Cisco Stealthwatch

v7.3.2 ISE およびISE-PIC 構成ガイド

目次

はじめに

概要

このドキュメントでは、Cisco ISE を使用して Stealthwatch を導入するシスコのエンジニアとお客様に、Cisco ISE pxGrid に Stealthwatch v7.3.2 以降を接続するために必要な設定ワークフローの変更点を示します。

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、Stealthwatch は Stealthwatch Central Management から生成された証明書署名要求（CSR）を使用し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。この変更により、証明書の管理ワークフローは、以前のバージョンの Stealthwatch とは異なることになります。

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

証明書の展開

オプション 1：ISE 内部認証局を使用した証明書の展開（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 Central Management からクライアント証明書の CSR を生成

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、[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）] タブの [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。[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. [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. 前のセクションで生成した 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. [証明書パスワード(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 アイデンティティ(Additional SSL/TLS Client Identities)]セクションで証明書を Stealthwatch Central Management にアップロードするときに要求されます(「**はじめに**」を参照)。
8. [作成(Create)]をクリックします。

> 証明書の生成に失敗した場合は、pxGrid_Certificate_Template のキー長が、Stealthwatch で作成した CSR のキー長と一致していることを確認してください。PxGrid_Certificate_Template のキー長を編集するには、[Certificate Template]フィールドの横にあるリンクをクリックします。

Stealthwatch Central Management

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. Central Management で[SMC 設定(SMC Configuration)]の[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。
3. [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. 前のセクションで入力したパスワードを入力します。
6. [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。

> ISE サブ CA 証明書が ISE pxGrid ノードで使用される証明書を発行した認証局のものではない場合は、この手順でその CA 証明書を取得する必要があります。

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、[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、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)] 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。
6. [新規追加(Add New)] をクリックします。
7. 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。
8. [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 pxGrid ノードへの接続を設定するには、「**ISE 設定の追加**」の章に進みます。

オプション 2:外部認証局(CA)サーバを使用した証明書の展開

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、[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)] タブの [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。[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. [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。別の外部 CA も使用できます。

1. Microsoft Active Directory 証明書サービス(https://server/certsrv/)に移動します。ここで、server は MS サーバの IP または DNS です。
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. 前のセクションで生成した 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. Central Management で[SMC 設定(SMC Configuration)]の[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。
2. [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. 前のセクションで入力したパスワードを入力します。
5. [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、[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。[アプライアンス構成の編集(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、ファイルをローカルに保存します。

外部 CA を使用した ISE サーバ pxGrid 証明書の作成

1. Microsoft Active Directory 証明書サービス(https://server/certsrv/)に移動します。ここで、server は MS サーバの IP または DNS です。
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. 前のセクションで生成した 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)]>[信頼証明書(Trusted Certificates)]の順に選択します。
6. [インポート(Import)]>[証明書ファイル(Certificate file)]の順に選択し、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）]の順に選択します。
3. 前のセクションで生成した 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、生成済みの **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）]の順に選択します。
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 pxGrid ノードへの接続を設定するには、「**ISE 設定の追加**」の章に進みます。

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、同じドメイン内のすべてのクラスタで同じ IP アドレスを使用することはできません。

Cisco ISE 構成の設定ページを開く

1. SMC のメインメニューから、[展開(Deploy)] > [Cisco ISEの統合(Cisco ISE Integration)] の順に選択します。
2. ページの右上隅で、[新しい設定の追加(Add New Configuration)] をクリックします。

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企業ツリーと 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 クライアントアイデンティティ(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、アプライアンスはアイデンティティをクライアントとして認証できます(つまり SMC が ISE に提供するクライアント証明書です)。
- [PxGridノード1(PxGrid Node 1)]: 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。
- [PxGridノード2(オプション)(PxGrid Node 2 (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。最初の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。
- [PxGridノード3(オプション)(PxGrid Node 3 (optional))]: アプライアンスが統合されている ISE クラスタ上のターシャリ 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。最初のノードとセカンダリノードへの接続が失敗すると、ターシャリノードが使用されます。
- [クライアント名(Client Name)]: この一意の名前が 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

統合する ISE 製品を選択してください。

- [Cisco ISE]: すべての統合オプションを有効化できます。
- [Cisco ISE-PIC]: セッション更新のみを有効化できます。

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、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。これは、ISE、アクセスレイヤデバイスに手動で設定された、または SXP プロセス内で他のシステムから学習した IP-to-SGT バインディングの可能性があります。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。
- [セッション(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最新情報を受信できます。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。[マシン認証から導出されたセッションの追跡(Track sessions derived from machine authentications)]を有効にして、ユーザセッションの最新情報と一緒にマシンセッションの最新情報も受信します。

その他のパラメータ

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。

- ●([緑色ステータス(Green Status)])アイコンは、ノードへの接続が確立されていること、およびシステムが 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。
- ●([黄色ステータス(Yellow Status)])アイコンは、ノードとの接続が保留中かつ進行中か、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であることを示しています。
- ●([赤色ステータス(Red Status)])アイコンは、ノードへの接続が確立されていないこと、または 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。このアイコンをクリックすると、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示すエラーメッセージを確認できます。

更新アイコン

([更新(Refresh)])アイコンをクリックすると、関連するクラスタとの接続が更新されます。

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、メインメニューから [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。

ISE 統合フェールオーバーの設定

ISE 統合フェールオーバーでは、ISE セッションの最新情報を受信するようにプライマリおよびセカンダリ SMC を設定できます。これにより、プライマリ SMC に障害が発生し、セカンダリ SMC がプライマリロールに切り替わった場合でも、ユーザに関する情報を SMC レポートで引き続き使用できます。

ISE 統合フェールオーバー設定では、次の操作が必要です。

- プライマリ SMC とセカンダリ SMC の両方で ISE 統合を設定します。
- プライマリ SMC とセカンダリ SMC の両方に異なる ISE クライアント証明書を生成します。
- プライマリ SMC とセカンダリ SMC の両方の ISE 設定で異なるクライアント名を指定します。

> SMC フェールオーバー関係を確立済みの場合は、ISE 統合設定を変更するために、セカンダリ SMC をプライマリ SMC に切り替える必要がある場合があります。

ISE 統合フェールオーバーを設定するには、次の手順を実行します。

1. 「**ISE 設定の追加**」の手順に従って、プライマリ SMC を設定します。一意の ISE クライアント証明書を生成し、一意のクライアント名を割り当てるようにしてください。
2. セカンダリ SMC に対してこれらの手順を繰り返し、一意の ISE クライアント証明書を生成し、一意のクライアント名を割り当てるようにします。

   pxGrid ノードと ISE 統合オプションがプライマリ SMC のこれらのオプションと一致していることを確認します。

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 Flow Collector が処理できる同時アクティブセッションの数は、アプライアンスで使用可能なメモリの総量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	セッションの総数
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