventory）] ページで、SMC の [アクション（Actions）] メニューをクリックします。[アプライアンス設定の編集（Edit Appliance Configuration）] を選択します。
7. [全般（General）] タブを選択します。
8. [信頼ストア（Trust Store）] セクションに移動し、エクスポート済みの ISE CA 証明書をインポートします。
9. [新規追加（Add New）] をクリックします。
10. 証明書のフレンドリ名を指定して [ファイルの選択（Choose File）] をクリックし、エクスポート済みの ISE CA 証明書を選択します。
11. [証明書の追加（Add Certificate）] をクリックして変更を保存します。

これで証明書が導入され、2 つのシステム（Stealthwatch と ISE）は相互に信頼するようになりました。「**ISE 設定の追加**」の章に進み、ISE pxGrid ノードへの接続をセットアップします。

# オプション 2：外部認証局（CA）サーバを使用した証明書の導入

## Stealthwatch pxGrid クライアント証明書の生成

### Stealthwatch pxGrid クライアント証明書の CSR の生成

1. StealthWatch Management Console にログインします。
2. [グローバル設定（Global Settings）] アイコンをクリックしてから、[中央管理（Central Management）] をクリックします。
3. アプライアンス マネージャの [インベントリ（Inventory）] ページで、ISE に接続する SMC の [アクション（Actions）] メニューをクリックします。[アプライアンス設定の編集（Edit Appliance Configuration）] を選択します。
4. [アプライアンス（Appliance）] タブの [追加の SSL/TLS クライアント ID（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。[CSR の生成（Generate a CSR）] フォームが開きます。
6. [RSA キー長（RSA Key Length）] を選択し、[CSR の生成（Generate a CSR）] セクションの残りのフィールドを入力します。
7. [CSR の作成（Generate CSR）] をクリックします。生成プロセスは数分かかることがあります。
8. [CSR のダウンロード（Download CSR）] をクリックし、CSR ファイルをローカルに保存します。

### 外部 CA を使用した Stealthwatch pxGrid クライアント証明書の作成

> この例では MS Server 2012 の Microsoft Active Directory 証明書サービスを使用しますが、別の外部 CA を使用することもできます。

1. https://server/certsrv/（server は MS サーバの IP または DNS）で Microsoft Active Directory 証明書サービスに移動します。
2. [証明書を要求する（Request a certificate）] をクリックします。
3. [高度な証明書要求（Advanced certificate request）] の送信を選択します。
4. 前の項で生成した CSR ファイルの内容を [保存された要求（Saved Request）] フィールドにコピーします。

5. [証明書テンプレート（Certificate Template）] で [pxGrid] を選択し、[送信（Submit）] をクリックします。
6. 生成された証明書を **Base-64** 形式でダウンロードし、**pxGrid_client.cer** として保存します。

## SMC への Stealthwatch pxGrid クライアント証明書の追加

1. 中央管理で SMC 設定の [追加の SSL/TLS クライアント ID（Additional SSL/TLS Client Identities）] セクションに移動します。
2. [追加の SSL/TLS クライアント ID（Additional SSL/TLS Client Identities）] セクションには、作成したクライアント証明書をインポートするフォームが含まれています。
3. 証明書のフレンドリ名を指定し、[ファイルの選択（Choose File）] をクリックして証明書ファイルを探します。
4. 前の項で指定したパスワードを入力します。
5. [クライアント ID の追加（Add Client Identity）] をクリックしてシステムに証明書を追加します。
6. [設定を適用（Apply Settings）] をクリックして変更を保存します。

## SMC 信頼ストアへの CA ルート証明書のインポート

1. Microsoft Active Directory 証明書サービスのホーム ページにアクセスし、[CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。
2. [Base-64] 形式を選択して [CA 証明書のダウンロード（Download CA certificate）] をクリックします。
3. 証明書を **CA_Root.cer** として保存します。
4. StealthWatch Management Console にログインします。
5. [グローバル設定（Global Settings）] アイコンをクリックしてから、[中央管理（Central Management）] をクリックします。
6. アプライアンス マネージャの [インベントリ（Inventory）] ページで、SMC の [アクション（Actions）] メニューをクリックします。[アプライアンス設定の編集（Edit Appliance Configuration）] を選択します。
7. [全般（General）] タブを選択します。
8. [信頼ストア（Trust Store）] セクションに移動し、エクスポート済みの CA_Root.cer 証明書をインポートします。

9. [新規追加（Add New）] をクリックします。
10. 証明書のフレンドリ名を指定して [ファイルの選択（Choose File）] をクリックし、エクスポート済みの ISE CA 証明書を選択します。
11. [証明書の追加（Add Certificate）] をクリックして変更を保存します。

## ISE サーバ pxGrid 証明書の生成

### ISE サーバ pxGrid 証明書の CSR の生成

1. ISE 管理インターフェイスを開きます。
2. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [証明書署名要求（Certificate Signing Requests）] に移動します。
3. [証明書署名要求（CSR）の作成（Generate Certificate Signing Request (CSR)）] を選択します。
4. [証明書の用途（Certificate(s) will be used for）] フィールドで [pxGrid] を選択します。
5. 証明書を生成する ISE ノードを選択します。
6. 必要に応じて、その他の証明書の詳細を入力します。
7. [生成（Generate）] をクリックします。
8. [エクスポート（Export）] をクリックしてローカルにファイルを保存します。

### 外部 CA を使用した ISE サーバ pxGrid 証明書の作成

1. https://server/certsrv/（server は MS サーバの IP または DNS）で Microsoft Active Directory 証明書サービスに移動します。
2. [証明書を要求する（Request a certificate）] をクリックします。
3. [高度な証明書要求（Advanced certificate request）] の送信を選択します。
4. 前の項で生成した CSR の内容を [保存された要求（Saved Request）] フィールドにコピーします。
5. [証明書テンプレート（Certificate Template）] で [pxGrid] を選択し、[送信（Submit）] をクリックします。
6. 生成された証明書を **Base-64** 形式でダウンロードし、**ISE_pxGrid.cer** として保存します。

## ISE 信頼ストアへの CA ルート証明書のインポート

1. Microsoft Active Directory 証明書サービスのホーム ページにアクセスし、[CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。
2. [Base-64] 形式を選択して [CA 証明書のダウンロード（Download CA certificate）] をクリックします。
3. 証明書を **CA_Root.cer** として保存します。
4. ISE 管理インターフェイスにログインします。
5. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [信頼できる証明書（Trusted Certificates）] を選択します。
6. [インポート（Import）] > 証明書ファイルを選択し、ルート証明書をインポートします。
7. [ISE 内の認証用に信頼する（Trust for authentication within ISE）] チェックボックスを必ずオンにします。
8. [送信（Submit）] をクリックします。

## 証明書署名要求（CSR）への ISE 証明書のバインド

1. ISE 管理インターフェイスにログインします。
2. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [証明書の管理（Certificate Management）] > [証明書署名要求（Certificate Signing Requests）] を選択します。
3. 前の項で生成した CSR を選択し、[証明書のバインド（Bind Certificate）] をクリックします。
4. [CA 署名付き証明書のバインド（Bind CA Signed Certificate）] フォームで、以前に生成した **ISE_pxGrid.cer** 証明書を選択します。
5. 証明書のフレンドリ名を指定して [送信（Submit）] をクリックします。
6. 再起動を求められたら [はい（Yes）] をクリックします。
7. 証明書の交換を求められたら [はい（Yes）] をクリックします。
8. [管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）] を選択します。
9. 外部 CA によって署名された作成済みの pxGrid 証明書がリストに表示されます。

これで証明書が導入され、2 つのシステム（Stealthwatch と ISE）は相互に信頼するようになりました。「**ISE 設定の追加**」の章に進み、ISE pxGrid ノードへの接続をセットアップします。

# ISE 設定の追加

現在のドメインに Cisco ISE クラスタを設定するには、次の手順を実行します。

> 使用される StealthWatch システムの各ドメインの Cisco ISE クラスタを設定する必要があります。複数の独立した Cisco ISE クラスタを Stealthwatch システムのドメインに追加できますが、同じドメイン内の複数のクラスタで同じ IP アドレスを使用することはできません。

## 設定

次の設定を定義します。

- [クラスタ名（Cluster Name）]：この名前は、SMC デスクトップ クライアントのエンタープライズ ツリーと SMC Web UI の ISE 設定のリストに表示されます。
- [証明書（Certificate）]：これは、SMC 設定インターフェイスの [追加の SSL/TLS クライアント ID（Additional SSL/TLS Client Identities）] セクションにある [フレンドリ名（Friendly Name）] フィールドに入力した名前と同じです。この証明書により、アプライアンスは ID でクライアントを認証できます（つまり SMC が ISE に提供するクライアント証明書です）。
- [プライマリ pxGrid ノード（Primary pxGrid Node）]：アプライアンスが統合されている ISE クラスタ上のプライマリ pxGrid ノードの IP アドレス。
- [セカンダリ pxGrid ノード（オプション）（Secondary pxGride Node (optional)）]：アプライアンスが統合されている ISE クラスタ上のセカンダリ pxGrid ノードの IP アドレス。このノードは、フェールオーバーのために使用されます。プライマリ ノードへの接続が失敗すると、セカンダリ ノードが使用されます。
- [ユーザ名（User Name）]：この名前は、ISE アプライアンスで ISE クラスタ上の pxGrid クライアント リストに表示されます。

## 統合オプション（任意）

ISE クラスタに対して有効にする統合オプションを選択します。

- [適応型ネットワーク制御（Adaptive Network Control）]：ISE のエンドポイントに分類（ANC ポリシー）を適用して、ISE に設定されている認証ポリシーに従ってネットワーク アクセスを変更できます。

- [静的 TrustSec 分類（Static TrustSec Classifications）]：認証プロセス以外でエンドポイント IP と静的に関連付けられた TrustSec セキュリティ グループ タグ（SGT）に関する情報を受信できます。これには、ISE やアクセス レイヤ デバイスに手動で設定された、または SXP プロセスで他のシステムから学習した IP と SGT のバインディングの情報などがあります。このデータは、元のフローにエンドポイント IP アドレスが一致する SGT が存在せず、SGT が割り当てられたエンドポイント IP アドレスにセッションが関連付けられていないフローの拡大に使用されます。
- [ユーザ セッション（User Sessions）]：ユーザ名、エンドポイントの MAC アドレス、デバイス プロファイル、および TrustSec セキュリティ グループに関する情報を含む、ユーザ セッションの更新を受信できます。この情報は、TrustSec セキュリティ グループ情報を含むフローを拡大し、SMC レポートでユーザとセッションを監視するために使用されます。

# 追加パラメータ

## ノード ステータス インジケータ

各 IP アドレス フィールドの横に配置されたノード ステータス インジケータは、追加された各ノードの接続ステータスを示します。これらは、最初のノードの設定と保存後に表示されます。

- 緑色のステータス インジケータは、ノードへの接続が確立され、システムが pxGrid に関する必要なすべての情報トピックをサブスクライブしていることを示しています。
- 赤色のステータス インジケータは、ノードへの接続が確立されていないか、pxGrid に関する必要な情報トピックのサブスクリプションに失敗したことを示しています。接続が存在しない理由、または失敗したサブスクリプションを確認するには、情報アイコンをクリックすると、次の情報が表示されます。
    - [接続中（Connected）]
    - [接続は保留中です（Connection is pending）]：接続は進行中か、または ISE の [pxGrid サービス（pxGrid Services）] ページでのクライアントの承認を待機中
    - [システムエラー（System error）]：詳細についてはログを確認
    - [ノードに到達できませんでした（The node couldn't be reached）]：接続タイムアウト
    - [ユーザが ISE 上の [pxGrid サービス（pxGrid Services）] ページで承認されていません]

- [ISE は SMC によって信頼されていない証明書を提示しています（ISE is presenting a certificate that is not trusted by the SMC）]
- [SMC から提示されたクライアント証明書はISEに信頼されていません（Client certificate presented by the SMC is not trusted by ISE）]

## オプション ステータス

オプション ステータスは、統合オプションが正常に機能するために必要な ISE pxGrid 機能のサブスクリプションの状態を示します。

- [ANC]：正常に機能するには適応型ネットワーク制御および SessionDirectory 機能のサブスクリプションが必要な [適応型ネットワーク制御（Adaptive Network Control）] 統合オプションのステータス。
- [セッション（Sessions）]：正常に機能するには SessionDirectory 機能および TrustSecMetadata 機能のサブスクリプションが必要な [ユーザセッション（User Sessions）] 統合オプションのステータス。
- [SGT 分類（SGT Classifications）]：正常に機能するには SessionDirectory 機能および TrustSecMetadata 機能のサブスクリプションが必要な [SGT分類（SGT Classifications）] 統合オプションのステータス。

統合オプションのステータスには、次のようなものがあります。

- [接続中（Connected）]：システムは ISE に関する必要なすべての情報トピックをサブスクライブしています。
- [オフ（Off）]：この ISE 設定の統合オプションはオフになっています。
- [使用不可（Not available）]：pxGrid への接続がまだ確立されていないため、サブスクリプション情報を利用できません。
- [ユーザは [...] 機能のサブスクリプションを承認されていない（User is not authorized to subscribe to [...] capability）]：ISE 設定ページで指定されたユーザ権限が不十分なため、1 つ以上の必要な機能のサブスクリプションに失敗しました。

## 更新アイコン

関連するノードへの接続を更新するには、更新アイコン（二重矢印）をクリックします。

## Cisco ISE または Cisco ISE-PIC での pxGrid の承認

1. 次のいずれかを実行します。
    a. Cisco ISE を使用している場合は、このアプライアンスにログインし、メイン メニューで [管理（Administration）] をクリックします。開いたページで、[pxGrid サービス（pxGrid Services）] タブをクリックします。
    b. Cisco ISE-PIC を使用している場合は、このアプライアンスにログインし、メインメニューで [サブスクライバ（Subscribers）] をクリックします。開いたページで、[クライアント（Clients）] タブをクリックします。
2. 表示されたテーブルの [クライアント名（Client Name）] 列で、該当するサブスクライバの名前の横にあるチェックボックスをオンにし、テーブルの上部にあるサブメニューで [承認（Approve）] をクリックします。

## [Cisco ISE の設定（Cisco ISE Configuration）] ページの更新

1. SMC Web アプリケーションの [Cisco ISE の設定（Cisco ISE Configuration）] ページに戻り、ページを更新します。
2. 該当する IP アドレス フィールドの横にあるノード ステータス インジケータが、Cisco ISE クラスタまたは Cisco ISE-PIC クラスタへの接続が確立されていることを示す緑色であることを確認します。

# 保存した Cisco ISE クラスタの編集または削除

[アクション（Actions）] 列で、省略記号をクリックしてコンテキスト メニューを開き、適切なオプションを選択します。

- Stealthwatch システム上に存在している Cisco ISE クラスタから、最後に残ったノードを削除することはできません。
- [ライセンス供与されていない機能（Unlicensed Feature）] アラームが Cisco ISE クラスタに対してアクティブになっていても、すべての Cisco ISE クラスタを削除できます。それを行ってから数分以内にアラームが非アクティブになります。
- ISE クラスタを削除しても、履歴のために、クライアント ユーザ名は Cisco ISE から削除されません。ユーザ名は、[pxGridユーザ名（pxGrid Username）] リストの ISE ボックスに引き続き表示されます。

# 拡張 ISE の導入をサポートするための Stealthwatch 設定の調整

デフォルトでは、Stealthwatch フロー コレクタが処理できるセッション数は、アプライアンスで使用可能な合計メモリによって決まります。

次の仕様を参照してください。

| 合計 RAM | セッション数 |
|---|---|
| 8 G 未満 | 131,072 |
| 8 G 以上 | 262,144 |
| 16 G ~ 128 G | 524,288 |
| 128 G 以上 | 2,097,152 |

フロー コレクタがデフォルトでサポートする数を超える ISE セッションを処理できるようにするには、アプライアンスに追加の設定が必要です。ホスト、ユーザ、セッション、デバイスなどの重要なオブジェクトに関する情報を保持するメモリ内データ構造のサイズを設定することになります。

アプライアンスの設定を調整する場合は、テクニカル サポートにお問い合わせください。

# 著作権情報



このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図などの図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。